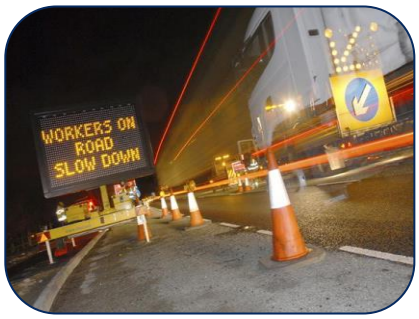
Transport Research Laboratory
Creating the future of transport




FINAL PROJECT REPORT PPR616

Benchmarking study of NSA enforcement powers: final report

S Tong

Prepared for: European Railway Agency

Project Ref: ERA/2011/SAF/OP/03

Quality approved:

Simon Tong (Project Manager)	*S Tong*	Michael Pittman (Technical Referee)	*M Pittman*

Disclaimer

This report has been produced by the Transport Research Laboratory under a contract with European Railway Agency. Any views expressed in this report are not necessarily those of European Railway Agency.

The information contained herein is the property of TRL Limited and does not necessarily reflect the views or policies of the customer for whom this report was prepared. Whilst every effort has been made to ensure that the matter presented in this report is relevant, accurate and up-to-date, TRL Limited cannot accept any liability for any error or omission, or reliance on part or all of the content in another context.

When purchased in hard copy, this publication is printed on paper that is FSC (Forest Stewardship Council) and TCF (Totally Chlorine Free) registered.

Contents amendment record

This report has been amended and issued as follows:

Version	Date	Description	Editor	Technical Referee
1	05/04/12	Interim draft	ST	MP
2	22/05/12	Final draft	ST	MP
3	29/06/12	Revised final draft 1	ST	MP
4	06/07/12	Revised final draft 2	ST	MP

Executive Summary

Background

European Member States that operate railways do so as part of a harmonised network. Each Member State (as well as Norway) is required by Directive 2004/49/EC to operate a National Safety Authority (NSA). Each NSA is expected to be independent of railway undertakings (RUs) and infrastructure managers (IMs). The primary functions of each NSA are to oversee state railway operations and to issue safety certificates to RUs and safety authorisations to IMs. Certificates and authorisations are granted on the basis of the RU/IM having a safety management system (SMS). The SMS must comply with the European safety regulatory framework and specifically with the requirements of Regulations 1158/2010 and 1169/2010.

According to Directive 2004/49/EC, NSA have a duty to supervise all RUs and IMs with a valid safety certificate/authorisation to ensure that they are operating in accordance with their SMS and to enforce the regulatory framework should any RU or IM demonstrate non-compliance, or a potential or real safety hazard. Regulations 1158/2010 and 1169/2010 introduced principles to govern supervision of RUs/IMs. These principles require supervision to be proportionate, consistent, targeted and transparent. In carrying out supervision, NSA must prioritise their resources, be accountable for their actions and cooperate with other NSA. A forthcoming Regulation (the Common Safety Method on Supervision) will govern further the supervision activities of NSA.

Objectives

This study examines how NSA carry out their duty of supervision and enforcement within the European rail market with a view to identifying good practice and supporting the process of harmonisation. The overall aim of this work is to establish whether there is a baseline level of good practice for supervision and enforcement activity. To achieve this aim, the project has the following specific objectives:

i. To explore the supervision and enforcement activity, responsibilities and powers of each NSA that is subject to EU regulation.

ii. To compare the supervision and enforcement activity, responsibilities and powers of NSA with those of competent authorities responsible for enforcement in other key industrial sectors across the EU.

iii. To develop good practice guidance for NSA enforcement activity.

Approach

This study comprised three main tasks.

Task 1 – NSA survey

Task 1 was an investigation of supervision and enforcement methods used by NSA. An online questionnaire survey was issued to all participants in the NSA Network, which is organised by the European Railway Agency. The questionnaire explored how each NSA supervises and enforces. It focused on the organisation and structure of NSA, the competence development of staff, planning and delivering supervision, delivering enforcement, and self-evaluation and continuous improvement. The questionnaire was

issued in English and NSA were given foreign language support on request. A response was received from 22 NSA out of a total 25.

The questionnaire was followed by interviews with a subsample of NSA that represented a range of supervision practices. The interviews were by telephone with seven NSA and in person with four NSA. The interviews focused on collecting detailed information on how NSA had interpreted and implemented the regulated principles of supervision and how closely their practices are consistent with the forthcoming Common Safety Method on Supervision.

Task 2 – Survey of competent authorities in other industrial sectors

Task 2 was an investigation of supervision and enforcement methods used by competent authorities in other industrial sectors. A desktop review of Member State websites for occupational health and safety and civil aviation safety authorities sought evidence of good practice on the supervision principles and practices specified by the regulatory framework for rail. As with Task 1, follow-up interviews were conducted by telephone with a small number of competent authorities.

Task 3 – Analysis

Task 3 brought together the findings from the first two tasks and mapped them against the regulatory framework. The examples of practice from NSA and competent authorities were collated thematically and according to the core activities of an NSA related to supervision, and were then rated against the principles of supervision. Ratings of -1, 1, 2, or 3 were awarded in accordance with the degree to which the example represented good practice (or not, in some cases). Examples of good practice were then grouped according to each core NSA activity or attribute related to supervision to recommend baseline good practice and then two progressively higher levels of good practice for NSA that wish to develop beyond the baseline recommendations.

Findings and recommendations

Findings are grouped according to six core NSA activities and attributes related to supervision. This study provides baseline recommendations for good practice (highlighted in orange) across each of an NSA's core activities and attributes related to supervision. Further recommendations encourage NSA to reach progressively higher levels of good practice (indicated by yellow and then green highlights).

NSA structure and organisation

The first core NSA attribute was the way each NSA chose to structure and organise itself for supervision and enforcement. The study identified that some NSA have full or partial separation of staff for the two activities of assessment (of safety certificates/ authorisations) and supervision. Other NSA have the same team of staff carrying out these activities. In addition, a few NSA reported separating staff teams according to whether they were addressing matters for RUs or IMs.

In light of these structural differences, it is recommended that NSA should implement:

- Good internal communication between the activities of assessment and supervision, irrespective of how the NSA is structured.
- A process for providing independent or peer reviews of any decisions.
- A consistent knowledge base when selecting staff for specific supervision tasks.
- A single decision-making policy across all supervision teams within the NSA.
- Cooperation with other government safety authorities to deliver consistent supervision and enforcement across all rail-related activities, including those that are not directly under the remit of the NSA.
- A process for consulting with the NSA budget holder to ensure that the NSA has a remit and resources to at least fulfil the tasks assigned to it by the Safety Directive.
- A system for staff to efficiently store and exchange information about each RU/IM.
- An organogram to show the market how the NSA is structured.
- A single committee to oversee and harmonise NSA supervision and other activities. The committee could be represented by senior figures from each division of the NSA.

A further route to delivering effective assessment and supervision is to ensure that each NSA has a general strategy to guide it. NSA varied in their implementation of a strategy; a few had no strategy and of those NSA that did, the strategies varied in duration from 1–7 years.

It is recommended that each NSA has a long-term strategy (>1 year), that is at least published online, and outlines clear strategic goals and a plan for achieving them.

Such a strategy could be enhanced if NSA:

- Organise strategic goals thematically to better engage the market.
- Use multiple methods of dissemination (e.g. posters, presentations, videos) to target RUs/IMs widely, and at all staffing levels.
- Establish measurable service standards (e.g. related to how the NSA will respond during assessment and supervision activities) by which the NSA can verify that it is fulfilling its commitments to the market.
- Adopt 'action plans' to describe how strategic goals will be achieved.
- Adopt an inclusive approach to strategy development and delivery that engages the marketplace (e.g. through conferences, national / regional events, online pledges).
- Create organisational structures to deliver the strategy (e.g. create working groups, formed from NSA and market members, tasked with delivering specific goals).

Not all NSA had a national legislative structure that was compatible with the European safety regulatory framework. Conflicts between national and European legislation were reported to create market confusion. To avoid this, NSA are recommended to:

- Have a statutory function to update or propose national laws and standards.
- Have a legal structure to permit enforcement of all relevant EU legislation.
- Incorporate relevant EU legislation within the national legislative framework.

The majority of NSA do meet the requirement to have a complaints policy for the market to access, but dissemination of policies is inconsistent. It is recommended that complaints policies are:

- Documented on the NSA website.
- Routinely issued to RUs/IMs during regulatory contact and supervision activities.
- Supported by a clear internal process whereby complaints can be escalated up the line management chain within the NSA if they cannot be resolved initially.
- Facilitated by online forms and accessible contact information for the NSA.

NSA are also required to have cooperation agreements with each other. The majority have informal agreements to cooperate, typically on a bilateral basis. To facilitate and develop cooperation agreements—and work towards the goal of supervising and enforcing collaboratively across borders—it is recommended that NSA:

- Assign and publicise a point of contact for cooperation purposes (e.g. a dedicated email, telephone number and/or member of staff).
- Be open and proactive about information exchange (especially with regard to RUs that are operating across borders).
- Liaise with each other regarding the reassessment of safety certificates that are nearing the end of their validity and consider timing to minimise the impact on interdependent Part A and Part B certificates for RUs operating across borders.
- Organise collaborative meetings with other NSA that currently share cross-border traffic, or have markets that would like to expand across borders.
- Agree on how to supervise collaboratively in a way that overcomes language differences and enables NSA to collect the necessary evidence.
- Proactively offer basic information to each other regarding Part A assessments if it is pertinent to an RU's application for a Part B certificate in another Member State.
- Undertake joint supervision activities with other NSA.
- Cooperate with other domestic and European non-rail safety authorities that may influence parts of the rail industry to ensure a coordinated approach.

Competency for supervision and enforcement

The second core NSA attribute related to supervision is the staff competency that is required for supervision and enforcement. Less than half of NSA have formal programmes to train staff for supervision activities and only a quarter of NSA have formal courses to ensure that staff are kept aware of the current legislative framework. To ensure supervision and enforcement is only carried out by competent persons (as per the regulations), it is recommended that NSA:

- Ensure staff are trained to a universal level in essential skills such as auditing techniques.
- Ensure new staff are competent to supervise at the required level before being permitted to work independently. It is recommended that new staff are shadowed by experienced staff and 'signed off' when they have demonstrated the required skills.
- Set competence management as a strategic goal.
- Provide targeted technical training in rail systems (knowledge should be sufficient to supervise but not to subsume the responsibility that RUs/IMs have for safety under the SMS-based approach).
- Source training efficiently by going in-house or, if appropriate, via the rail market.
- Monitor staff competence (e.g. with examinations, case study assessments).
- Consolidate training courses with other domestic government safety authorities.
- Introduce internal online competence management systems to facilitate ongoing staff development and review.

Planning supervision

The third core NSA activity related to supervision is planning. The majority of NSA have, or are developing, a supervision strategy.

It is recommended that all NSA develop a general strategy for supervision activities, not least because it can be used to present a clear case to the NSA budget holder (typically the Ministry) for the resourcing that is needed to meet the planned supervision activities.

Almost all NSA assessed themselves as very targeted in their approach to planning supervision and yet approximately a third did not have specific supervision plans for specific RUs/IMs. It is recommended that NSA:

- Plan supervision for specific RUs/IMs based on an assessment of RU/IM capability.
- Supplement supervision planning by reviewing relevant incident data.
- Distribute planned supervision activities across the periodicity of the certificate/ authorisation to allow more regular supervisory contact with RUs/IMs.
- Implement a systematic, quantitative approach to assessing the capability of an RU/IM, and its risk relative to other RUs/IMs, and use this to plan supervision.
- Access models of incident precursors to plan supervision that will address the events and actions that are believed to lead to incidents.

It is recommended that NSA do not plan supervision based solely on distributing NSA resources equally across RUs/IMs.

Supervision practices

One aspect of the fourth core NSA activity related to supervision is implementing appropriate supervision practices. Most NSA use a range of supervision methods (interviewing staff at RUs/IMs, reviewing documents from RUs/IMs, examining outcomes from the SMS at RUs/IMs) at least every 18 months. Just over half of NSA do so more regularly. Whole checks of the SMS for an RU/IM occur every 1–5 years; some NSA carry out partial checks every 3–12 months or on an ad hoc basis. Currently, 50–90% of supervision activities are proactive. It is recommended that NSA:

- Audit using core methods of document checks (including examining SMS outcomes), interviews with a range of staff at RUs/IMs and frontline inspections.
- Check the whole SMS for each RU/IM at least once in a five-year period of validity for a safety certificate/authorisation.
- Allocate at least 50% of inspections to proactive supervision.
- Check individual parts of the SMS (if not the whole SMS) for each RU/IM more than once during a five-year period of validity for a safety certificate/authorisation.
- Follow an adaptive approach to scheduling supervision. A broad range of intervals between whole and partial checks of the effectiveness of the SMS for each RU and IM could be adopted based on the activities and capabilities of RUs/IMs.
- Plan supervision so that 80% of inspections are proactive.

Delivering supervision

Another aspect of the fourth core NSA activity related to supervision is how supervision is delivered to the market. NSA vary considerably in their approach to auditing RUs/IMs; for example, a single audit could last anywhere between seven hours and one month, depending on the NSA. Decision-making was subject to similar variation. NSA must routinely decide whether enforcement action against a particular RU/IM is required as a result of supervision findings. Although about three-quarters of NSA have demonstrated good practice by developing and publishing decision-making criteria to guide this process, few have created comprehensive, structured and fully documented decision-making processes. NSA may give decision-making power to individual staff, to managers, or collectively to teams. Some NSA review decisions formally by committee and/or informally in peer groups.

It is recommended that NSA:

- Adopt a structured approach to decision-making for enforcement that is common to all NSA. The approach should calculate the compliance gap and direct NSA towards a proportionate response.
- Be accountable for their decisions and demonstrate transparency by implementing and documenting an appropriate decision-making model. No specific model is recommended but it should enable each NSA to use a 'compliance gap' approach.
- Monitor delivery of audits to check they are in line with the planned programme.
- Develop and publish decision-making criteria.
- Request organograms or similar from each RU/IM Plan to help plan interviews with staff at all levels in an RU/IM when conducting an audit.

- Survey the market to understand how effective supervision is and how delivery could be improved.
- Consider if technology can facilitate supervision by, for example, enabling RUs/IMs to submit information and documents online.
- Consider if supervision methods can give RUs/IMs an opportunity to learn from the expertise of the NSA (e.g. by issuing guidance initially rather than enforcing). This is especially pertinent when managing the transition to an SMS-based approach.
- Implement an internal advice structure so that NSA staff can obtain senior guidance with ease.
- Include subcontractors in audits to estimate how effectively an RU/IM implements its SMS throughout its operations.
- Empower individual inspectors to make enforcement decisions.
- Manage resources in a way that matches staff expertise with the type of supervision activity. This should enable staff with a range of skills to be deployed so that no activities are neglected, whether they are high or low risk.
- Implement a whistle blowing policy to obtain honest feedback from the market.
- Consider multiple methods of sharing decision-making criteria and supervision strategies with the market.

Delivering enforcement

The fifth core NSA activity related to supervision is delivering enforcement. Enforcement can be delivered in a way that influences the behaviour of RUs and IMs, rather than just forcing their behaviour using the weight of the law. Delivering enforcement that influences behaviour is often related to good communication between NSA and the market. Whilst the majority of NSA reported that they were very transparent with the market, further examination indicated that this commitment often centred on an NSA's website. To develop their website communication further, it is recommended that NSA:

- Publish all key (non-sensitive) NSA documents, processes and procedures on the NSA website.
- Provide online links for RUs/IMs for relevant and useful information sources.
- Make resources and tools available for download (e.g. audit checklists).
- Feature information and guidance on key industry issues on their website.
- Publish news and current information about the sector.
- Adopt innovative website structures to catalogue information (e.g. according to themes) in order to assist users when searching.
- Providing foreign language translations of all or part of the website and its contents to facilitate users from other countries. Language differences can be a barrier to cross-border cooperation so NSA may wish to prioritise translation for languages of neighbouring Member States or those with which they share the most rail trade.
- Publish enforcement decisions and actions.

It is desirable for NSA to find additional ways of communicating with the market beyond using a website. It is recommended that NSA:

- Meet regularly with RUs/IMs outside of formal supervision activity (e.g. by hosting informal meetings for RUs/IMs to attend and openly discuss current issues).
- Assign specific staff to specific RUs/IMs as a primary liaison.
- Host and participate in conferences with stakeholders.
- Issue monthly incident reports to the market.
- Develop a strategy for communication.
- Collect feedback from the market (e.g. via survey) to identify the most effective methods of communication.
- Issue leaflets for when there is supervisory contact to remind RUs/IMs of their rights and obligations during the process.
- Update the industry on progress with the NSA strategy. This helps to maintain focus and momentum.
- Offer targeted in-depth guidance to RUs/IMs on key topics.

Such communication may help to influence market behaviour and thus reduce the requirement for strict enforcement using legal means. Nevertheless, there are occasions when NSA must enforce using legal means. It is therefore recommended that NSA:

- Use a standardised report form for all cases that may lead to enforcement action. This can improve consistency of decision-making and provide a clear record for accountability purposes.
- Report all enforcement action to the executive board of the affected RU/IM to ensure that remedial action filters through all levels of the organisation.
- Issue an enforcement policy statement to the market to explain the purpose of enforcement and what principles and procedures the NSA will follow.
- Specify applicable financial penalties and (at least internally) define the criteria for applying each financial penalty to ensure consistency.
- Ensure each of the enforcement measures available to the NSA are accessible so that the full range of powers/penalties can be applied as appropriate. Some NSA report a reluctance to use specific enforcement measures due to administrative complexity.
- Ensure that dialogue between the NSA and the affected RU/IM is a part of any enforcement activity to ensure that each party has an opportunity to explain its case and consider fully all of the evidence available.
- Review the existing range of enforcement measures.

The final recommendation—to review existing enforcement measures—is particularly important if NSA recognise that their current national regulatory framework does not provide a clear and consistent legal basis for enforcing the requirements of the European framework. An NSA without this is advised to form an internal working group with

relevant government ministries/organisations to address concerns with the enforcement measures that are available to the NSA.

NSA self-evaluation and continuous improvement

The final core activity of an NSA related to supervision is to evaluate its own processes so that it can continuously improve. Almost equal numbers of NSA reported improved supervision performance as reported no change. However, the evaluation methods used to enable NSA to rate their own performance varied considerably. From the evidence collected, it is recommended that NSA:

- Establish basic review procedures. Regular staff discussions, random peer reviews of cases, and structured annual case reviews are suggested as a minimum requirement. Reviews should be targeted, with measurable outcome criteria.
- Develop a culture of self-evaluation and improvement.
- Survey marketplace satisfaction with NSA supervision and enforcement. Survey staff at a range of levels within RUs/IMs and include RUs/IMs that have been subject to enforcement measures.
- Link evaluation data to strategic goals to present a coherent development cycle.
- Respond to market feedback on procedures by changing them if they are overly burdensome and ineffective. NSA may win or lose market support according to how responsive they are to valid market concerns.
- Monitor how NSA activity is presented in the media.
- Monitor usage of NSA guidance and tools that are provided online.

Summary

NSA have demonstrated reasonable maturity with regard to adopting supervision and enforcement practices from the current and forthcoming European safety regulatory framework. Across the network of NSA there are differences in the extent to which the regulations are being implemented and this study summarises such differences so that NSA can learn from each other and work towards greater consistency in the future.

The recommendations are issued to the European Railway Agency for implementation, either as recommendations to the NSA Network for further action or as the foundations for further work at a European level.

Contents

1 Introduction

1.1 Background

The European Union provides a focal point for the harmonisation of European railways and within it the European Railways Agency (ERA) has a specialised responsibility for regulatory activities in this sector. However, each Member State (as well as Norway) with a railway is required by Directive 2004/49/EC (the 'Safety Directive') to operate its own National Safety Authority (NSA). Each NSA is expected to be independent of railway undertakings (RUs) and infrastructure managers (IMs). NSA[1] also need a degree of independence from the Ministry of Transport of the Member State, although this does not have to be absolute.

This study examines how NSA supervise and enforce the rail market across Europe with a view to identifying good practice and supporting the process of harmonisation and opening up of the European rail market.

1.2 Safety certification and authorisation

The primary functions of each NSA are to oversee Member State railway operations and to issue safety certification for RUs and safety authorisations for IMs. Two types of RU safety certification are required currently:

- Part A – a 'European portable' certificate demonstrating that the NSA in the Member State in which the RU is based accepts the generic safety management system (SMS) components adopted by the applicant. This sets out the applicant's general safety management arrangements.
- Part B – a certificate demonstrating that the NSA in the member state in which the RU intends to operate accepts the provisions adopted by the RU to meet the requirements necessary for safe operation over the relevant network in that Member State.

Implicit in any application for a safety certificate/authorisation from an RU or an IM is the understanding that the certificate will be granted on the basis of having and maintaining a safety management system (SMS). The NSA should establish during the certification/authorisation process that the SMS conforms to the requirements of the European safety regulatory framework.

1.3 Common Safety Methods

The introduction of the Safety Directive in 2004 (Directive 2004/49/EC) highlighted different levels of compliance among Member States; some already had safety authorities whereas others were either in the process of establishing an NSA or were yet to do so. Member States with an existing safety authority had developed their own approaches to monitoring railway safety. To harmonise the rail market in response to this diversity in practice, the Agency began to develop Common Safety Methods (CSMs) on issues such as Conformity Assessment.

To deliver a CSM on Conformity Assessment, new regulations for safety certification and authorisation came into force on 3rd January 2011 (Commission Regulations EU

[1] 'NSA' is used throughout this report as both a singular and plural acronym (i.e. it refers to either a *single* national safety authority or *multiple* national safety authorities).

1158/2010 and 1169/2010 for RUs and IMs, respectively). An annex to each of these new regulations set high level supervision principles for NSA to follow.

A Common Safety Method on Supervision is forthcoming and will provide regulatory detail on the type of detailed arrangements expected of NSA to establish a supervision regime.

1.4 Supervision

The supervision regime of an NSA should enable it to oversee—on a continuous basis and in accordance with Article 4 of the Safety Directive—the level of compliance among RUs/IMs with the legal requirement to use an SMS. An intended purpose of both the principles of supervision and the forthcoming CSM on Supervision is to provide NSA in all Member States with greater confidence in the administration of Part A safety certificates (in particular, the assessment and continued supervision of the SMS). The CSM on Conformity Assessment has already established the hierarchical relationship between Part A and Part B certificates (Part A is hierarchically superior) and has set out detailed assessment criteria that must be applied. The Part B certificate should therefore be an assessment of how the generic SMS (established and approved for the Part A certificate) is applied to specific operational circumstances. NSA are not expected to reassess the Part A certificate when considering an application for a Part B certificate. However, the Agency is aware that this practice does sometimes occur, primarily because there is a lack of mutual trust between NSA. It is important that NSA develop trust in a uniform approach to conformity assessment and continued supervision. Mutual trust in this process is expected to deliver many benefits such as minimising bureaucracy, resource use and costs, and easing entry into many parts of the railway market.

A further reason for regulating a uniform approach to supervision regimes is associated with the Agency recommendation to migrate from the current two-part safety certification scheme to a single safety certificate by 31st December 2020. A single safety certificate would require RUs to assume complete responsibility for safe operation; to meet this requirement several NSA may need to relinquish some of their existing direct responsibilities for the safe operation of the railways in their Member State.

There remains also a need for improvements in supervision for essential safety reasons. This was highlighted by the Agency's own report following the collision between two passenger trains in Buizingen, Belgium on 15th February 2010 (SAF/VIS/10/BE/RE.01). The report into the activities of the Belgian NSA indicated that it was "not adequately performing the necessary supervisory activities". The report also suggested that further promotion, active monitoring and targeted enforcement was required to address the main risks within the railway system, as encouraged by the supervision principles in the latest EU Regulations.

1.5 Enforcement

One outcome of supervision is that NSA may identify non-compliances and safety hazards across RUs/IMs. Directive 2004/49/EC places a requirement on NSA to establish penalties that apply to infringements of the Safety Directive and any provisions that are adopted pursuant to it (Article 32). The penalties should be "effective, proportionate, non-discriminatory and dissuasive". Enforcement measures can exist on a spectrum: at one extreme, there can be strict measures to 'force' behaviour, using legal tools to achieve compliance (e.g. revocation of a safety certificate or authorisation; prohibiting

use of a vehicle); at the other extreme there can be persuasive measures to 'influence' behaviour without necessarily imposing the weight of law (e.g. verbal or written advice). Along the spectrum of enforcement there may be many ways of both forcing behaviour and influencing behaviour.

1.6 The principles of supervision

The principles of supervision, as adapted from Regulations 1158/2010 and 1169/2010, state that NSA shall:

- Apply the principle of **proportionality** between enforcement and risk. Action taken by a NSA to achieve compliance or bring RUs/IMs to account for not meeting their legal obligations shall be proportionate to any risks to safety or to the potential seriousness of any non-compliance, including any actual or potential harm.
- Apply the principle of **consistency** of approach to ensure that a NSA takes a similar approach in similar circumstances to achieve similar ends.
- Primarily **target** supervision at those activities which it believes give rise to the most serious risks or where the hazards are least well-controlled. To do so, the NSA shall have methods and power to assess the day-to-day performance of RUs/IMs.
- Decide on **priorities** to use their resources effectively but the decision on how best to do that should rest with each individual NSA. Action shall be focused on those who are responsible for the risk and who are best placed to control it.
- Apply the principle of **transparency** to help RUs/IMs understand what is expected of them (including what they should or should not do) and what they should expect from the NSA.
- Be **accountable** for their decisions in accordance with Article 17(3) of Directive 2004/49/EC. NSA shall therefore have policies and principles by which they can be assessed. Moreover, NSA shall also have a complaints procedure.
- Develop **cooperation** arrangements between each other in order to share information with each other and to coordinate their response to any breaches of safety. This is particularly important for Part B safety certificates. In addition, NSA shall develop cooperation arrangements with other competent authorities in order to share information and to develop unified approaches to issues that impinge on railway safety.

1.7 Objectives and scope of this work

This study explores how NSA have interpreted the principles of supervision set out in Regulations 1158/2010 and 1169/2010, and how they enforce the safety regulatory framework based on these principles. With this knowledge, it will be possible to identify examples of better practice and use these to guide NSA towards operating in a fair and effective manner that is consistent across all states that operate the railways of Europe.

Therefore the overall aims of this work are to establish the minimum benchmark level of supervision and enforcement activity undertaken by NSA (i.e. a baseline level of activity), map current activity against the relevant parts of the safety regulatory

framework, and provide better practice guidance to improve upon this. To achieve this aim, the project has the following specific objectives:

i. To explore the supervision and enforcement activity, responsibilities and powers of each NSA that is subject (either compulsorily or voluntarily) to EU regulation.

ii. To compare the supervision and enforcement activity, responsibilities and powers of NSA with those of Competent Authorities responsible for enforcement in other key industrial sectors across the EU.

iii. To develop good practice guidance for NSA enforcement activity.

1.8 Structure of this report

This report is structured as follows:

- Section 2 describes the study approach.
- Section 3 presents the study findings.
- Section 3.1 presents findings related to the structure and organisation of NSA, including staffing, strategies and polices.
- Section 3.2 describes further the practices for training staff and developing competencies for supervision and enforcement.
- Section 3.3 outlines different approaches to supervision strategies, including how they are targeted and how resources are prioritised to deliver such strategies.
- Section 3.4 outlines how supervision plans are developed, resourced and reviewed.
- Sections 3.5 and 3.6 document the range of supervision practices adopted by NSA, including audit methods and decision-making approaches.
- Section 3.7 discusses NSA transparency and communication with the market.
- Section 3.8 describes enforcement powers and penalties held by NSA, and methods of enforcement.
- Section 3.9 reports how proportionate and consistent NSA are.
- Section 3.10 discusses how NSA self-evaluate.
- Section 4 is a summary and discussion of the study findings.
- Appendix A presents the case study examples used for the NSA questionnaire.
- Appendix B presents detailed tables of findings referenced in the report.
- Appendix C presents a full list of all the recommendations made in this report.

2 Approach

This study comprised three main activities:

- An investigation of supervision and enforcement methods used by NSA (Task 1).
- An investigation of supervision and enforcement methods used by competent authorities in other industrial sectors (Task 2).
- A mapping exercise to bring together the findings from both investigations and map their fit with relevant parts of the European safety regulatory framework.

The methods used for these tasks are described in the following subsections.

2.1 Task 1: NSA survey

The first phase was to consult with the National Safety Authority (NSA) of each EU Member State, plus Norway which has adopted EU rail regulations. This consultation was questionnaire-based at first (Task 1.1) and then evolved into detailed discussions with a subsample of NSA (Task 1.2).

2.1.1 Task 1.1: NSA questionnaire

A questionnaire was developed to explore how each NSA undertakes supervision and enforcement. The questionnaire was designed using background information from the Agency, the knowledge of the core study team, an initial search of individual NSA websites, and the relevant parts of the European safety regulatory framework.

The questionnaire was divided into sections, with items on the following:

- Staff for supervision and enforcement, including training, team structures and competence management.
- Methods of supervision and enforcement, including frequency with which different methods were used.
- Supervision strategies, including information on how supervision is targeted and planned, and the resources required.
- Strategies and methods for communicating with the market.
- NSA legal powers and penalties.
- Examples of case studies used to test the proportionality and consistency of supervision/enforcement responses.
- Supervision principles (as described in the Annexes to Commission Regulation (EU) 1158/2010 and Commission Regulation (EU) 1169/2010) and the extent to which they were followed by respondents.
- Market awareness and size.

The majority of questions had multiple choice response options; 'closed questions' were created in preference to open response items as this would reduce the burden of responding.

The Agency provided feedback on a draft of the questionnaire and approved the final version for issue. This version was then hosted online and was piloted by the GB NSA. Minor revisions were made after piloting before the questionnaire was made available to the whole network of NSA.

The questionnaire was hosted online for five months during which time NSA were invited to respond. The questionnaire was launched at one of the plenary meetings of the NSA Network and the project team was on hand to explain the rationale behind the survey and demonstrate the online version as required. At the same time, the Agency issued an email invitation to all NSA with a link to the online questionnaire. This was followed by regular reminders by email and, in some cases, by telephone or in person.

The questionnaire was hosted in English but NSA were invited to request a translation if this was required. Two NSA requested that the questionnaire be translated. Responses were typically provided online although a small number of NSA opted to respond by email by marking an electronic copy of the questionnaire.

In addition, respondents were invited to email any documents (e.g. legislation, strategies) that supported their responses to the questionnaire.

Once issued, the questionnaire was not altered to ensure that the same questions were answered by each NSA. Data were collated automatically by the online questionnaire programme. Responses in a language other than English were translated back to English professionally. The final set of responses was compiled in an Excel database for analysis.

2.1.2 Task 1.2: NSA interviews

The questionnaire survey was followed by interviews with a subsample of 12 NSA. The follow-up discussions provided further understanding of the range of different approaches to supervision and enforcement adopted by NSA.

The subsample of NSA selected for interviews was agreed in consultation with the Agency. Selection was based on interviewing NSA that represented a range of responses to the online questionnaire, with particular attention given to the following criteria:

- Geographical situation, including the extent of cross-border rail traffic.
- Network size.
- The size of the NSA's supervision and enforcement team(s).
- An average of the self-ratings provided by NSA to multiple questions.

Interviewing a sample of NSA was intended to provide 'a complete and representative overview' of NSA activity and requirements. To structure the interviews around this goal, a topic guide was created and agreed with the Agency. This guide built on the issues discussed in the online questionnaire and sought further information, much of which would have been impractical to collect from a questionnaire. The range of topics covered included:

- Each of the principles of supervision, including how the principle had been interpreted and the methods used to meet the requirements.
- How each NSA had approached competence management for its staff.
- NSA legal powers and penalties, including satisfaction with the range available.

- NSA strategies and plans for supervision, including content, scope, development and evaluation.
- Methods of communication with the market and the market feedback on these.

The selected NSA were contacted by email to arrange a date and time for the interview that was convenient. Respondents were initially invited to take part by telephone although the option to have an interview in person was offered. Overall, four interviews were carried out in person with the NSA in the GB, Poland, Denmark, and the Czech Republic. In addition, NSA were offered the option of having direct translation if they were not comfortable participating in English. Two NSA (Poland and Bulgaria) took this option. All interviews were recorded digitally and transcribed in full.

2.2 Task 2: survey of competent authorities in other industrial sectors

The second task was to consult with other competent authorities (CAs) that perform a similar function to NSA but in different industrial sectors. This consultation comprised a desktop review followed by direct contact with a subsample of CAs.

2.2.1 Task 2.1: competent authority desktop review

The industrial sectors that have been recommended for further investigation are aviation, occupational health and safety, and petro-chemicals. Specifically:

- Aviation authorities: Each Member State has an aviation authority that is responsible for maintaining safety and regulatory compliance within the airline industry. The European focal point for these CAs is EASA.
- Occupational health and safety authorities: Within each EU Member State, there is a national organisation for the promotion and enforcement of health and safety in the workplace. The sector of occupational health and safety has a European focal point in the European Agency for Safety and Health at Work (EU-OSHA, which does not have any regulatory authority).
- Petro-chemical authorities: The regulations that apply to the petro-chemical industry are likely to depend on the activities in question; for example, there are several fields of operation from offshore exploration and extraction through to onshore storage and processing, as well as transportation. Major accidents in the petro-chemical industry have prompted the issuing of European Directives. In Europe, the Seveso accident in Italy in 1976 prompted the adoption of legislation aimed at the prevention and control of such accidents. The latest is Council Directive 96/82/EC, (the 'Seveso II Directive'), which was extended by Directive 2003/105/EC. It applies to thousands of industrial establishments where dangerous substances are present in quantities exceeding the thresholds in the directive. In the GB, this Directive has been adopted by national law as the Control of Major Accident Hazards Regulation (COMAH) 1999 and there is a COMAH Competent Authority responsible for the supervision, coordination and enforcement of the regulations. However, it consists of three existing government bodies covering the environment and health and safety. This structure appears to be followed in other EU Member States so our investigations into the petro-

chemical authorities began via occupational health and safety. The findings in this interim report do not yet include many CAs from this sector.

The desktop review focussed on exploring the website of each authority. The search was structured by a list of topics for which evidence was sought on each website. This list was agreed with the Agency in advance of this task and was similar in scope to the range of items captured by the NSA questionnaire.

The majority of websites were not in English. A website translation tool was used when searching sites not in English. Care was taken not to rely on the information in the official English language sections of some websites, as these often have less information than the native language version of the site.

Findings were reported in a table together with information on the relevance of each finding.

2.2.2 Task 2.2: competent authority interviews

The desktop review of competent authorities was followed by interviews with a subsample. Together with the Agency, a shortlist of authorities in the sectors of OHS and civil aviation were drawn up. Authorities were selected on the basis of demonstrating examples of good practice on their websites that could be explored in further detail during an interview. Each interview was semi-structured and guided by the same themes that were discussed in the NSA interviews (Task 2.2), with the exception of any direct references to the rail regulatory framework.

The selected CAs were contacted initially by email to invite them to participate in a telephone interview with the option of foreign language support. Four interviews were conducted; two with OHS authorities (GB and Denmark) and two with civil aviation authorities (GB and Latvia)[2]. All interviews were recorded digitally and transcribed in full.

2.3 Analysis

The online NSA questionnaire (Task 1.1) and interviews with NSA (Task 1.2) produced both quantitative and qualitative data to analyse. Where possible, responses were categorised and summary statistics provided. However, the majority of analysis was qualitative.

A thematic approach to qualitative analysis of the data sources has been used. The themes selected were based on the principles of supervision and the different core activities and attributes of an NSA related to supervision. For each theme, examples have been collated from different data sources and the relevance of each example has been considered (including the fit with the principles of supervision).

In addition, the project team and the client took part in an expert panel review of the desktop review findings (Task 2.1). This workshop discussed the sources of data and rated their fit with the principles, the regulatory framework and the goal of pinpointing good practice.

Task 3 collated and scored these examples of good practice according to whether the examples demonstrated poor practice, baseline good practice, further good practice or a high level of good practice. The scoring system is described at the start of section 3.

[2] A greater number of interviews were planned but it was unfortunate that the other authorities that were contacted did not have the resources available to respond in the timeframe provided.

3 Findings

The findings presented in this section are from the questionnaire survey of NSA (Task 1.1), the interviews with NSA (Task 1.2), the desktop review of competent authorities (Task 2.1)—including findings from the expert panel review—and the interviews with competent authorities (Tasks 2.2). Questionnaire findings are tabulated separately from findings that emerged from the interviews and desktop review.

Tables of results for questionnaire findings are colour-coded to assist with identifying common approaches, where appropriate (Figure 3.1). The colour-coding is based on a scale of poor practice through to good practice. Greyscale shading indicates no response or that insufficient data were provided. Not all tables of questionnaire findings are colour-coded as in some examples the information is descriptive and it is not appropriate to classify it as good or poor practice. In some tables, the NSA country itself may be colour-coded. This will be done when it is possible to make an overall assessment of an NSA's level of practice for a particular topic.

Good practice **Poor practice**

Figure 3.1: Colour-coded system of identifying good practice in tables of questionnaire findings (Task 1.1)

Interview extracts and findings from the desktop review and expert workshop are often presented together in a table. The source can be identified by:

- An 'I/D' column: if marked with 'I' the source was an interview; if marked 'D' the source was the desktop review.
- A column labelled 'sector' indicates whether it is a finding from the rail sector ('Rail'), occupational safety and health ('OSH') or aviation ('aviation').
- A column labelled 'MS' indicates which Member State provided the information. (For simplicity, Member States are identified by the international licence plate code used for motor vehicles.)

For each finding from the interviews or desktop review, a comment is provided in italics underneath to discuss the value of the finding, labelled 'our opinion'. This provides an explanation as to why the example was included and in what ways it is an example of good practice.

Each example is then followed by columns that indicate which of the principles of supervision are addressed and to what extent. Relevant columns will contain a number and be shaded according to the system presented in Table 3.1.

Table 3.1: Scoring and shading system for identifying good practice in tables of interview and desktop review findings (Tasks 1.2, 2.1 and 2.2)

Score and corresponding colour	Description
-1	Poor practice (works against the corresponding principle)
[Blank]	Not related to the corresponding principle
1	Baseline good practice (a fair example that satisfies the principle)
2	Further good practice (a good example that satisfies the principle)
3	Higher level good practice (an excellent example that satisfies the principle)

When summarising key findings in the text of this report, the same system of colour coding is also used to present different 'levels' of good practice, from baseline (orange) through to further good practice (yellow) through to higher level good practice (green). This will indicate how NSA are recommended to progress from a baseline to a higher level of good practice.

Findings are organised according to six core activities and attributes of an NSA that relate to supervision and enforcement (Figure 3.2).

Figure 3.2: The core activities and attributes of an NSA relating to supervision and enforcement

3.1 NSA structure and organisation

3.1.1 NSA market size and staffing structure

Responses to the questionnaire indicated that the number of staff responsible for supervision and enforcement at an individual NSA ranged from 3–170. The range indicates three staffing levels:

- Small (up to 10 staff) – 11 NSA fall into the small category (Czech Republic, Portugal, Denmark, Latvia, Lithuania, Sweden, Estonia, Spain, Norway, Finland and Ireland).
- Medium (11–100 staff) – seven NSA fall into the medium category (Poland, Channel Tunnel, Netherlands, Bulgaria, France, Italy and Hungary).
- Large (over 100 staff) – three NSA fall into the large category (Romania, Great Britain and Germany).

NSA were asked to specify the number of RUs and IMs that had been issued with a valid safety certificate or authorisation. Table 3.2 shows that, of the 22 NSA responding:

- Six (Spain, Latvia, Bulgaria, Portugal, the Channel Tunnel, Ireland) supervise 10 or fewer.
- Eleven (GB, Estonia, Lithuania, Denmark, Austria, Netherlands, Hungary, Norway, France, Finland and Italy) supervise between 10 and 60.
- Three (Romania, Poland and Czech Republic) supervise 60–100.
- Two (Sweden and Germany) supervise at least 100.

Data from the World Bank was also used to provide the number of route-km of railway in each of the responding Member States (as of 2010). Table 3.2 shows that, of the 22 NSA responding:

- Nine (Estonia, Lithuania, Latvia, Ireland, Denmark, Portugal, Netherlands, Bulgaria and Norway) oversaw less than 5,000 route-km each – a relatively small proportion of the European network.
- Five (Austria, Finland, Hungary, Czech Republic and Sweden) oversaw between 5,000 and 10,000 route-km each – a moderate proportion of the European network.
- Four (Romania, Spain, Italy and Poland) oversaw between 10,000 and 20,000 route-km each – a large proportion of the European network.
- Three (GB, France and Germany) oversaw more than 30,000 route-km each – a very large proportion of the European network.

Some relationships are evident between the number of staff an NSA has for supervision, the number of RUs and IMs it supervises, and the route-km it oversees (Table 3.3). For example, of the nine NSA that oversee a small number of route-km, a majority (seven) also have a small number of staff for supervision, and all supervise a small or medium number of RUs/IMs. However, there are some notable exceptions:

- Finland has a small number of staff to supervise a moderate number of RUs/IMs and a moderately-sized network.
- Sweden and the Czech Republic also have a small number of staff to supervise larger networks with a substantial number of RUs and IMs.
- Poland has a moderate number of staff to supervise a large number of RUs and IMs, operating on a large network.
- France has a moderate number of staff to supervise a moderate number of RUs/IMs operating across the second-largest network in Europe.

Some of these exceptions—for example Sweden—suggest that it is possible to supervise moderate–to–large parts of the European network with a small number of staff. However, it is not common and NSA that oversee the largest sections of the network also happen to have large staffing capacities.

Most NSA divide at least some of the staff for supervision into teams that are responsible for different supervision activities, except for Poland and Portugal. A summary of staffing provisions is provided in Table 3.2.

Table 3.2: NSA market size and staffing provisions

NSA	No. staff	No. of RUs/IMs with valid safety certs or authorisations?	No. route km (000s)*	Staff in teams?	Notes
Great Britain	106	40-60	31.47	Yes	
Sweden	9	RU 104 (37 safety certificate) IM 403 (4 in main network)	9.96	Yes	Full-time equivalents
Estonia	10	24	.79	Yes	2 teams
Lithuania	7	19	1.77	Some of them	Flexible teams formed around aims of individual inspections
Romania	103	60	13.62	Yes	
Germany	170	300	33.71	Yes	
Denmark	5	24	2.13	Yes	1 team
Spain	10	9 RUs and 2 IMs	15.32	Yes – although the tasks of supervision and assessment are carried out by a single	Approximate. Staff are responsible for supervision and enforcement, not

NSA	No. staff	No. of RUs/IMs with valid safety certs or authorisations?	No. route km (000s)*	Staff in teams?	Notes
				team that is not divided.	inspections. Staff now organised across two levels: 1) Audit and supervision of the SMS of RUs/IMs. Guides for supervision (audits) are currently under development. These functions will be realised directly by the NSA. 2) Functions of specific inspection (staff, rolling stock …), that are carried out with the collaboration of ADIF, the national infrastructure manager. Throughout the questionnaire it will be made reference to the system of supervision by means of the audit of the SMS.
Latvia	6	6	1.90	Yes	
Poland	16	65	19.7	No (Teams are established for the purpose of individual supervision activities. They consist of experts responsible for certification / authorization process and inspectors representing regional divisions carrying out inspections in line	Includes 2 that assess applications plus 2 from each of 7 regional departments. In addition, there are 62 staff involved in supervision under the old regime (not through SMS but through documentation,

NSA	No. staff	No. of RUs/IMs with valid safety certs or authorisations?	No. route km (000s)*	Staff in teams?	Notes
				with old approach on the daily basis. The information is shared mainly at the preparatory stage of an inspection.) Team size and number based on type of supervisory activity.	technical field inspections, etc). The old approach to supervision still plays a key role in our inspection regime, as most SMS have been certified very late, at the turn of 2010 and 2011. Due to this, inspection plans have been prepared on the basis of the old approach.
Bulgaria	23	10	4.10	Yes	
Austria	-	35	5.07	Yes	Supervision is not done by someone exclusively; it is a part-time task and so it is quite difficult to provide an exact figure. At the moment there are staff changes across the 2–3 divisions that are concerned with supervision.
Portugal	3	6	2.84	No	
Czech Republic	3	75	9.57	Yes	These 3 staff are trained to supervise using the SMS-based approach. The NSA has a further 100 staff approximately who supervise 'in connection with their profession'. The NSA stated, 'we supervise almost everything', which would suggest that responsibility for safety has not been

NSA	No. staff	No. of RUs/IMs with valid safety certs or authorisations?	No. route km (000s)*	Staff in teams?	Notes
					passed to RUs/IMs.
Netherlands	21	About 40	3.02	Yes	Relates only to staff who supervise and enforce – there are additional staff who carry out certification and reassessment.
Channel Tunnel	17	6	.058	Yes	8 from GB; 9 from France
Hungary	54	39	7.89	Some of them	7
Norway	4	16	4.11	Yes	-
Ireland	1.5	3	1.92	Yes	1.5 full-time equivalents (2 people)
France	50 (36 for supervision). 28 staff carry out checks.	25 (22 RU and 3 IM as of 29/11/11)	33.61	Yes - for supervision: the Department is organized into several areas (including operating, equipment, infrastructure, traction, signalling, environment and personnel). Teams are based on themes of control.	50 (36 belong to the department's Eve EPSF responsible for "supervision". 28 carry out checks. RU and IM are not the only ones affected by "supervision" performed by the EPSF (also training centres, etc). - Other people are particularly associated with the activity "Influencing behaviour".)
Finland	2	12	5.92	Some of them	-
Italy	40		18.01	Some of them	About 25 people are in a team

*Source: World Bank, 2010

Table 3.3: Relative size of staff, network and RUs/IMs for each NSA

	Relative size		
NSA	**No. staff**	**No. of RUs/IMs**	**No. route km**
Germany	Large	Extra Large	Extra Large
France	Medium	Medium	Extra Large
Great Britain	Large	Medium	Extra Large
Poland	Medium	Large	Large
Italy	Medium	Medium	Large
Spain	Small	Small	Large
Romania	Large	Large	Large
Sweden	Small	Extra Large	Medium
Czech Republic	Small	Medium	Medium
Hungary	Medium	Medium	Medium
Finland	Small	Medium	Medium
Austria	-	Medium	Medium
Norway	Small	Medium	Small
Bulgaria	Small	Small	Small
Netherlands	Small	Medium	Small
Lithuania	Small	Medium	Small
Estonia	Small	Medium	Small
Channel Tunnel	Small	Small	Small
Denmark	Small	Medium	Small
Portugal	Small	Small	Small
Ireland	Small	Small	Small
Latvia	Small	Small	Small

3.1.2 Staffing the activities of assessment and supervision

One of the activities performed by an NSA is the assessment of RUs/IMs who are applying for, or renewing, a safety certificate or authorisation. A second activity is the subsequent supervision and enforcement of the operations of these RUs/IMs. It is understood that effective supervision should receive inputs from the assessment process, and reassessments should receive inputs from previous supervision activities. The staff that carry out these activities could either be in the same team or they could be separated; how these staff are structured in teams may have a direct effect on the exchange of information between these two activities.

According to the questionnaire survey, six NSA (GB, Denmark, Spain, Latvia, Czech Republic, Hungary) have the same staff carrying out the activities of assessment and supervision (Table 3.4). This may present fewer potential problems in sharing information across the two tasks.

The remaining 16 NSA in the sample have either a partial division between staff who carry out these two activities (11 NSA) or a complete division of staff (5 NSA). Of these NSA:

- Most (ten) share all information across separate teams carrying out these tasks from each of the key stages in these tasks.
- Four share at least a little information. France has an electronic document management system for exchange of information. Of note, Poland shares little information from the initial award and during reassessment.
- Two (Netherlands and Finland) have neither the same staff carrying out assessment and supervision and nor do the separate teams share information from assessment tasks with those who are supervising and enforcing. Whilst this may encourage supervisory staff to make their own judgements and carry out their investigations independently and without influence, it may lead to situations where issues are highlighted at the award stage but not followed up effectively after the award is issued. The Dutch NSA has a medium level of staffing so could perhaps benefit from being able to target its supervision activities in line with findings from assessments and

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.3/4/7) and 1169/2010 (Annex III.3/4/7):

"3. NSA shall apply the principle of consistency of approach to ensure that a NSA takes a similar approach in similar circumstances to achieve similar ends.

4. NSA supervision activity shall be targeted primarily at those activities which a NSA believes give rise to the most serious risks or where the hazards are least well-controlled.

7. NSA shall be accountable for their decisions in accordance with Article 17(3) of Directive 2004/49/EC. NSA shall therefore have policies and principles by which they can be assessed."

CSM on Supervision (Article 5)

"1. The NSA shall use information gathered during the assessment of a RU/IM's safety management system prior to issuing the safety certificate or safety authorisation for its supervision of the continued application of their safety management system after issuing the safety certificate or safety authorisation.

2. The NSA shall also use information gathered during supervision activities in its assessment activity prior to the renewal of a safety certificate or safety authorisation, in order to establish the extent of the reassessment of a RU/IM's or infrastructure manager's safety management system."

reassessments. It should be noted that the Finnish NSA declared only two staff are employed for supervision and enforcement purposes and this may be a reason for the clear separation of activities.

Table 3.4: NSA staffing structures for assessment and supervision

NSA	Same staff doing assessment and supervision?	How much information is exchanged...		
		After an RU/IM is awarded a new safety certificate/ authorisation?	When supervising an RU/IM while it is operating?	When an RU/IM is being reassessed for a safety certificate/ authorisation?
Great Britain	Yes	-	-	-
Sweden	Partly	Much info	Much info	Much info
Estonia	Partly	All info	All info	All info
Lithuania	No	All info	All info	All info
Romania	No	All info	All info	All info
Germany	Partly	Some info	Some info	Some info
Denmark	Yes	-	-	-
Spain	Yes	-	-	-
Latvia	Yes	-	-	-
Poland	Partly	Little info	Much info	Little info
Bulgaria	Partly	All info	All info	All info
Austria	Partly	All info	All info	All info
Portugal	Partly	All info	All info	All info
Czech Republic	Yes	-	-	-
Netherlands	No	Little info	Little info	Little info
Channel Tunnel	Partly	All info	All info	All info
Hungary	Yes	-	-	-
Norway	No	All info	All info	All info
Ireland	Partly	Some info	Little info	Some info
France	Partly (Information the team needs is exchanged through a system of electronic document management	All info	All info	All info

NSA	Same staff doing assessment and supervision?	How much information is exchanged...		
		After an RU/IM is awarded a new safety certificate/ authorisation?	When supervising an RU/IM while it is operating?	When an RU/IM is being reassessed for a safety certificate/ authorisation?
	(EDM) available to interested persons)			
Finland	No	Little info	Little info	Little info
Italy	Partly	All info	All info	All info

Table B.1 presents a range of opinions from NSA regarding the different approaches to structuring the teams responsible for supervision and assessment. One of these approaches is to separate the staff who deal with assessment from those who conduct supervision. Evidence from NSA with direct experience of separating the tasks of supervision and assessment indicates that the drawbacks of this system are numerous and do not fit well with the principles of supervision. For example:

- The Dutch NSA described how 'too little' information was shared between the two tasks and how the information that was shared was done so selectively.
- The Swedish NSA used to separate the two tasks and discovered that it created market confusion when the NSA would identify non-conformities through supervision that were formally approved during the assessment process.

Although the Swedish NSA has since merged the activities of assessment and supervision, its current structure separates these activities according to whether the RU/IM is an RU or an IM. This has also created market confusion because the two departments have applied the assessment criteria differently; thus, an RU/IM that is both an RU and an IM may find that the same SMS is approved for its IM activities but has non-conformities for its RU activities (due to the NSA having an entirely different application of the assessment criteria).

A second approach is to partly share the two activities of assessment and supervision. As shown in Table 3.4, the majority of NSA reported operating a mixed structure where staff may be responsible for both tasks but still retain some separation. A priority for any NSA that opts for a degree of separation between these two activities is to ensure there is a two-way communication process. For example, the Spanish and French NSA open documentation for all staff to view. The French have an electronic document management system that retains copies of all audit and inspection findings and other information relevant to an individual RU/IM. It means that assessment staff can view previous supervision activity when considering a renewal, and supervision staff can review findings from the assessment audit to guide supervision.

Another consideration may be the consistency of the approach used. The Austrian NSA described its ability to use a mixed approach where sometimes the auditor/inspector will have a good knowledge of the RU/IM and sometimes they will not. If the level of prior

experience is to vary, it may be good practice to ensure that for each specific case, there is a baseline of at least one person with good knowledge of the RU/IM, which is a requirement that the German NSA applies.

Several NSA highlighted that the division of labour between assessment and supervision was often unequal and it was therefore not an efficient use of resources to have a team specifically assigned to assessment when (re)assessments could be infrequent. This was irrespective of the market size. For example, the Portuguese NSA, which supervises a relatively small market, commented that it would be inefficient to separate the staff for assessment because there would not be enough work to sustain their employment. At the other end of the market, the GB NSA, which oversees a large market, commented that if the teams were separated, there would be 'people sat doing nothing for long periods of time'. The German NSA also prefers to mix its staff because the majority can be engaged with supervision activities for the majority of the time and then assessment teams can be assembled as required from the pool of supervision staff. In times of economic restraint, these are strong arguments in favour of a mixed approach.

A third approach is to have the same staff responsible for supervision and enforcement. If an NSA opts for no separation between the teams who carry out these activities, there is a potential risk of introducing bias into the process of supervision and/or assessment. This bias may be in the form of regulatory capture, where the relationship between the NSA and the RU/IM becomes so close as to compromise the NSA's function[3]. All NSA would be encouraged to establish procedures to guard against this possibility, but especially those NSA without some structural separation between the assessment activities. For certification, an example can be drawn from the Danish NSA; each case is put before a certification committee that consists of senior staff and peers that have had no direct involvement in that particular assessment. It is reported that this ensures quality and independence. A second approach to guard against bias is to have in place a clear process for targeting supervision activity and making enforcement decisions. Together these approaches are expected to allow the benefits of a continuous line from certification/authorisation to supervision without realising the disbenefits of this structure.

When these findings were presented to the NSA Taskforce on Supervision, the recommended baseline good practice measures were:

- Good internal communication should exist between assessment and supervision, regardless of the NSA structure.
- Decisions during assessment or supervision should be peer reviewed or assessed via some independent process, regardless of the NSA structure.

[3] The process of regulatory capture can be subtle; for example, if an NSA inspector is responsible for assessing, supervising and then reassessing an RU/IM, they may find themselves making assumptions about the processes that the RU/IM has in place based on their considerable knowledge of the organisation. These assumptions can be misplaced because the inspector feels they 'know' the RU/IM in detail. The process therefore requires some independence and objectivity to guard against this problem. This does not have to be in the form of separating staff into different teams to force decisions to be made by different people – it is possible to implement a review process instead.

These baseline measures may be supplemented by further guidance to:

- Be consistent with the staff selection and level of prior knowledge required for assessment and supervision tasks. This is especially pertinent for NSA that loosely define the structural division of staff for these activities.
- Avoid generating market confusion by allowing fundamentally different decision-making processes to emerge as a result of staffing divisions within the NSA.

NSA that wish to operate according to further good practice are recommended to:

- Facilitate good communication between assessment and supervision (and across any other staffing divisions) by implementing a system for storing and exchanging information and documents related to each RU/IM.
- Follow a structured approach to supervision so that targeted activity is not directed solely by findings from assessment/reassessment (see Sections 3.3 and 3.4 on planning supervision).
- Follow a structured decision-making process (see Section 3.6.2 and 3.6.3 on decision-making).

In summary, the examples provided in Table B.1 provide evidence that supports an NSA structure with few divisions (if any) between the activities of assessment and supervision. Where divisions exist (whether they are formal or informal) there appears to be value in developing methods of communication to bridge the divisions. It seems that effective communication is rooted in the exchange of both dialogue and documents. Independent oversight of the assessment and supervision process reduces the risk that bias will emerge if the activities are not separated. Following this guidance is expected to help NSA operate according to the principles of proportionality, consistency, transparency and accountability.

Key findings:

- NSA resources vary considerably, from 3–170 staff in the surveyed sample
- Most NSA have a partial division of staff for the functions of assessment and supervision.
- Separating assessment and supervision functions can restrict information exchange and may lead to inconsistencies.
- To reduce bias when not fully separating assessment and supervision, NSA have peer reviews and independent panels.

Good practice recommendations:

- Good internal communication between assessment and supervision functions. This can be assisted with systems for document management and exchange.
- Independent or peer review of NSA assessment/supervision decisions.
- Ensure supervision and assessment activities work from a consistent knowledge base.
- Ensure supervision is targeted in conjunction with a national strategy.
- Ensure decision-making is directed by an NSA-wide policy.

3.1.3 General safety authority structures

From the review of other industrial sectors and rail (Table B.2) it is evident that how a safety authority is structured may affect the consistency with which it operates and its ability to target and prioritise resources for supervision. The structure and remit of a safety authority can have negative influences:

- Division of policy-making decisions can alter the strategic focus of the supervision team with undesirable results (e.g. the Dutch NSA).
- Limits to the jurisdiction of safety authorities can lead to situations where RUs/IMs are subject to enforcement by different authorities for similar activities, without any coordination between the authorities.
- The range of activities assigned to a safety authority may affect where and when resources are required, and the availability of such resources for supervision activities (e.g. the Polish NSA).

Some baseline recommendations for NSA that wish to follow good practice would be to:

- Cooperate with other government safety authorities. The NSA remit may not include all rail-related activities, such as the construction of infrastructure when there is no mainline traffic (e.g. the Danish NSA), or health and safety issues; however, it is beneficial to the market if different government safety authorities show consistency across supervision and enforcement practices, and decision-making.
- Consult with the budget-holder for the NSA if too many activities are assigned to the NSA for the resources it has available. The purpose of an NSA is defined in the Safety Directive (Article 16.2); it is not desirable for resources to be diverted from these tasks for purposes that do not appear in the Safety Directive.

Some additional recommendations that may assist NSA with harmonising various activities and departments are to:

- Produce an organogram that makes it clear how the organisation is constructed (e.g. Irish aviation authority). Making the structure of the authority public may help to explain any differences that the market may experience when dealing with different departments (although such differences should still be addressed internally).
- Oversee NSA activities by a single committee (e.g. Belgian aviation authority). The committee comprises senior staff from each separate division to represent the different activities strategically. This approach may benefit NSA that do divide their activities by department (the Dutch NSA is introducing this type of strategic level communication between departments).

3.1.4 Sub-contracting

Article 16.3 of the Safety Directive is explicit that an NSA may not subcontract its tasks to an IM, RU or procurement entity. Table B.3 shows that Spain sub-contracts some supervision and enforcement activities to ADIF, the national IM. In support of the practice, the NSA describes how its main IM has the experience to carry out these inspections, as well as the available staff. Although the IM has 'autonomy', the NSA retains control over enforcement decisions related to these `inspections. However, a concern about this approach is that it may divide some of the NSA's supervision activities and leave parts of the market open to self-supervision.

Ireland sub-contracts the "undertaking of SMS (Safety Management Systems) audit [to] suitably qualified consultants". Although not described as 'subcontracting', the Austrian NSA also followed this practice. This is the process of using an accredited body to certify the SMS of an RU/IM, which is discussed in section 3.6.1

3.1.5 Strategies, policies and principles

Table B.4 provides examples of strategies from safety authorities in other industrial sectors. Collectively, the evidence from these authorities establishes a number of items that are potentially good practice. According to this evidence, strategies should:

- Be published online at the very least.
- Outline supervision and enforcement policy. This should include methods of engaging with the market and the decision-making policies, with the latter having inputs and decision points for the RU/IM as well as the safety authority. The latter appears clearest when defined in a diagram (e.g. flow diagrams used by the Irish aviation authority).
- Outline a range of goals (both short- and long-term) with a strategy for measuring and achieving them. Strategies may target change over a period of several years.
- Organise goals in accordance with a common theme throughout the strategy, such as the 'significant seven' safety concerns in the strategy of the GB aviation authority. The thematic approach used by this authority permeates all its activities and aims to be a memorable focus for the market.
- Consider other methods of dissemination such as posters, presentations, leaflets and videos. The strategy should consider how to target staff at all levels across the market and not simply those at each RU/IM who have explicit safety responsibilities.
- Establish measurable service standards and set the NSA goals for delivering a certain level of service. NSA should be mindful that they are also there to serve the market by providing services such as assessments and the principle of transparency requires that NSA are clear about what the market can expect of them.
- Describe the principles that will be followed by the authority. Some authorities have shown further commitment to such principles by adopting separate codes of practice (e.g. the GB aviation authority). It is desirable if the principles expand on how the NSA has

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV. 4/6/7) and 1169/2010 (Annex III.4/6/7):

"4. NSA supervision activity shall be targeted primarily at those activities which a NSA believes give rise to the most serious risks or where the hazards are least well-controlled.

6. NSA shall apply the principle of transparency to help RUs/IMs understand what is expected of them (including what they should or should not do) and what they should expect from the NSA.

7. NSA shall be accountable for their decisions in accordance with Article 17(3) of Directive 2004/49/EC. NSA shall therefore have policies and principles by which they can be assessed."

Draft CSM on Supervision (Article 3)

"1. To give effect to this approach, the NSA shall develop a supervision strategy outlining how it targets its activities and sets its priorities for supervision. The NSA shall also have in place a supervision plan or plans as part of meeting the requirements of realising the approach.

2. The NSA shall collect and analyse information from a variety of sources. It shall use the information collected and the outcomes of supervision for the purposes set out in Article 1 of this Regulation."

interpreted the regulated principles of supervision, and indicate how these will be delivered.

- Develop separate 'action plans' that describe precisely the method of delivering the strategy over the coming year (e.g. the Irish aviation authority). Such actions plans can be renewed several times in the lifetime of a (longer-term) strategy.
- Adopt an inclusive approach where RUs/IMs are engaged positively with the strategy and have a clear role to play. The GB OSH authority follows this practice not only in its strategy (entitled 'Be part of the solution') but also with its service pledge that is hosted online and encourages RUs/IMs to sign up to a commitment, which is then publicised.
- Outline organisational structures that will work to deliver the strategy. Examples include committees of experts/working groups tasked with identifying ways of delivering improvements and joint authority-industry working groups.

Table B.5 provides examples of strategies from NSA. The GB NSA is currently working with a five-year strategy and it is following the example of the GB OSH authority by making it a 'consulted document'. Industry is further engaged with the strategy by the Rail Management Maturity Model, a system established by the NSA to monitor and report on the continuous development of each dutyholder[4] in the market.

The Danish NSA can be recommended for adopting a strategy that has a clear structure and guides RUs/IMs through the processes of the NSA, from goal setting through to supervision and evaluation. Clear links are made with each of the regulated supervision principles.

The Austrian NSA is an example of an authority that is yet to launch its strategy but is already considering a long-term approach from the outset, of 4–5 years, accompanied by more frequent delivery plans. Table B.6 provides examples of the various inputs to strategies. The principles of supervision require that supervision activity is targeted and prioritised. The development of strategic plans may be informed by a few key sources of information:

- Top-down and bottom-up inputs feature in the strategies of several NSA. It appears more common for strategies to be developed based on high-level incident data; however, several NSA collate the experiences of frontline inspectors to identify emerging concerns that have not appeared in the data but are perhaps worthy of some supervision in the coming period (e.g. the GB NSA, the Dutch NSA).
- Input from industry consultation can be large-scale (e.g. the GB OSH authority) or it can be targeted discussions with RUs/IMs (e.g. the Austrian NSA).
- Regulatory influence is a factor in determining how and when a strategy is developed. The Austrian and Polish NSA are examples of authorities that are awaiting the forthcoming CSM on Supervision before committing to a strategy.
- NSA may look to European regulations and guidance to support strategic plans, particularly when it comes to resource allocation. The Polish NSA would like further direction on this so it can put forward a case to its Ministry to fund adequate resources for a new strategy.

[4] 'Dutyholder(s)' is a term used to define organisation(s) that have been permitted to participate in the market in accordance with the regulatory framework for their industry. In the rail market, dutyholders are RUs and IMs.

Table B.7 describes NSA that do not have strategies. For some NSA, there is a need to develop first the procedures that will form the strategy. The Spanish and Czech NSA are examples of authorities that have yet to do this. In the case of the Spanish NSA, the focus will be to develop a strategy that assists the sector in adhering to the SMS-based approach. It is evident that the Spanish NSA is aiming to increase its supervision in line with the European approach. The Czech NSA has a different focus and is aiming for a strategy to deliver reassessments of safety certificates in the near future; resourcing this task is its priority and supervision of the SMSs of RUs/IMs is a later strategy goal. Its strategy approach is very short-term. The Bulgarian NSA is another authority without a formal strategy; however, it believes it can create a strategy document from its existing procedures which are documented and disseminated.

In summary, strategies provide vital direction for safety authorities and for the market. Supervision in accordance with the regulatory principles must be targeted, prioritised and transparent—a strategy that follows good practice can fulfil these principles. It can also set out the supervision and enforcement approach taken by the authority. Including items such as the decision-making strategy can satisfy further principles by demonstrating consistency, proportionality and accountability. To summarise baseline good practice, NSA are recommended to develop a strategy that is:

- Published online.
- Covers at least an annual period.
- Outline strategic goals and the policies and procedures that will be used to deliver them.

For NSA to develop a strategy that exceeds baseline good practice, it is recommended to:

- Consider a longer-term strategy (covering multiple years).
- Ensure the strategy is informed by top-down and bottom-up data inputs.
- Adopt more innovative approaches to presentation and dissemination of the strategy (e.g. organise strategic goals thematically, use different media for dissemination).
- Incorporate the regulated principles of supervision.
- Develop action plans to realise the strategy.
- Commit to and set measurable standards for the service that the NSA provides to the market.

An even higher level of good practice would encourage NSA to:

- Include stakeholders in strategy development and reflect this in the final document.
- Implement organisational structures and resources to ensure that the strategy is delivered.

3.1.6 Regulatory frameworks

Article 16.2(f) of the Safety Directive states that NSA should at least be responsible for "developing the safety regulatory framework including the system of national safety rules". The existence of national safety rules alongside the European safety regulatory framework should be considered "as a transitional stage, leading ultimately to a situation in which European rules will apply". Several examples of incompatibility and inconsistency between national and European regulations were reported during this study.

As described by the GB OSH authority, it is desirable if it is a statutory function of the authority to propose or update national laws and standards. Otherwise there can be incompatibilities between national legislation and the European framework. Several examples are provided in Table B.8. Specifically:

- Enforcement of European regulations may be limited in a Member State that does not have a legal structure to enforce all items in the regulations (e.g. the Dutch NSA). Although regulations apply directly, there are benefits to incorporating parts of the regulations—such as the principles of supervision—into national legislation (e.g. the Bulgarian NSA).
- Poor transposition of directives can undermine essential parts of the regulatory framework, as described by the Czech and Polish NSA.
- Conflicts may exist between national and European legislation. This can create market confusion, as described by the Polish NSA.

Where there is a need for transition from national to European regulatory frameworks, different routes to achieving compliance should be explored. The Polish NSA has encountered difficulties with updating its national regulatory framework and, as a result, the market has not had regulatory direction towards the appropriate SMS-based approach. To counter this issue, RUs are engaging with academic organisations that can provide assistance with SMS development and management in accordance with the European framework. This has received the full support and cooperation of the NSA.

Applicable safety regulatory framework:

Directive 2004/49/EC (Article 16.2(f))

"Monitoring, promoting, and, where appropriate, enforcing and developing the safety regulatory framework including the system of national safety rules"

CSM on Supervision (Annex 3)

"(c) contribute its views and any proposals to the Member State to overcome any deficiencies in the safety regulatory framework when necessary."

Key findings:

- Some NSA have national legislation that is incompatible with European legislation.
- Conflicts between national and European legislation can create market confusion.

Good practice recommendations:

- NSA to be given statutory function to propose/update national laws/standards.
- NSA legal structure to permit enforcement of all relevant EU legislation.
- NSA to incorporate relevant EU legislation within national framework.

Baseline recommendations for NSA are proposed:

- NSA to have a statutory function to update or propose national laws and standards.
- NSA to have a legal structure that enables them to enforce all of the relevant items within the European safety regulatory framework.

NSA that wish to develop their regulatory frameworks beyond a baseline level are advised to:

- Incorporate parts of the European safety regulatory framework into national legislation to avoid any doubt regarding what items should apply to the market.

3.1.7 Complaints policies and procedures

Of those NSA responding to the questionnaire, four (Spain, Portugal, Italy and the Channel Tunnel) were without a complaints procedure for RUs and IMs to follow (Table 3.5). Of those NSA with a complaints procedure, it was most common to inform RUs/IMs by letter/email or via the NSA's website. Several NSA also provided information about their complaints procedures alongside any written decisions or audit reports that were issued to RUs/IMs. This requirement was often written into national law. All NSA did not issue such information in any leaflets and nor was it discussed during workshops. However, almost all NSA believed that the RUs and IMs that they supervised were aware of the complaints procedure; only the Portuguese NSA stated that its RUs/IMs were not informed.

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.6) and 1169/2010 (Annex III.6):

"7… Moreover, national safety authorities shall also have a complaints procedure."

CSM on Supervision (Article 7)

"2. The national safety authority shall also have and publish a procedure to enable railway undertakings and infrastructure managers to complain about decisions taken during supervision activities, without prejudice to the requirement for a judicial review of those decisions."

Table 3.5: How NSA publicise their complaints procedures

NSA	Methods used to notify RUs/IMs of the complaints procedure					
	Complaints procedure?	Direct email/ letter	Website	In person	Other	Specify
Great Britain	Yes	Yes	Yes	Yes	No	-
Sweden	Yes	Yes	Yes	Yes	No	-
Estonia	Yes	Yes	Yes	Yes	No	-
Lithuania	Yes	Yes	Yes	No	Yes	Procedure to follow is described in the legal acts that are officially published.
Romania	Yes	Yes	No	No	No	-
Germany	Yes	Yes	No	No	Yes	Each decision issued in writing contains information on legal remedy. The general procedure is established by law.
Denmark	Yes	No	Yes	No	No	Informed when decisions have been made
Spain	No	Yes	No	Yes	No	Not done yet. It is under development.
Latvia	Yes	Yes	Yes	Yes	No	-
Poland	Yes	No	No	No	Yes	Every decision issued by the NSA has to contain relevant information on a complaint procedure and the law basis for the decision. This is a requirement set in Polish law and it applies also to all other public authorities.
Bulgaria	Yes	Yes	Yes	No	No	-
Austria	Yes	Yes	No	No	Yes	Laid down in law (Allgemeines Verwaltungsverfahrensgesetz 1991), also included in the written decisions of the authority.
Portugal	No	No	No	No	No	-
Czech Republic	Yes	No	No	No	Yes	National legislation and in the report of the audit.
Netherlands	Yes	Yes	No	No	No	
Channel Tunnel	No					

NSA	Methods used to notify RUs/IMs of the complaints procedure					
	Complaints procedure?	Direct email/ letter	Website	In person	Other	Specify
Hungary	Yes	Yes	No	No	No	-
Norway	Yes	Yes	Yes	Yes	Yes	-
Ireland	Yes	No	Yes	No	No	In person: i.e. to RM & IM at supervision meeting
France	Yes	No	Yes	No	-	French regulations control the ESPF; the 'regulator', ARAF (Regulatory Authority Activities Railway), can take the case of anyone who believes that unfair treatment, discrimination or other practices of the EPSF has the effect of unreasonably restricting access to its rail network. During supervision activities, the EPSF has a procedure that allows RUs/IMs to put their case forward before a decision is made to restrict, suspend, or withdraw an authorization. The draft reports made during inspections are routinely subjected to comments and observations from controlled entities. This is the subject of a procedure available on the website of the EPSF.
Finland	Yes	No	No	No	No	
Italy	No	-	-	-	-	

RUs and IMs can complain to all NSA by letter and (with the exception of Poland, Austria, the Czech Republic, Hungary, Italy and Norway) by email (Table 3.6). Complaints by telephone and in person were less commonly accepted and it was rare for NSA to have a website form to complain. The method used may depend on the type of complaint: for example, a formal complaint against an NSA decision may need to be made in writing.

The majority of NSA had received no complaints in the last 12 months. Seven NSA (GB, Sweden, Germany, Denmark, Latvia, Netherlands, Ireland and Italy) had received at least one, although numbers were generally not high. The exception was Germany (50 complaints) although this has to be considered in the context of it supervising 300 RUs/IMs.

Spain did not report any complaints as it has not yet carried out any supervision or enforcement activities that could give rise to a complaint.

Table 3.6: Methods of complaining to NSA

NSA	Via website form	By email	By letter	By phone	In person	Other	Specify	Number of complaints in last 12 months
Great Britain	No	Yes	Yes	Yes	Yes	No	-	0-10
Sweden	No	Yes	Yes	No	No	No	-	2
Estonia	Yes	Yes	Yes	Yes	Yes	No	-	0
Lithuania	No	Yes	Yes	No	No	No	-	0
Romania	No	Yes	Yes	Yes	Yes	No	-	0
Germany	No	Yes	Yes	Yes	Yes	Yes	Complaints may be made in any form. Formal objections to NSA decisions have to be written or verbal.	50
Denmark	No	Yes	Yes	Yes	Yes	No	-	1
Spain	No	Yes	Yes	Yes	Yes	No	-	We have received no complaints because we do not carry out supervision or enforcement activities. (This is under development)
Latvia	Yes	Yes	Yes	Yes	Yes	No	-	4
Poland	No	No	Yes	No	No	No	The interested entity has to submit formal complaint within the time specified in the decision that is the subject of the	0

NSA	Via website form	By email	By letter	By phone	In person	Other	Specify	Number of complaints in last 12 months
							complaint.	
Bulgaria	No	Yes	Yes	Yes	Yes	No	-	0
Austria	No	No	Yes	No	No	No	-	0
Portugal	No	Yes	Yes	Yes	Yes	No	-	0
Czech Republic	No	No	Yes	No	No	No	-	0
Netherlands	Yes	Yes	Yes	Yes	Yes	No		A few
Channel Tunnel	No	Yes	Yes	Yes	Yes	No		0
Hungary	No	No	Yes	No	No	No	-	0
Norway	No	No	Yes	No	No	No	-	0
Ireland	No	Yes	Yes	No	Yes	No	-	1
France	Yes	Yes	Yes	Yes	Yes	No		0
Finland	No	Yes	Yes	No	No	No		0
Italy	No	No	Yes	No	No	No		2 complaints from RU since 2008 not agreeing with the results of an audit; in one of these case, the RU wrote to the Ministry too, in the other one the RU wrote to the NSA only.

Table B.9 provides further examples of complaints procedures from the desktop study and NSA interviews. Some authorities are explicit with their complaints procedure, providing information and details online and in printed material distributed to dutyholders during regulatory contact (e.g. the GB and Irish OSH authorities, the Irish aviation authority). NSA may also wish to establish direct methods of contact for the market and any other stakeholders, such as the complaints telephone line provided by the Bulgarian NSA, which is also open to the public and could provide a supplementary source of safety-related information.

In summary, baseline good practice for complaints procedures would be to:

- Document the complaints procedure on the NSA website.
- Provide details of complaints procedures during any regulatory contact and especially with any enforcement action.
- Consider how complaints will be dealt with initially and how grievances will be escalated internally. An independent review process is advised (although in this context 'independent' can still mean within the NSA but not linked to the specific case). The process of judicial review through the courts should remain available.

Key findings:

- Majority of NSA have a complaints procedure but dissemination of this is inconsistent.
- Complaints are relatively rare.

Good practice recommendations:

- NSA should provide details of complaints procedures online and during enforcement activities.
- Internal management and escalation of complaints should be formalised.
- NSA should ensure complaints procedures are accessible.
- NSA should advocate a right to respond for RUs/IMs subject to enforcement.

NSA that wish to adopt further good practice could:

- Facilitate access to the complaints procedure with online forms and accessible contact information.
- Attempt to resolve complaints early in the process by providing RUs/IMs an opportunity to feedback on any enforcement decisions before they are formalised.

A piecemeal approach to adopting the principles of supervision (e.g. the Spanish NSA) is not recommended. All the principles of supervision should be adopted to a certain extent to ensure that the correct approach is built in to the supervisory operations of the NSA from the outset. It may be more difficult to adjust procedures once ways of working have already been established.

3.1.8 Cooperation

The European safety regulatory framework requires NSA to develop cooperation arrangements. The framework specifies that such cooperation is particularly important when RUs choose to operate across borders and are subject to certification and supervision by more than one NSA. Such cooperation can help to build trust between NSA, which may initially develop along the axes of need (i.e. routes where RUs are operating across borders) and is expected to develop more widely to encompass all NSA and other rail and even non-rail competent bodies.

Table 3.7 shows that 14 of the 22 NSA responding to the questionnaire have arranged to cooperate with other NSA by sharing information and coordinating their responses to breaches of safety. Not having cooperation arrangements was not necessarily a barrier to sharing information; of the eight that did not have such arrangements, four (Spain, Bulgaria, Portugal, Netherlands) all sent safety-related information to and received it from other NSA in the last 12 months. The Irish, Finnish and GB NSA had received such information in the last 12 months and only Romania had neither sent nor received such information over the past year.

Of the 14 NSA with arrangements to cooperate with other NSA, ten (Sweden, Germany, Latvia, Austria, the Czech Republic, the Channel Tunnel, Hungary, Norway, Italy and France) all exchanged information in both directions during the last year. The remaining NSA had all either sent or received such information in the last year with the exception of those in Lithuania and Denmark.

These findings indicate a reasonable flow of safety-related information between NSA irrespective of whether specific arrangements are in place to share such information. The range of information that has been shared is broad, and includes:

- Incidents related to maintenance failures.
- Decisions to award Part B safety certificates and information regarding related assessments.
- Vehicle information (e.g. safety-related rolling stock failures).

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.8) and 1169/2010 (Annex III.8):

"NSA shall develop cooperation arrangements between each other in order to share information with each other and to coordinate their response to any breaches of safety. This is particularly important for Part B safety certificates. In addition, NSA shall develop cooperation arrangements with other competent authorities in order to share information and to develop unified approaches to issues that impinge on railway safety."

CSM on Supervision (Article 8)

"1. NSA involved in supervision of a RU operating in more than one Member State shall coordinate their approaches to supervision to secure that the SMS of the RU is effective and covers all relevant activities. Such co-ordination activity shall involve agreement on what information to share between NSA in order to ensure a common approach to supervision of the relevant RU. Such activity shall include sharing information on their supervision strategy and plan or plans, including any relevant outcomes, to enable a joint approach to dealing with non-compliances.

2. NSA shall also develop co-operation arrangements with NIBs, certification bodies for ECMs and other competent authorities in order to share information and to coordinate their response to any non-compliance with the safety regulatory framework."

- Information about forthcoming audit activities.
- Information about supervision activities (e.g. reports).

Where appropriate, NSA appear to circulate this information to the RUs and IMs that they supervise. It also guides in part their supervision activities.

Table 3.7: Cooperation between NSA

NSA	Cooperate?	SENT info	No. times	What was sent?	RECEIVED info	No. times	What was received	How was info used?
Great Britain	No	No	-	-	Yes	1	Details of significant incident regarding Italian LPG tanker and failures in maintenance.	Influence behaviour of RU.
Sweden	Yes	Yes	2-5 times	Letters and decisions from supervision part B. Information about assessment of application part B.	Yes	2-5 times	Letters and decisions from supervision part B. Letter of coming activities/ audits Different decisions	Information and discussion about revised supervision plans Action put in place Risk-based supervision Information for coming audits
Estonia	Yes	No	-	-	Yes	2	Information was relevant with rolling-stock	Unfortunately the information was no good, because we don't have such kind of rolling-stocks
Lithuania	Yes	No	-	-	No	-	-	-
Romania	No	No	-	-	No	-	-	-
Germany	Yes	Yes	5	Mostly information on safety-critical failures of rolling stock (also distributed via	Yes	5	Again, mostly information on safety-related failures of rolling stock.	Own investigations and inspections, discussions with RUs / Keepers.

NSA	Cooperate?	SENT info	No. times	What was sent?	RECEIVED info	No. times	What was received	How was info used?
				ERA SIS).				
Denmark	Yes	No	-	-	No	-	-	-
Spain	No	Yes	1	A safety alert was sent to the ERA Safety Information System related to a combined failure of bearing and temperature sensor of a engine.	Yes	5	Safety alerts from the ERA Safety Information System.	Distribution of the safety alerts to the sector.
Latvia	Yes	Yes	4	About safety certificates, about putting into service of RS, about maintenance of rolling stock	Yes	5	About safety certificates, about putting into service of RS, about maintenance of rolling stock	Develop supervision actions.
Poland	Yes	No	-	-	Yes	3	Information on draft reports from two derailments of freight wagon in Austria, safety alert from German NSA on the possibility of wheel axle cracks in TRAXX locos. All of information shared with use of SIS application.	The NSA distributed the information on risks to relevant identified stakeholders. The NSA also issues recommendations to the concerned companies and obliges them to send feedback information regarding the fulfilment of the recommendations.
Bulgaria	No	Yes	0	-	Yes	0	-	-

NSA	Cooperate?	SENT info	No. times	What was sent?	RECEIVED info	No. times	What was received	How was info used?
Austria	Yes	Yes	-	-	Yes	5	Concerning wagons	-
Portugal	No	Yes	3	Information related with authorisation to put into service wagons and rolling stock maintenance workshops	Yes	2	Information related	To reach a bilateral agreement to authorise to put into service wagons and the mutual recognition of rolling stock maintenance workshops.
Czech Republic	Yes	Yes	0	-	Yes	2	Accidents caused by wheelset.	NSA informed RUs and maintenance workshops.
Netherlands	No	Yes	A few times	Vehicle problems	Yes	A few times	About vehicle problems	We checked if the problem might be at hand in our land.
Channel Tunnel	Yes	Yes	-	Communicate informally on regular basis with EPSF & ORR	Yes	None	Communicate informally on regular basis with EPSF & ORR	To share possible best practice and update for other NSA.
Hungary	Yes	Yes	10	-	Yes	10	-	Supervision process developed.
Norway	Yes	Yes	2-4	Supervision reports. Copy of decisions	Yes	2	Information about issuing certificate	Just as information
Ireland	No	No	-	-	Yes	1-2	Rolling stock issues	Directly advised to RU/IM to review and take action as required
France	Yes	Yes	1	Incident rolling stock: Freight train derailment due to axle problem.	Yes	5	Rolling stock incidents	Cooperation is only for SHARING, not coordinating responses. EPSF broadcast these alerts to RUs

NSA	Cooperate?	SENT info	No. times	What was sent?	RECEIVED info	No. times	What was received	How was info used?
								who then strengthened their monitoring.
Finland	No	No	-	-	Yes	2	General	Checked if the issues is relevant in our country.
Italy	Yes	Yes	-	Mainly in relation to accidents/ abnormalities.	Yes	-	Mainly in relation to accidents/ abnormalities.	In order to impose/ enforce an order or for a specific inspection activity.

NSA generally agreed that it was at least 'quite useful' to share safety-related information with other NSA (Table 3.8). Only Estonia and the Czech Republic felt there was less value in doing so, although this may have been related to their specific experiences (for example, Estonia reported that information received in the last year was potentially useful but not directly relevant to rolling stock on its part of the network). Arguably, it is the willingness to engage in this process that makes it valuable as there are indications that the community of NSA as a whole benefits from information exchange.

Several NSA report sharing information with other bodies. It was fairly common for information to be exchanged with national investigative bodies (NIBs) and in a few countries (e.g. GB, Sweden) with other health and safety/regulatory bodies. The GB NSA and the Czech Republic NSA also shared such information with certification bodies for ECMs.

Table 3.8: Value and scope of cooperation

NSA	Usefulness	Information shared with… National investigative bodies?	Certification bodies for ECMs?	Other competent authorities?	If other, please specify:
Great Britain	Quite useful	Yes	Yes	Yes	Other health and safety regulatory bodies
Sweden	Very useful	Yes	No	Yes	Swedish work and environment authority
Estonia	Slightly useful	Yes	No	No	-
Lithuania		No	No	Yes	Our supervision/ enforcement strategy is

NSA	Usefulness	Information shared with… National investigative bodies?	Certification bodies for ECMs?	Other competent authorities?	If other, please specify:
					officially published.
Romania	Quite useful	No	No	No	-
Germany	Very useful	Yes	No	No	-
Denmark	Very useful	No	No	No	-
Spain	Quite useful	No	No	Yes	Not yet because our supervision/enforcement procedures are under development. In addition, our NSA is going to be the national certification body for ECMs.
Latvia	Very useful	Yes	No	No	-
Poland	Very useful	Yes	No	No	-
Bulgaria	Very useful	Yes	No	Yes	-
Austria	Very useful	No	No	No	Under development
Portugal	Quite useful	Yes	No	No	-
Czech Republic	Slightly useful	No	Yes	No	-
Netherlands	Extremely useful				
Channel Tunnel	Quite useful	Yes	No	Yes	Information shared with national transport ministries and regulatory bodies
Hungary	Very useful	Yes	Yes	No	-
Norway	Quite useful	Yes	Yes	No	-
Ireland	Quite useful	No	No	Yes	ERA was sent copy
France	Quite useful	Yes			-
Finland	Quite useful	Yes	No	Yes	IM
Italy	Very useful	No	No	Yes	Ministry

Table 3.9 shows how information that has been shared could be used in several ways. Of the benefits listed in the questionnaire:

- Ten NSA used information that was shared to find solutions to specific problems that they had encountered in their supervision and enforcement strategies.
- Nine NSA had used shared information to help develop a supervision and enforcement strategy.
- Four NSA had used shared information as a way of benchmarking their supervision and enforcement activities.
- One NSA reported using the shared information to help other organisations develop supervision and enforcement strategies or similar approaches.

Six NSA (GB, Lithuania, Romania, Denmark, Spain, and Poland) had not used shared information in any of the ways listed. Only Poland had stated an alternative use, which was to help coordinate activities between different institutions. The Italian NSA did not provide a response.

Table 3.9: Acting on information from other NSA

NSA	What is information from cooperation used for?				
	To develop a supervision/ enforcement strategy	To benchmark supervision/ enforcement	To help other organisations develop supervision/ enforcement strategies or similar	To find solutions to specific problems with the NSA supervision/ enforcement strategy	Other
Great Britain	No	No	No	No	-
Sweden	Yes	Yes	No	No	-
Estonia	No	No	No	Yes	-
Lithuania	No	No	No	No	-
Romania	No	No	No	No	-
Germany	Yes	No	No	Yes	-
Denmark	No	No	No	No	-
Spain	No	No	No	No	-
Latvia	Yes	No	No	No	-
Poland	No	No	No	No	To

NSA	What is information from cooperation used for?				
	To develop a supervision/ enforcement strategy	To benchmark supervision/ enforcement	To help other organisations develop supervision/ enforcement strategies or similar	To find solutions to specific problems with the NSA supervision/ enforcement strategy	Other
					coordinate activities between different institutions.
Bulgaria	No	Yes	No	Yes	-
Austria	Yes	No	No	Yes	-
Portugal	No	No	No	Yes	-
Czech Republic	Yes	No	No	No	-
Netherlands	Yes	Yes	Yes	Yes	-
Channel Tunnel	No	No	No	Yes	-
Hungary	Yes	No	No	Yes	-
Norway	No	No	No	Yes	-
Ireland	Yes	No	No	No	-
France	No	No	No	Yes	-
Finland	Yes	Yes	No	No	-
Italy	-	-	-	-	-

Table B.10 provides examples from the desktop review and the interviews that show cooperation between authorities outside of the rail sector. Some of the key good practice points from these examples are listed below:

- Cooperation with other domestic safety authorities can be beneficial. The Hungarian OSH authority describes cooperation across the various inspectorates in its government. This may have value for NSA that wish to be consistent with other government departments, especially when it comes to authorities that may

have some remit over rail activities (such as for occupational safety and health). Cooperation may extend to sharing policies and procedures to establish a consistent approach between different domestic safety authorities.

- Stakeholder cooperation can be in the form of regular forums and conferences. The German OSH authority has established one such forum in law as an annual opportunity to bring together key stakeholders. This structured approach to cooperation ensures that it is given sufficient priority.
- The Austrian OSH authority has established an annual regional conference with neighbouring states to provide a consistent and harmonious approach across borders. Such cooperation arrangements, especially in the form of a regular conference, have considerable value. When countries are geographically close there is value in developing a common approach to cross-border working. The conference is also a common platform for discussing issues of mutual concern, new regulations, etc. and arriving at a common approach to these, rather than doing so independently. Whether or not formal cooperation agreements are in place, the platform for dialogue in this example demonstrates a good practice approach.

Table B.11 provides examples from the interview findings of how NSA cooperate. A common theme in almost all examples of cooperation is that they are typically local, bilateral agreements between neighbouring NSA, NSA that share cross-border traffic, or in response to Part B applications received from foreign undertakings; the cooperation in these examples has been prompted by the necessity of an NSA dealing with activities that extend beyond its borders. In doing so, NSA have raised several issues:

- Cooperation can be on specific topics, such as maintenance, as reported by the Dutch NSA. The maintenance covenants it has in place are helpful for stimulating safe, cross-border trade and it is a response to market-driven requirements.
- Cooperation between NSA is largely informal. Informal links enable exchange of information, particularly in relation to Part B applications. Information can be exchanged in both directions via such agreements; so if the SMS or operations of a foreign RU raise concerns, the supervising NSA can use cooperation links to report this back to the NSA responsible for the Part A certificate (which will theoretically be able to explore whether the issues exist in the RU's source SMS).
- Cooperation can include joint supervision activities as adopted between Germany and the Netherlands as well as between some of the Nordic states. Such cooperation enables NSA to better understand the links between the SMS that is described for Part A and Part B certificates (where Part B is to be issued by a different Member State) by sharing audits.
- Cooperation between NSA can facilitate foreign RUs in understanding the national rules before submitting an application for a Part B certificate.

Outstanding issues that may need to be resolved for cooperation to be more successful include:

- A need to establish contacts at each NSA for the purpose of cooperation. This could be as simple as a dedicated email address, telephone number or an

individual assigned with that task. Without a clear point of contact, the initial link has been reported as being difficult to initiate.

- A need to establish a more formal approach to cooperation at European level – a 'template' to encourage cooperation that goes beyond bilateral agreements between specific NSA that focus on the axes of need. This is particularly important with respect to language differences and the scope of NSA powers to request information from foreign undertakings (as raised by the Czech and Polish NSA).
- A concern about the timing of renewals. The Swedish NSA was aware that renewals for Part B certificates were dependent on Part A renewals being completed first, and the timing of these processes could be critical to the continued operation of some rail services. Cooperation could have a role to play in smoothing the timing of renewals.
- A need to share best practice as well as safety-related information. This point, made by the Bulgarian NSA, somewhat contradicts the attitude of the GB NSA, which has avoided increasing cooperation with other NSA primarily on the basis of different railway systems and no cross border traffic at present (Channel Tunnel excepted, which is the responsibility of a separate NSA). It did not acknowledge that other NSA may also wish to share best practice.

In summary, the recommendations to achieve a baseline level of good practice are to:

- Assign a point of contact for cooperation (e.g. a dedicated email, telephone number and/or member of staff). Provide details of this online or share directly with all NSA.
- Be open to exchanging information with regard to Part B applications from foreign RUs. Consistent application of the safety regulatory framework is still developing so some NSA may wish to exercise prudence in requesting information from the NSA that issued the Part A certificate for an RU that is applying for a Part B in a different Member State.
- Liaise with relevant NSA regarding the reassessment of safety certificates that are nearing the end of their validity. It has been noted that the interdependence between Part A and Part B certificates will require a coordinated effort from NSA to ensure that reassessment does not lead to RUs being unable to operate for any period of time due to certificates not being reissued promptly.

NSA that wish to demonstrate further good practice in cooperating with other NSA are recommended to:

- Proactively offer basic information to an NSA regarding Part A assessments if it is pertinent to an RU's application for a Part B certificate in another Member State.
- Organise collaborative meetings with NSA that currently share cross-border traffic, or have markets that would like to expand into other Member States. Involve other relevant stakeholders as appropriate.
- Agree on how to supervise jointly in a way that overcomes language differences and enables NSA to collect the necessary evidence.

Additional recommendations for good practice in cooperation are for NSA to:

- Listen to market requirements — where are there demands for NSA to collaborate to improve cross-border trade? (E.g. maintenance covenants to cover cross-border standards for maintenance of rolling stock).
- Proactively offer supervision and investigative support to other NSA on matters of shared interest (e.g. incidents in another Member State that involve a domestic RU).
- Undertake joint supervision activities with other NSA.
- Cooperate with other domestic safety authorities that may have an influence on areas of the rail industry to establish a coordinated approach.

There have also been repeated calls from NSA for ERA to develop a structure and guidance for cooperation. This is forthcoming and will be delivered as part of a guidance document to accompany the CSM on Supervision. Drafts of the guidance outline the recommendations for formal cooperation agreements between NSA to develop joint supervision plans for RUs.

Key findings:

- Majority of NSA have informal arrangements to cooperate.
- Exchange of safety-related information is the most common type of cooperation.
- NSA generally recognise the value of cooperation, especially for developing and refining supervision strategies.
- Cooperation can take many forms: the exchange of information; the sharing of services and expertise; formal agreements on acceptable practices.

Good practice recommendations:

- Assign a contact point at each NSA for cooperation enquiries.
- Exchange information relating to Part B applications.
- Consider the impact on Part B certificates when NSA are planning reassessments.
- NSA should organise meetings and conferences for the purpose of cooperation.
- Supervise jointly with other NSA those RUs that engage in cross-border activities.
- Address language differences to facilitate cooperation supervision.

3.2 Competency for supervision and enforcement

The following subsections (3.2.1–3.2.4) discuss three key questions related to the competence of staff for supervision and enforcement. Specifically:

- How do NSA define the competence that is necessary for staff who carry out supervision and enforcement?
- How do NSA manage competence, including identifying training needs?
- Are existing teams resourced with competent staff for the activities of supervision and enforcement?

3.2.1 Skills/competence required of staff for supervision and enforcement

In the questionnaire, respondents were invited to report the skills and competence that were required for the role for supervision. Table B.12 describes the requirements of each NSA.

Figure 3.3 summarises the proportion of NSA that specified that a particular competence was a requirement for staff who carry out supervision and enforcement. Auditing skills, knowledge of rail systems and legislative knowledge were the most common requirements and were specified by at least 50% of NSA. A third of NSA required interpersonal skills from staff, such as the ability to liaise with representatives of RUs and IMS, and explain and negotiate where appropriate. Just over a quarter of NSA demand higher level education of their staff.

It was not common to expect staff to already have knowledge of SMS when joining an NSA although a small proportion did set such a requirement. Only the GB NSA specified that staff would need to develop skills in occupational health and safety, reflecting how this particular NSA has a remit that includes this aspect, unlike most other NSA.

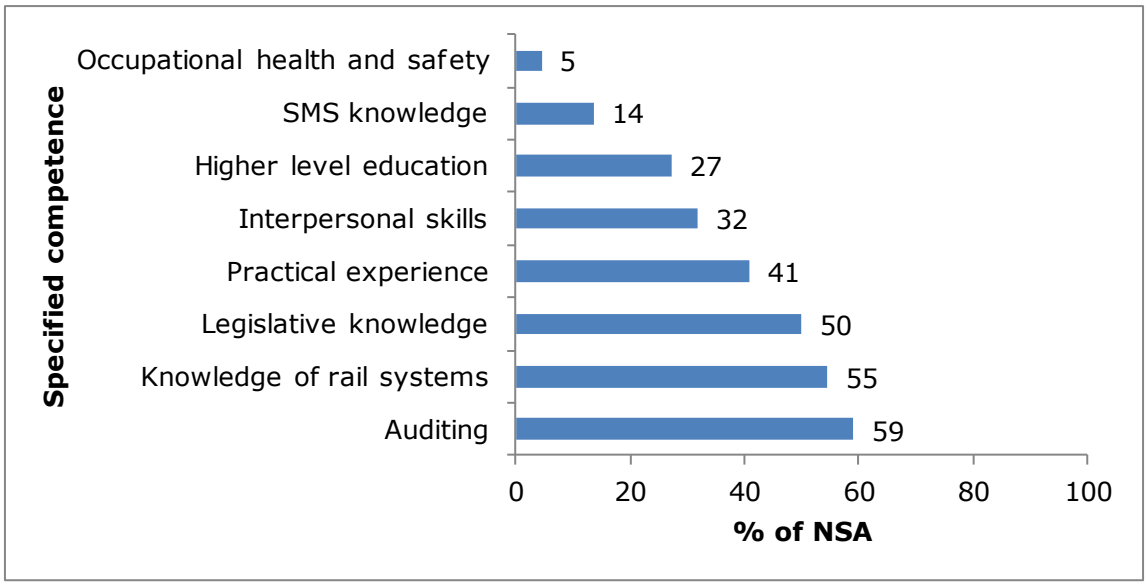


Figure 3.3: Proportion of NSAs that specified a particular competence was required

3.2.2 Competence management

Table B.13 provides examples of how authorities can plan for the training of staff who undertake supervision and enforcement. For an NSA that wishes to operate within the principles of supervision, these examples raise important points to consider:

Applicable safety regulatory framework:

CSM on Supervision (Article 6)

"The national safety authority shall have a system in place to ensure that supervision activities are undertaken by competent persons."

- What are the training needs for the supervision team and can specific needs be met? The GB NSA has a programme for targeting training needs that requires input from team managers and the strategic priorities of the NSA.
- How can training be efficient? Resource management is often a key issue for NSA. The examples here suggest that training can be delivered efficiently if the authority:
    - Delivers training to those who need it, and when they need it.
    - Shares common training needs with other government departments. Basic audit training is one example of where this can be possible, as shown by the GB, Dutch and Swedish NSA.
    - Utilises market experience where appropriate. The Danish NSA uses its main IM to deliver some of the technical training on railway systems to its staff. This is based on the IM having existing training provisions and being well-placed to deliver relevant information to NSA staff.
    - Utilises in-house expertise. Sometimes senior inspectors within an NSA are best placed to deliver training, which is one of several approaches used by the GB NSA. This approach is offers the flexibility to tailor for specific training needs.

The examples all show that there is not one single approach to training provisions that best meets the principles and a combination may be the most appropriate way to ensure supervision staff have the required competencies to act proportionately and consistently.

Competence management of its own staff is a factor that may also affect an NSA's ability to target its supervision activity and prioritise how its resources are used. It is advisable to plan training so that it has a strategic basis. The Polish NSA describes the risks to functionality that can emerge if training is not incorporated into the strategy; in effect, the NSA may find itself insufficiently staffed by those with the skills required to develop into the role set by the European safety regulatory framework.

As an aside, incorporating plans for competence management is a way of the NSA leading the market by example; the Belgian NSA incorporates such provisions in its public 'Action Plan'. The Latvian CAA documents the scope of its training online, which may give dutyholders confidence in the competence of the safety authority.

A note of caution is required when considering the approach to competence management adopted by the Spanish NSA. There is a reliance on existing experience (most staff have a rail background) but the risk is that uniform practices may not follow, so supervision may become inconsistent and disproportionate. Whilst all staff may be highly skilled,

these skills may vary, particularly for essential activities such as auditing. It is desirable for NSA to establish a baseline level of expertise that its entire staff must have.

Table B.14 provides several examples of how training is delivered to staff. Although the principles of supervision make no specific reference to training of staff, for an NSA to function in accordance with the principles it will need staff that have received suitable training. In particular, for an NSA to be accountable for its enforcement decisions, it is arguable that part of the 'policies and principles' by which it can be assessed could relate to training policies.

Examples from Table B.14 for consideration include:

- The structure, scope and duration of 'on-the-job' training. The vast majority of NSA use this type of training for new inspectors, which typically has the new inspector being accompanied on audits by a more experienced member of staff. The various practices suggest this process may last for a period of 4–18 months. If this process is followed, NSA may also wish to consider how to close the process (for example, the Swedish NSA involves key figures in a final meeting to discuss the outcomes of the accompanied audits).
- Repeating accompanied audits to check on progress of new staff after a period of allowing them to work independently (e.g. the Austrian NSA).
- A focus on audit training, specifically. This has been described as an essential training requirement to help the NSA fulfil its activities, particularly with regard to guiding rather than advising RUs/IMs.

Competence management should also be structured in a way that encourages staff to engage with the process. Continuous improvement is a feature of competence management and from the outset it is desirable for staff to be willing to adopt new practices. The Polish NSA is currently facing challenges from staff regarding the adoption of the SMS-based approach to supervision.

Table B.15 provides examples of how training provisions and future requirements can be assessed. NSA report the following practices:

- Review supervision data by inspector to identify any weaknesses in the competencies of specific staff (e.g. the GB NSA). A set of performance assessment criteria may be required, such as the length of time taken to complete each case.
- Online competence management systems, which are completed by inspectors to identify training gaps (e.g. the GB NSA). Other authorities may follow a similar process manually (e.g. the Danish NSA).
- Final examinations for new starters (as practiced by the Austrian OHS authority).
- Panel assessment of new starters, as practiced by the GB NSA. The benefits of this approach are that the review discussion is based upon a technical examination of current work and a presentation of two cases, which roots the assessment in the competences that are required for the role.

Processes that enable NSA to be aware of training gaps can facilitate consistency and help to prioritise resources. Table B.16 offers a couple of examples from the GB NSA related to updating the legal knowledge and skills of staff carrying out supervision. Such

training involves regular updates on new regulations and peer discussions of legal decisions. Such measures are expected to deliver consistency in supervision and help to ensure that the NSA remains accountable for its actions, with staff being knowledgeable of those polices that they can apply when supervising. As the Danish NSA discusses, it is desirable for new regulations to be incorporated via a training programme so that the NSA is consistent in its response and only adopts what is necessary.

3.2.3 Training staff for supervision

Table 3.10 shows that, of the 20 NSA responding to the questionnaire:

- Ten (GB, Sweden, Germany, Portugal, Netherlands, Channel Tunnel, Norway, Ireland, Italy and France) provide training courses and on-the-job training to staff.
- Four (Romania, Latvia, Poland, and the Czech Republic) have no formal training provisions for staff. All expect staff to enter the organisation with sufficient knowledge and then improve upon this independently. The Polish NSA would like to offer training but has limited resources to do so.
- The remaining NSA provide at least some formal training.

Table 3.10: Training requirements for new supervision staff

NSA	Training course	OTJ	Other/comments
Great Britain	Yes	Yes	Guided reading of enforcement related / technical information on intranet or dedicated competencies site to ensure inspector skills are updated and maintained.
Sweden	Yes	Yes	1.) Specific internal training course for new inspectors have started 2011. 2.) Special training for inspections of dangerous goods
Estonia	No	Yes	
Lithuania	No	Yes	
Romania	No	No	Self-training
Germany	Yes	Yes	
Denmark	No	Yes	ISO, lead auditor cause
Spain	No	Yes	
Latvia	No	No	Assumed knowledge/skills - Specific education and experience in railway field to be employed, plus specific courses and practical work
Poland	No	No	No relevant training offered, also we lack enough resources in terms of both money and people. Building competence is based mostly on self-training and exchange of experience between staff. This approach is

NSA	Training course	OTJ	Other/comments
			based on limited budget for training and lack of training meeting specific requirements of the NSA.
Bulgaria	No	Yes	No
Austria	No	Yes	No
Portugal	Yes	Yes	Participation on seminars, international meetings of working groups and task forces (ERA, Commission)
Czech Republic	No	No	Exam from the knowledge of legislation.
Netherlands	Yes	Yes	
Channel Tunnel	Yes	-	For GB half of the channel tunnel: provided by GB mainland regulator – the Office of Rail Regulation (ORR) For FR half: provided by EPSF (FR NSA)
Hungary	No	Yes	
Norway	Yes	Yes	
Ireland	Yes	Yes	
France	Yes	Yes	
Finland	No	Yes	2 staff with long railway experience and all auditors have audit experience and special auditor training courses
Italy	Yes	Yes	

3.2.4 Ensuring awareness of the safety regulatory framework

Table 3.11 shows that, of the 20 NSA responding to the questionnaire:

- Six NSA (GB, Estonia, Germany, Spain, Italy and the Netherlands) have specific courses and on-the-job training to ensure that staff have a good awareness of the safety regulatory framework.
- Three NSA (Romania, Latvia and Czech Republic) have no formal training on the safety regulatory framework. Latvia stated that staff should have this knowledge prior to taking on the role.
- The remaining NSA provide at least some formal training. Of note: Sweden has started a new internal training course for its inspectors; Denmark will make provisions in response to individual needs; Poland and Portugal try to engage with the wider community of stakeholders and NSA to share knowledge – Polish staff specifically find language is a barrier to this, however. The Irish NSA uses team briefings and the French NSA has a similar approach.

Table 3.11: Methods to make staff aware of the safety regulatory framework

NSA	Specific course	OTJ	Other/comments
Great Britain	Yes	Yes	Assessment against dedicated competency framework and specific guidance documents / training on relevant issues.
Sweden	No	Yes	1.) Specific internal training course for new inspectors have started 2011. 2.) Internal calibration meetings, information, website
Estonia	Yes	Yes	
Lithuania	No	Yes	
Romania	No	No	No
Germany	Yes	Yes	
Denmark	Yes	No	No formal procedure on this topic, training can be provided if found appropriate
Spain	Yes	Yes	
Latvia	No	No	Before the staff start to fulfil their duties they should know the regulatory framework. The new staff study the legislation under the supervision of head of unit.
Poland	No	Yes	The EU legal acts and guides are distributed among NSA staff. They are also published on the NSA website. Information about the requirements is shared during UTK staff meetings in the form of presentations. Meetings with ERA experts are also organized, both on bilateral basis and as general workshops. Main problems that we face in this process are linked with the low command of English language in the NSA.
Bulgaria	No	Yes	
Austria	No	Yes	
Portugal	No	Yes	Participation in seminars, international meetings of working groups and task forces (ERA, Commission)
Czech Republic	No	No	
Netherlands	Yes	Yes	
Channel Tunnel	Yes	No	
Hungary	No	Yes	
Norway	No	Yes	
Ireland	No	Yes	Team briefings

NSA	Specific course	OTJ	Other/comments
France	No	Yes	Yes - Periodic internal meetings for information relating to the European regulations.
Finland	No	Yes	Internal education and training
Italy	Yes	Yes	

In summary, a baseline level of good practice for competence management could require NSA to:

- Set competence management as a strategic goal.
- Establish training for all staff for essential supervision practices, such as auditing skills.
- Establish a process to ensure that new staff can supervise to an acceptable standard before being permitted to work with greater independence. Shadowing and mentoring new staff is a common approach.

Further good practice may require NSA to:

- Address technical needs with targeted training. Technical knowledge should be moderated by the SMS-based approach which requires RUs and IMs to have the technical capabilities to be responsible for safety management.
- Make use of in-house expertise for developing competencies of new or less experienced staff. Make use of industry expertise if required knowledge is not in-house.
- Implement a process for monitoring staff competence. Examples include examinations and case study assessments.

Additional good practice measures may require NSA to:

- Consolidate training provisions across domestic government safety authorities where appropriate.
- Introduce internal online competence management systems to facilitate ongoing development and review.

Key findings:

- Less than half of NSA have formal training courses for staff. On-the-job training and informal approaches are most common.
- Only a quarter of NSA have formal courses to ensure that staff are kept aware of the current safety regulatory framework.
- New staff are most commonly shadowed/mentored by more experienced staff on induction.
- Competence assessments of new staff may be decided by examination, case study reviews and peer group discussions.

Good practice recommendations:

- Ensure competence management has a strategic priority.
- Focus on development of essential skills for supervision, such as auditing practices.
- Monitor induction of new staff, and existing staff regularly, to ensure satisfactory competence.
- Source training in-house, from other domestic authorities or via the market where appropriate. For efficiency, consolidate training.
- When updating legal awareness of the framework, ensure staff are aware of the pertinent points and the implications for supervision and enforcement activities.

3.3 Supervision strategies

This section discusses supervision strategies, with subsections 3.3.1–3.3.5 examining how targets for supervision are set, reviewed and prioritised. A summary and recommendations are provided in subsection 3.3.6.

Table 3.12 shows that 15 NSA have a strategy for supervision, while five are in the process of developing a strategy and two do not have a strategy. Spain intends to base its strategy on the CSM on Supervision.

Table 3.12: NSA with strategies for supervision

NSA	Strategy?	If not, why?
Great Britain	Yes	-
Sweden	Yes	-
Estonia	Under development	-
Lithuania	Yes	-
Romania	Yes	-
Germany	Yes	-
Denmark	Yes	-
Spain	No	There is no general strategy for supervision and enforcement established (it is under development) because: • The creation of the structure of the NSA has not finished • Little maturity of the safety certification system in Spain (and few RUs in the sector) • Awaiting development of the CSM on Supervision to establish a strategy according to it • No foreign RUs
Latvia	Yes	-
Poland	Under development	We plan to use guidance from EU regulations as a basis for our general supervision and enforcement strategy.
Bulgaria	Yes	-
Austria	Under development	-
Portugal	Under development	-
Czech Republic	No	It has not been completed yet.
Netherlands	Under development	There is a strategy but it is not in writing
Channel Tunnel	Yes	
Hungary	Yes	

NSA	Strategy?	If not, why?
Norway	Yes	
Ireland	Yes	
France	Yes	
Finland	Yes	
Italy	Yes	

3.3.1 Targeting supervision and enforcement activity

The forthcoming CSM on Supervision suggests that in setting up a supervision strategy and plan(s), NSA should identify target areas for supervision activity that will guide how resources are deployed. One approach could be to identify target areas at a national level (e.g. level crossings, which can affect multiple RUs and IMs); another approach could be to identify target areas at the level of individual RUs/IMs. In response to the questionnaire, Table 3.13 shows that:

- Seven NSA (GB, Romania, Denmark, Bulgaria, Austria, Finland and Italy) set targets for supervision and enforcement activity at a national level as well as for individual RUs/IMs.
- Two NSA (Czech Republic and the Channel Tunnel) do not set any targets for supervision and enforcement activity.
- Germany and Sweden do not target areas at a national or individual RU/IM level; instead they appear to follow a risk-based approach that targets areas related to the risks presented by each RU/IM.
- All other NSA target at a national or individual level. The Polish NSA has targets that are based on maintaining a current level of safety (rather than striving to further improve) which arises from its existing supervision regime (which is co-existing with the EU safety regulatory framework at the present time).

Taken as a whole, there are 13 NSA that target supervision activities at a national level and seven that target at the level of specific RUs/IMs.

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.4/5) and 1169/2010 (Annex III.4/5):

"4. NSA supervision activity shall be targeted primarily at those activities which a NSA believes give rise to the most serious risks or where the hazards are least well-controlled.

5. NSA shall decide on priorities to use their resources effectively but the decision on how best to do that should rest with each individual NSA. Action shall be focused on those who are responsible for the risk and who are best placed to control it."

CSM on Supervision (Article 8)

"1. The NSA shall develop a supervision strategy outlining how it targets its activities and sets its priorities for supervision.

3. The NSA shall regularly review the strategy and plan or plans in light of experience, using the information collected and the outcomes of supervision."

Table 3.13: Setting supervision targets

NSA	Sets supervision/ enforcement targets at a national level	Sets supervision/ enforcement targets for each RU/IM	Other, please specify:
Great Britain	Yes	Yes	No
Sweden	No	No	Targets for risk-based supervision
Estonia	Yes	No	No
Lithuania	Yes	No	No
Romania	Yes	Yes	No
Germany	No	No	There are general aspects of targeting and aspects relating to each RU / IM.
Denmark	Yes	Yes	No
Spain	Yes	No	The NSA has not set targets yet (as the supervision strategy is under development) but they will be set at a national level
Latvia	Yes	No	No
Poland	Yes	No	Setting the targets was linked up to now with the old approach to supervision. It included framework plans for supervision activities, which set rules and timeframe for controls carried out by regional departments. The targets have been set on the basis of safety related information collected during previous years. The supervisory activities were focused on maintaining the current safety level.
Bulgaria	Yes	Yes	No
Austria	Yes	Yes	No
Portugal	No	Yes	No
Czech Republic	No	No	No

NSA	Sets supervision/ enforcement targets at a national level	Sets supervision/ enforcement targets for each RU/IM	Other, please specify:
Netherlands	Yes	No	No
Channel Tunnel	No	No	No
Hungary	Yes	No	No
Norway	Yes	No	No
Ireland	No	Yes	No
France	-	-	The Ministry sets EPSF high-level objectives in achieving control. EPSF establish an annual inspection plan (audits systematic, cyclical audits, inspections). The EPSF may have to step up its controls to situations, e.g. incidents.
Finland	Yes	No	No
Italy	Yes	No	No

3.3.2 *Frequency of target reviews*

According to the questionnaire, half of NSA review their supervision targets every 12 months (Table 3.14).

Table 3.14: Frequency with which NSA review supervision targets

NSA	Frequency of reviewing targets of supervision/ enforcement	If never/other, why?
Great Britain	Every 12 months	-
Sweden	Other	Depends of risk-based supervision
Estonia	Every 12 months	-
Lithuania	Every 12 months	-
Romania	Every 12 months	-
Germany	Other	There is no formal requirement to review each XX months.
Denmark	Every 12 months	-
Spain	Other	The frequency for reviewing the targets has not been set yet but

NSA	Frequency of reviewing targets of supervision/ enforcement	If never/other, why?
		it is expected to be every 2 years.
Latvia	Every 12 months	-
Poland	Other	We do not have any experience in this matter for the CSM approach to supervision. We estimate that once the new system is fully established, we will be doing it once a year.
Bulgaria	Every month	-
Austria	Every six months	Currently under development.
Portugal	Every 12 months	-
Czech Republic	Never	We have no specific targets.
Netherlands	Every 12 months	
Channel Tunnel	Never	Not relevant, scope of infrastructure does not require target setting – arrangement would not be proportionate
Hungary	Every 12 months	-
Norway	Other	On an irregular basis.
Ireland	Every month	Note: this review would not be formally documented.
France	Other	The annual plan of controls is reviewed regularly. A new annual plan is produced annually.
Finland	Every 12 months	-
Italy	Every 12 months	-

3.3.3 *Self reported ratings for targeted supervision*

According to Regulations 1158/2010 and 1169/2010, NSA supervision activity shall be targeted primarily at the activities which carry the most serious risks or have the least well-controlled hazards. The majority of NSA (16 out of 22) reported that they carry out 'very' or 'completely targeted' supervision and enforcement (Table 3.15). Five NSA (Estonia, Poland, Austria, Finland and Portugal) are 'quite targeted' in their activities whereas the Czech Republic is only 'a little targeted'.

Table 3.15: NSA ratings for targeted supervision

NSA	Targeted	Examples
Great Britain	Very targeted	
Sweden	Very targeted	Target to risk and risk-based

NSA	Targeted	Examples
Estonia	Quite targeted	
Lithuania	Very targeted	
Romania	Very targeted	
Germany	Very targeted	
Denmark	Very targeted	
Spain	Very targeted	Nowadays, inspections are carried out depending on sensible points (which would generate risks).
Latvia	Very targeted	For RUs and another companies dealing with dangerous goods NSA has a special inspector to control this issue.
Poland	Quite targeted	Bear in mind that the activities in the supervision plan for 2011 do not refer to separate undertakings risks but to main risks identified for the whole market.
Bulgaria	Very targeted	
Austria	Quite targeted	
Portugal	Quite targeted	
Czech Republic	A little targeted	
Netherlands	Very targeted	
Channel Tunnel	Completely targeted	
Hungary	Very targeted	
Norway	Very targeted	
Ireland	Very targeted	
France	-	
Finland	Quite targeted	
Italy	Very targeted	Examples of good targeting: • A RU having not solved (in a little or great part) the prescriptions/conditions contained in the safety certificate. • A RU that did not provide any answer to the NSA's remarks/advices/orders. • A RU subjected for a certain period (in absence of traffic) to an audit judged compulsory to restart the commercial service.

3.3.4 Priority areas to target supervision

Table 3.16 lists the areas of priority for each NSA, in order of priority from 1 (more important) to 8 (less important). Priorities will vary according to the operating characteristics of different parts of the network. Respondents were required to rank each area differently; it was not possible to assign the same rank to two or more areas. Germany and France opted not to rank the areas in order of priority.

Table 3.16: NSA priority areas for supervision

NSA	Contractor management	Level crossings	Competence management	Train dispatch inc. SPADS	Unauthorised access/ trespass (exc. suicides)	Maintenance of rolling stock	Maintenance of signalling	Maintenance of track
Great Britain	5	1	6	7	8	3	4	2
Sweden	2	7	1	6	8	5	4	3
Estonia	7	6	2	1	8	4	5	3
Lithuania	8	1	7	3	2	4	5	6
Romania	6	5	7	1	8	2	3	4
Germany	(Such a prioritisation is inappropriate).							
Denmark	8	5	4	7	6	1	3	2
Spain	8	6	1	3	7	2	4	5
Latvia	7	5	6	1	8	4	2	3
Poland	7	2	1	6	8	3	4	5
Bulgaria	8	7	3	1	2	4	6	5
Austria	8	7	6	5	4	3	2	1
Portugal	7	5	6	4	8	1	2	3
Czech Republic	7	1	5	6	8	3	2	4
Netherlands	5	3	2	1	7	6	8	4
Channel Tunnel	4	N/A	5	6	7	1	3	2
Hungary	8	5	4	6	7	3	1	2
Norway	3	7	2	5	8	4	6	1
Ireland	3	1	2	8	7	4	6	5
France	-							

NSA	Contractor management	Level crossings	Competence management	Train dispatch inc. SPADS	Unauthorised access/ trespass (exc. suicides)	Maintenance of rolling stock	Maintenance of signalling	Maintenance of track
Finland	1	7	4	2	8	3	6	5
Italy	3	4	5	7	8	2	6	1

During the interviews, NSA were invited to discuss the reasoning behind the ordering they gave.

The Danish NSA would have preferred an option to rank some areas as equivalent; for example, maintenance of tracks and rolling stock would have been given equivalent priority. The NSA explained that priority is given to avoiding catastrophe:

> *'Are we trying to avoid catastrophe or are we dealing with what is happening actually, what is killing people on a daily basis on the railway? And the background for this is we are prohibiting the catastrophe; that's mainly* [what we are doing]*. That's why maintenance of the rolling stock and the track is the major issue.'*

However, the amount of resource that is targeted at each area *"might not be proportional with the ranking"*. Level crossings were ranked fifth in the list of priority areas and yet the Danish NSA explained that more resources would be allocated to supervision of level crossings than other higher priority areas. The NSA explained the reasoning behind this approach:

> *'It's where is the biggest risk? The danger in rolling stock or tracks can lead to a major disaster with hundreds of people killed, something like that. A level crossing is maybe two people, one person. That's how you should see the ranking. But where is the risk highest? That is on the level crossing so we have to look into our system and we will say how is the state of maintenance at this point? It's good, we feel confident. With the state of the level crossings, it's not so good so we will target our resources there.'*

A further point of discussion was the supervision of competence management and contractor management. Neither was rated as highly as maintenance issues by the Danish NSA and yet there is a view that effective maintenance requires competent staff and contractors to deliver it. The Danish NSA stated that:

> *'I would actually have included competences in the maintenance of the rolling stock, the maintenance of the tracks. I would not have had a* [separate] *line for the competences. We are looking at where are the competences needed? They are definitely needed concerning maintenance of rolling stock and tracks. And it's the main cause actually of making the safety management system work that you have the competences. And our main focus is the safety management system. If we are looking at competences in a company, big or small, part of that audit, we include checking competences. And management competences is actually what*

we are going to look into. But if we go on an audit for maintenance, we will look at competences and we will also look at the contracts.'

The comments of the Danish NSA indicate that supervision topics such as management competencies and contractor management cannot be segregated from the activities where these skills are required. The NSA is therefore aware that when it is supervising an area where such skills are needed, it will ensure these skills are being delivered by the SMS.

The Austrian NSA expressed similar concerns regarding the prioritisation of these areas.

'It's… depending on the incidents and the… number of incidents. Each point in itself may have at a certain point, at a certain time, the highest priority, so… because there are so many different points and data to be considered… it's quite difficult to put this list into prioritisation. Maintenance is one important problem, but on the other hand if I have the best maintenance rules and no persons who have the skills for this, it's also not possible. I think there is a lot to be considered with doing a real profound prioritisation. Level crossing, for instance, was I think one or two years ago one of the main points of our ministry to improve… so this, two years ago this would have been put higher into priority than something else.'

As well as echoing the point made by the Danish NSA that competence is an integral to delivering effective maintenance, the Austrian NSA added that incident data and wider strategy influences at a national and European level can also affect prioritisation.

The GB NSA had similar priorities to the Danish NSA in that its priorities for supervision were 'prevention of catastrophic failure'. Although it ranked level crossings and maintenance issues as the first four priorities, given the option the NSA would have ranked all four items as equal. Contractor management was the next priority:

'Contractors do deliver a lot of the upgrades, significant renewals on the infrastructure. They're not directly controlled by the railway dutyholders. We know that that performance is not as good as we would like, and there are regular incidents there due to the contractor… relationship, so there's significant safety risk in there.'

This was followed by competence management:

'Competence underpins all activity on the railway. You rely on your people to maintain the track, maintain the crossings. Going back to my principle of inspector competence, you've got to do the same with all the railway staff, i.e., you've got to make sure that they maintain that competence, and you've got to keep an eye on it.'

The GB NSA reported that competence and contractor management are subsumed into the maintenance of level crossings and structural subsystems, so assigning priorities is a difficult task. However, *'The problem is that just because you prove someone's competent it doesn't mean they're going to do it properly'*. Trespass was reported to be the lowest priority because the GB NSA stated that the vast majority of trespass is suicide and it felt reasonably powerless to expect RUs/IMs to prevent this type of access.

The Swedish NSA was one of three NSA (the others being Poland and Spain) that rated competence management as the highest priority. As with other NSA, it would have

preferred to rank several items as equivalent but its view on competence management was unequivocal:

> *'It's more important to have…* [a] *good competence management system, so you can be sure that you have the right staff… if the maintenance of the signal system is not working, it's a danger, but why is it not working: is it because you have not the skills, or is it because you have not enough resources, or what is it? I think competence management system is a bullet point for a lot of these different levels…'*

The Spanish NSA confirmed that its principal priority was to ensure competence was being managed appropriately and that other items were somewhat out of scope.

3.3.5 Prioritising resources

Regulations 1158/2010 and 1169/2010 specify that one of the principles of supervision should be for NSA to prioritise use of their resources effectively to ensure that action is focused on those who are responsible for (and best placed to control) risk. NSA should be able to make their own decisions on how to allocate resources to ensure this goal can be achieved.

Table 3.17 shows that all but one NSA reported authority to prioritise how its resources were used (Hungary did not have such authority). However, the details of this process indicated that for some NSA there was an element of external control. Examples include Estonia (authority held by Ministry of Economics and Communication Affairs), Germany (authority for global shifts of prioritisation held by Ministry of Transport), Portugal (authority held by Director of the Railways Department) and the Czech Republic (authority held in part by Ministry of Transport).

The proportion of staff and monetary resources allocated to supervision and enforcement varied substantially between NSA. Of the 20 NSA responding:

- Four (Spain, Portugal, Czech Republic and Finland) allocated less than 10% of staff and of total budget to supervision and enforcement activities. However, in the case of the Czech Republic, this proportion reflects how the NSA is part of a much larger organisation responsible for rail, which is an issue shared to some extent by other NSA in Germany, Romania, Poland and Portugal.
- Four (Estonia, Romania, France and the Channel Tunnel) allocated at least 50% of staff to supervision and enforcement.
- The remaining NSA allocated between 11 and 50% of their staff to these tasks.

The interviews with NSA indicated that the dialogue between the NSA and the Ministry that provides it with a budget for resources can be a fairly open, two-way discussion. The German NSA stated:

> *'That's a yearly process, mainly oriented on the yearly budgeting procedure. That's where we have to justify why we need that staff, why we need maybe additional staff, why we don't need some staff anymore. If it's something we had to do in the past is no longer there then maybe we don't need the staff we had for that. That's a yearly process with fixed deadlines, which has to be run through every year.'*

This description suggests that NSA should be in a position to present a case for the resourcing they need based upon the supervision activities that they plan. Without a plan for supervision, it would be difficult to determine accurately the level of resource required.

Not all NSA reported such open dialogue with their respective Ministries. It is acknowledged that some NSA are allocated resources for supervision and enforcement that can fall short of what is genuinely required to supervise and enforce the market. Where this situation arises, a detailed supervision plan may lay the foundations for such dialogue about resources between an NSA and its Ministry; at the very least, it has been suggested that if a Ministry cannot resource the supervision plans fully, it should then be involved in deciding with the NSA which topics can be justifiably excluded from the supervision plan so that it fits with the available resource.

Table 3.17: NSA resource allocation

NSA	Who has authority?	Resources used for supervision		Comments
		% of all staff	% of total budget	
Great Britain	The NSA Board and Directors	40-50	40-50	ORR is the NSA but only RSD is involved in safety regulation. Our answer implies that the NSA only spends around 50% of its time regulating safety issues (the rest of its time is spent carrying out its economic function), but there is nowhere to clarify this.
Sweden	Government gives money in budget but NSA itself prioritises resources	10-15	5-10	-
Estonia	Ministry of Economics and Communication Affairs	70-80	90-95	-
Lithuania	NSA	25-27	15-20	-
Romania	NSA	70-80	-	As part of Romanian Railway Authority, NSA Romania hasn't its own budget. Therefore it is not possible to estimate NSA's budget percentage as part of RRA's.
Germany	NSA/Ministry of Transport	15-20	15-20	To some extent prioritisation is possible. For global shifts of prioritisation, agreement with Ministry of Transport has to be sought. Remark: EBA has far more tasks than the 'core' tasks of an NSA acc. to Art. 16 (2) of CD 2004/49/EC. Percentage of staff in supervision would be higher, if only the 'core' NSA tasks

NSA	Who has authority?	Resources used for supervision		Comments
		% of all staff	% of total budget	
				were the relation.
Denmark	Head of the supervision department	20-25	20-25	-
Spain	General Manager of Railway Infrastructures	5-10	7-9	-
Latvia	Head of NSA, heads of units	30-35	40-45	-
Poland	Board - President of UTK, two Deputy Presidents (out of which one is responsible for safety and the second for market regulation) and the Director General. Decisions depend on current priorities in the work of the Office (safety, regulation, passenger rights etc.), available resources and competences.	-	-	Generally resources are very limited thus there is little possibility of changing their assignment - this forces the NSA to make the same employees work on different aspects depending on current needs. This leads to a situation where staff assessing applications for safety certificates / authorisations also is involved in the supervision process. It is hard to define exact percentage, because of parallel functioning of two separate supervision regimes – one through SMS and the second through on site inspections of technical maintenance etc. Supervision through SMS is being carried out by 16 employees, apart from that there are also 62 employees involved in on the ground inspections (maintenance of infrastructure etc.). Additionally, please note that NSA is a part of a Railway Transport Office (UTK) comprising also the duties of regulatory body and national enforcement body (passenger rights), which makes it hard to point out what exact amount of staff and budget is linked to NSA activities. The total number of staff in UTK is 186, out of which approx. 106 are assigned to the NSA function (this figure excludes all accompanying staff - HR, IT, finance etc., which is shared also with other functions).
Bulgaria	The Head of the NSA and its senior management	40-50	30-40	Prioritisation of the resources depends on the severity of the safety-related issue
Austria	The leading person of the division, or, at the	-	-	Unfortunately an approximation of the

NSA	Who has authority?	Resources used for supervision		Comments
		% of all staff	% of total budget	
	next level, the Director.			percentages is not possible.
Portugal	The Director of the Railways Department	5-10	1-5	There are not specific staff assigned to perform supervision function. Supervision is a small part of the whole tasks that staff should do.
Czech Republic	Director of NSA and the Ministry of Transport.	3-4	3-4	This percentage is from all staff, not only from NSA. NSA is only part of Drazni Urad.
Netherlands	NSA director	50	50	
Channel Tunnel	The IGC as the NSA oversees the resources; the Channel Tunnel Safety Authority agrees the inspection & audit plan; the inspectors & auditors decide on the level of activity	50-60	40-50	
Hungary	-	15-30	15-30	
Norway	The Ministry and the NSA CEO.	10-20	10-20	
Ireland	Commissioner	20-30	10-20	
France	Director-General	50	55	
Finland	The Director General of the NSA, also other managers have an influence	<1	-	
Italy	The Ministry	30-50	-	

In order to focus action at those who are best placed to control risk, NSA must be aware of which individuals carry this responsibility at each RU/IM. The vast majority of NSA state that this information is carried for all RUs/IMs and is identified in the SMS of the RU/IM and recorded against the safety certificate/authorisation (Table B.17)

3.3.6 Summary

A small majority of NSA have a strategy for supervision and the vast majority plan to implement one in due course. There are 13 NSA that target supervision activities at a national level and seven that target at the level of specific RUs/IMs; the majority of these targets are reviewed annually. Approximately three-quarters of NSA report that their supervision is 'very' or 'completely' targeted.

Key findings:

- Majority of NSA are developing or have a supervision strategy.
- NSA report their supervision is very targeted.
- Approaches and priorities for targeting supervision vary.
- Most NSA allocate less than 50% of staff and budget to supervision.

Good practice recommendations:

- Use supervision strategy to plan resourcing together with budget holder.

Some insight was gained into how NSA choose which subjects and areas should be a target for supervision. A common approach to targeting was to supervise areas that could lead to catastrophic failures. However, there were different views as to where supervision should be targeted to achieve this goal. For example, several NSA focused on supervising the maintenance of structural subsystems such as rolling stock and track) whereas as several other NSA focused on supervising the competence management of RUs/IMs and their contractors. Those NSA that supervised the maintenance of structural subsystems as a priority acknowledged that supervising the competence and contractor management for those subsystems was an intrinsic part of supervision; however, these NSA felt that ultimately an organisation could demonstrate excellent competence management but still fail to follow through and act appropriately, hence the need to focus on maintenance specifically. A few NSA had a different perspective on priorities and reported that competence management was the highest priority for their supervision activities.

Once supervision priorities are set, they have to be resourced. Or supervision priorities may be set according to the resources that are made available. A baseline good practice approach to balancing the resources that are available with the supervision targets set by an NSA would be for the NSA to:

- Consult with the budget holder (typically the Ministry) to discuss what can be achieved with the allocated resources.
- Present a case for the resourcing it needs based upon the supervision activities that are planned. Without a plan for supervision, it would be difficult for either party to determine accurately the level of resource required.

From the budget allocated to supervision activities it was clear that some NSA are not set up with supervision as their primary activity. Three NSA allocated less than 10% of budget and staff to supervision, and the majority allocated less than 50% to supervision. Whilst this is not a direct indicator of how much supervision is carried out, in some instances it did confirm that an NSA was not adequately resourced to supervise.

3.4 Supervision plans

This section discusses the supervision plans that are created by NSA; specifically how plans are developed (subsection 3.4.1), how plans are resourced (subsection 3.4.2), and how plans are reviewed (subsection 3.4.3). A summary and recommendations are provided in subsection 3.4.4.

Table 3.18 shows that, in responding to the questionnaire, all except seven NSA (Estonia, Austria, Poland, Portugal, Finland, Italy and the Czech Republic) have developed plans for supervision and enforcement that are specific to RUs/IMs. In the case of Italy, the NSA has an annual plan that gives consideration to specific RUs.

Of the 15 NSA that did produce supervision and enforcement plans for specific RUs/IMs:

- Eight NSA had plans that covered the whole life of the safety certificate or authorisation (Lithuania, Romania, Denmark, Netherlands, the Channel Tunnel, Hungary, Ireland, and France). The French plan was described as a single plan with details relating to individual RUs, rather than separate plans for each.
- Three NSA (Sweden, Germany, and Norway) had plans that covered some of the life of the safety certificate or authorisation.
- Three NSA (Spain, Latvia, and Bulgaria) had plans that were not linked to the duration of safety certificates or authorisations.
- The GB NSA did not specify whether there was a link between its plans and the validity of safety certificates or authorisations.

When asked about the extent of implementation:

- Nine NSA (GB, Sweden, Romania, Denmark, Germany, Latvia, the Channel Tunnel, Ireland, and France) implemented all of the plans that were in place, to some extent.
- Five NSA (Lithuania, Spain, Bulgaria, Netherlands, and Hungary) did not implement all plans. Specifically, Lithuania implemented a fifth of the plans it had in place, the Netherlands had a plan only for the single IM, and the Spanish and Bulgarian NSA were not sufficiently established to have a reached a point where plans were formally in place and ready to be implemented fully.

Of the NSA that have no specific plans, the Czech Republic commented that each RU/IM is supervised once during the period that the safety certificate or authorisation is valid.

Table 3.18: NSA with supervision plans for specific RUs/IMs

NSA	Develop specific supervision/ enforcement plans for RUs/ IMs?	How many RUs/ IMs have a specific plan?	How many specific plans are being executed currently?	If any or not being executed, please explain why.
Great Britain	Yes	40-60	40-60	-
Sweden	Yes – to cover some of the life of the safety	Supervises 350 RU/IM and all are subject to supervision plans.	In 2011: 11 RUs and 3 IMs. All 350 are to some degree being	Every new RU have an audit in 12 months, every new IM have a

NSA	Develop specific supervision/ enforcement plans for RUs/ IMs?	How many RUs/ IMs have a specific plan?	How many specific plans are being executed currently?	If any or not being executed, please explain why.
	certificate or authorisation	Plans involve determining when supervision should occur and, by way of a colour-coded risk summary, what areas should be supervised.	executed however.	plan for supervision. In 2011: 11 RUs and 3 IMs
Estonia	No	0	-	-
Lithuania	Yes – to cover the whole life of the safety certificate or authorisation	44	9	-
Romania	Yes – to cover the whole life of the safety certificate or authorisation	60	60	-
Germany	Yes – to cover some of the life of the safety certificate or authorisation	All	All	There is a specific plan for all RUs / IMs. All of these plans are carried out. Plans are developed for specific RUs/IMs by the people at the NSA who are assigned as their lead contacts at the NSA.
Denmark	Yes – to cover the whole life of the safety certificate or authorisation	100	100	-
Spain	Yes – but it is not linked to the duration of the safety certificate or authorisation	4	4	The specific supervision plans are not been carried out yet due to they consist of a deadline and a subsequent audit, and the deadline hasn't expire yet.

NSA	Develop specific supervision/ enforcement plans for RUs/ IMs?	How many RUs/ IMs have a specific plan?	How many specific plans are being executed currently?	If any or not being executed, please explain why.
Latvia	Yes – but it is not linked to the duration of the safety certificate or authorisation	6	6	-
Poland	No	The supervision plan for 2011 has been created on the basis of general risks identified on the railway market, not on the basis of individual risks of separate RUs and IMs. The plan has been created in the old national framework, not on the basis of the CSM approach. The national approach assumes creation of supervision plans basing on problems and issues, not performance of a specific company. We plan to shift to the new system when CSM on supervision and CSM on monitoring will enter into force.		
Bulgaria	Yes – but it is not linked to the duration of the safety certificate or authorisation	Currently, specific supervision/enforcement plans are under development. So far the supervision/ enforcement activities have been done according to general supervision/enforcement plans of RUs/IM.		
Austria	No	-	-	-
Portugal	No	0	0	-
Czech Republic	No	All RUs and IMs are supervised once in the period when the certificate is valid.		
Netherlands	Yes - to cover the whole life of the safety certificate or authorisation (for the IM)	Only for the IM There is a supervision plan for the single IM but not for any of the RUs. The NSA described it as 'too much' to have supervision plans specific to individual NSA and instead preferred a general supervision regime (based on risk analysis of the sector). However, the size and complexity of the single IM warranted a specific supervision plan.		
Channel Tunnel	Yes - to cover the whole life of the safety certificate or authorisation	1	1	
Hungary	Yes – to cover the whole life of the safety certificate or authorisation	38	26	-
Norway	Yes – to cover	0	0	-

NSA	Develop specific supervision/ enforcement plans for RUs/ IMs?	How many RUs/ IMs have a specific plan?	How many specific plans are being executed currently?	If any or not being executed, please explain why.
	some of the life of the safety certificate or authorisation			
Ireland	Yes – to cover the whole life of the safety certificate or authorisation	2	3	-
France	Yes – to cover the whole life of the safety certificate or authorisation	There is no plan by RU but there is a general framework for audits valid regardless of the RU or the IM.		
Finland	No	-	-	Trafi (the NSA) is currently developing its supervision activities thus we have not yet created any specific plans. However, the staff assessing the applications informs the supervision if there are special safety concerns.
Italy	No - (but with some doubts due to the fact that in the development of the annual supervision plan we take in consideration also the situation of each RU and of the conditions of its safety certificate but it does not exist a supervision plan	The answer is linked to the previous point: there is not a specific supervision plan for each RU but it has been foreseen in the annual plan. However, a significant number of audits are currently carried out on each RU having obtained a safety certificate in order to verify the state of implementation of the plan and the possible elimination of the conditions/prescriptions contained in the safety certificate.		

NSA	Develop specific supervision/ enforcement plans for RUs/ IMs?	How many RUs/ IMs have a specific plan?	How many specific plans are being executed currently?	If any or not being executed, please explain why.
	for each RU. It is the same for the inspection activity).			

3.4.1 Developing supervision plans

The forthcoming CSM on Supervision recommends that supervision strategies and plans have a variety of data inputs. Information can be gathered from a wide range of sources, as indicated in Table 3.19.

The 20 NSA varied in the data they used. The findings show that:

- The only consensus source of information was public complaints, which all NSA use to develop supervision plans (except France, which had none to report).
- Eight NSA (Estonia, Lithuania, Spain, Latvia, Portugal, Hungary, Norway and Finland) used all of the sources specified in the table.
- Additional sources of data specified by NSA included other RUs/IMs (Sweden), number of train kilometres covered by the company and its overall complexity (Denmark), and political issues, or those that lead to incidents such as slippery track (Netherlands).

Applicable safety regulatory framework:

CSM on Supervision (Article 8)

"2. The national safety authority shall collect and analyse information from a variety of sources. It shall use the information collected and the outcomes of supervision for the purposes set out in Article 1 of this Regulation."

Table 3.19: Data sources used to inform supervision plans

NSA	From assessing SMS	From award of a safety cert or authorisation	From previous supervision / enforcement activities	From authorisations to place subsystems or vehicles into service	From accident reports or recommendations	From Annual Reports provided by RUs/IMs	From maintenance reports provided by entities in charge of maintenance (ECMs)	From public complaints	Other	If other, please specify:
Great Britain	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	
Sweden	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Information from other RU/IM
Estonia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	
Lithuania	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	
Romania	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
Germany	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes		Remark: ECM reports not available yet. Will become a source in the future.
Denmark	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Number of train kilometres and complexity of the company.
Spain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Latvia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	
Poland	No	No	Yes	No	Yes	Yes	No	Yes	Yes	Current plans are prepared on the basis of accident data, statistics and market information.

NSA	From assessing SMS	From award of a safety cert or authorisation	From previous supervision/ enforcement activities	From authorisations to place subsystems or vehicles into service	From accident reports or recommendations	From Annual Reports provided by RUs/IMs	From maintenance reports provided by entities in charge of maintenance (ECMs)	From public complaints	Other	If other, please specify:
										They are not focused on specific companies, rather on the market as a whole. New approach to supervision is planned to be introduced with the entry into force of CSMs on monitoring and supervision.
Bulgaria	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
Austria	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
Portugal	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	From the analysis of rail incident/ accident report made by the IM
Czech Republic	Yes	Yes	Yes	No	No	No	No	Yes	No	
Netherlands	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	For example from political issues, from incidents (like slippery tracks)

NSA	From assessing SMS	From award of a safety cert or authorisation	From previous supervision/ enforcement activities	From authorisations to place subsystems or vehicles into service	From accident reports or recommendations	From Annual Reports provided by RUs/IMs	From maintenance reports provided by entities in charge of maintenance (ECMs)	From public complaints	Other	If other, please specify:
Channel Tunnel	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	
Hungary	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	
Norway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	
Ireland	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
France	Yes	Yes	Yes	Yes	Yes	Yes	No	-	Yes	The case of public complaints was never presented.
Finland	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	
Italy	Yes	Yes	Yes	No	Yes	No	No	Yes	No	

Supervision plans are generally constructed by following a risk-based approach (Table B.18). However, the methods of approaching supervision planning do vary and methods are often combined and not used exclusively:

- **Capability-based planning:** There is an intrinsic link between the assessment process and the planning of supervision after a certificate or authorisation is issued. Assessment can be founded on a judgement of RU/IM capability; supervision planning is then described as the means by which this capability is tested. Confidence in a RU/IM can influence the focus of a supervision plan—it will direct activity towards areas where there is the least confidence in a RU/IM's systems (as reported by the GB NSA). The GB OSH authority elaborates on this point by explaining how confidence in a dutyholder's management competence can be a greater consideration than the size of risk that is being controlled (e.g. a poorly managed, low hazard site may be a greater focus of a supervision plan than a higher hazard site that is adequately controlled).
- **Systematic, quantitative planning:** The Danish NSA has established a quantitative risk-based prioritisation tool for assessing the risk associated with a RU/IM and the subsequent need for supervision activity. All RUs/IMs are ranked and this determines the allocation of audit days for each RU/IM; a baseline of two

audits during the lifecycle of a certificate/authorisation is always adhered to. The allocation of audit days is then transformed into individual supervision plans for each RU/IM which are distributed over the duration of the certificate/authorisation validity. This increases the NSA's contact with the RU/IM rather than concentrating supervision activity in a single period. The process is explained in full in the NSA's strategy document which is published online. It is interesting that the Danish OSH authority has also adopted quantitative measures for planning inspections—in its case, the inspection regime is planned according to the number of employees at each RU/IM.

- **Outcome-based planning:** The GB NSA described how it had begun to utilise safety risk models that had been created for the GB rail market (this information was provided during a discussion with the Taskforce on Supervision so it is not represented in Table B.18). These models provided the precursors to accidents and, through analysis of the model, the GB NSA was exploring how it could supervise certain precursors to potentially reduce the risk of certain outcomes occurring.
- **Incident-based planning:** Statistics on incidents are often used to determine the focus of supervision (e.g. the Bulgarian and Austrian NSA). As described by the Bulgarian and Swedish NSA, this approach is a mix of proactive and reactive supervision.
- **Resource-based planning:** In its simplest form, a supervision strategy can be a calculation of how many RUs/IMs will need to be visited within a period of time to ensure they are supervised at least once, as described by the Czech and Swedish NSA. NSA may also plan supervision according to the audit topics that they check during the initial assessment (e.g. the Austrian NSA).

An alternative approach to supervision planning is to consider the duration of validity for a certificate or authorisation when it is issued. The Dutch NSA analyses the risks presented by an applicant and can refer to a risk matrix to determine whether the certificate/authorisation should be for five years or less. The validity could be reduced to as little as a year based on higher risks. This creates a clear link between the assessment process and the subsequent supervision plan. It should be noted that the NSA has separate teams carrying out assessment and supervision, so the supervision team will still introduce periodic controls during the lifecycle of a certificate/authorisation; the reduced validity is a further supervision sanction applied by the assessment team.

Planning and resourcing supervision may also require blending SMS-based supervision with national inspection regimes, established prior to the European safety regulatory framework (e.g. the Czech Republic, Poland, and Germany). NSA in the situation must manage a transition from national to European supervision regimes. This may mean that supervision planning has to include more technical inspections for markets that have not adopted fully the SMS-based approach: as the Polish NSA was quick to point out, having an SMS does not mean that an RU/IM can suddenly switch to operating in accordance with the European framework. This transition period must be planned for.

3.4.2 Resources for supervision plans

The forthcoming CSM on Supervision is expected to require NSA to allocate resources that will enable them to implement supervision and enforcement plans. Table 3.20 shows that 11 of the NSA responding to the questionnaire both estimate and allocate the required resources to deliver their supervision/enforcement plans in full. Such resources include staff time and money. With the exception of Latvia, the remainder do so at least in part. The Bulgarian NSA has initiated monthly budget reviews to ensure a fluid approach to planning funding for supervision. Its supervision activities are revised monthly in accordance with available funds (Table B.18).

Table 3.20: Estimation and allocation of NSA resources for supervision plans

NSA	Estimate resources?	Allocate resources?
Great Britain	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Sweden	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Estonia	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Lithuania	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Romania	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Germany	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Denmark	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Spain	Partly – resources are estimated to deliver some plans or plans in part	Partly – resources are allocated some plans or plans in part
Latvia	No – resources are not estimated specifically for supervision plans	No – resources are not allocated specifically for supervision plans]
Poland	Partly – resources are estimated to deliver some plans or plans in part	No – resources are not allocated specifically for supervision plans]
Bulgaria	Partly – resources are estimated to deliver some plans or plans in part	Partly – resources are allocated some plans or plans in part
Austria	-	-
Portugal	No – resources are not estimated specifically for supervision plans	Partly – resources are allocated some plans or plans in part
Czech Republic	No – resources are not estimated specifically for supervision plans	Partly – resources are allocated some plans or plans in part

NSA	Estimate resources?	Allocate resources?
Netherlands	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Channel Tunnel	Partly – resources are estimated to deliver some plans or plans in part	Yes – resources are allocated to deliver all plans in full
Hungary	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Norway	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Ireland	Partly – resources are estimated to deliver some plans or plans in part	Partly – resources are allocated some plans or plans in part
France	Yes – resources are estimated to deliver all plans in full	Yes – resources are allocated to deliver all plans in full
Finland	Yes – resources are estimated to deliver all plans in full	Partly – resources are allocated some plans or plans in part
Italy	Partly – resources are estimated to deliver some plans or plans in part	Partly – resources are allocated some plans or plans in part

3.4.3 *Reviewing supervision plans*

The forthcoming CSM on Supervision is expected to require NSA to review their specific plans for supervision and enforcement of RUs/IMs. According to the questionnaire responses that were received, the majority of NSA would carry out such a review at least once a year (seven would do so every 12 months; five would do so more often). In general, NSA that do not set a specific review point adopt a risk-based approach whereby reviews are in response to incidents or new risks emerging (Table 3.21).

Table 3.21: Reviewing supervision plans

NSA	Frequency	Comments
Great Britain	Every 12 months	-
Sweden	Other	Depends if new risks show up (risk-based)
Estonia	Every month	-
Lithuania	Other	NSA review plans under specific circumstances, such as accidents in RU, public complaints, results from previous supervision.
Romania	Every 12 months	-
Germany	Other	There is no formal requirement to do it every XX months. Depends on each case.

NSA	Frequency	Comments
Denmark	Every 12 months	-
Spain	Other	It does not apply because the supervision method (for reviewing SMS) is currently under development. We foresee review specific supervision / enforcement plans when, e.g., regulation changes.
Latvia	Every 12 months	-
Poland	Other	NSA does not prepare specific plans for any RUs/IMs. General supervision plan is drafted for one year and it covers standard fields that are subject to control in a certain year. The plan is not oriented on entities, but on certain risks. Additionally the plan can be updated as an effect of an unexpected event (e.g. accident). Sometimes there are also ad-hoc controls being taken.
Bulgaria	Every three months	The supervision/ enforcement plans are common for all RUs/IM and they are reviewed and reported every three months
Austria	Other	As the supervision/enforcement plans are still in development no concrete answer can be given. It is planned to review them every 6 months.
Portugal	Never	Up to now there were not specific supervision/enforcement plans for RU/IM
Czech Republic	Never	-
Netherlands	Every 12 months	
Channel Tunnel	Every six months	
Hungary	Every 12 months	-
Norway	Every 12 months	-
Ireland	Every three months	Possibly more but as stated earlier not all reviews are always recorded.
France	Other	There is no specific plan for RU but there is a general framework for audits valid regardless of the RU or the IM.
Finland	Other	We don't have specific supervision plans for each stakeholder.
Italy	Every three months	When the annual audit plan is drawn up a specific review is made; in any case, every three months the plan is subjected to a revision in order to monitor its implementation state and the goal of the fixed targets or to plan again when necessary.

Upon reviewing specific supervision/enforcement plans for RUs/IMs, NSA have reported taking a variety of different actions (Table B.19). In order of most to least common, the actions NSA would take are:

- Change the activities targeted by the supervision plan (14 NSA)
- Change the resources allocated in the plan to specific RUs/IMs (8 NSA)
- Change the data collected by the plan (7 NSA)
- Change the entire plan (6 NSA)
- Change the general supervision/enforcement strategy of the NSA (3 NSA)
- Recommend a change in state legislation (3 NSA)
- Share outcomes of the review with other NSA (2 NSA)
- Inform the Agency of the outcomes of the review (1 NSA)

Austria, Portugal, Spain and the Czech Republic would take none of these actions; it is possible that this is due to a lack of experience of implementing and reviewing such plans.

3.4.4 Summary

In summary, the majority of NSA (15) have supervision plans that relate to specific RUs/IMs. About half of these plans cover the periodicity of the safety certificate or authorisation for the target RU/IM. One NSA described a distributed approach to supervision where the audit days assigned to an RU/IM would be spread over the periodicity of the certificate/authorisation so that the NSA would have more than one opportunity to assess an RU/IM.

Supervision plans can be developed using a variety of inputs and are generally constructed following a risk-based approach. Five different approaches were identified during this study. Two of these approaches focus on assessing the risks associated with a specific RU/IM: the first approach is capability-based and it requires the NSA to judge its confidence in the RU or IM to manage its risks; the second approach is systematic and quantitative and it scores the relative risk presented by different aspects of an RU or IM (one of these aspects is the NSA's confidence in the RU/IM's capability). These approaches to supervision planning are predominantly proactive.

Key findings:

- Three-quarters of NSA have supervision plans for specific RUs and IMs.
- Supervision plans may be based on judgement and/or systematic assessment of an RU or IM's capability and relative risk.
- Plans may also be based on frequency of previous incidents or their precursors.
- Plans are occasionally set based on even distribution of resources.
- Specific plans are typically reviewed annually or in response to data and/or incidents.

Good practice recommendations:

- At the very least, supervision planning should be informed by incident data (a reactive approach).
- Supervision plans should ideally be based on an assessment of RU/IM capability (a proactive approach).
- More systematic assessment of the relative risks of RUs/IMs is desirable for planning supervision.
- Supervision should not be planned on available resources only.
- Planned supervision can be distributed over the periodicity of the certificate/authorisation to increase contact with the RU/IM.

Two further approaches are led by data. NSA that engage in incident-based planning will review accident and near-miss statistics for the market and set supervision plans accordingly. This type of supervision planning is predominantly reactive. A more advanced approach is to use outcome-based planning which relies on data models to identify the potential precursors to such incidents. These precursors can then be incorporated into supervision plans.

A final approach to supervision planning is to simply distribute available resources evenly across the RUs and IMs that require supervision.

Figure 3.4 shows a good practice structure for planning supervision. It includes the five inputs to supervision plans that were discussed with the Taskforce on Supervision. It was agreed with the Taskforce that the ideal approach to supervision would be primarily driven by an assessment of RU/IM capability and relative risk, with secondary inputs from an assessment of incidents and/or their precursors. The Taskforce agreed that supervision should not be planned according to how resources can be distributed.

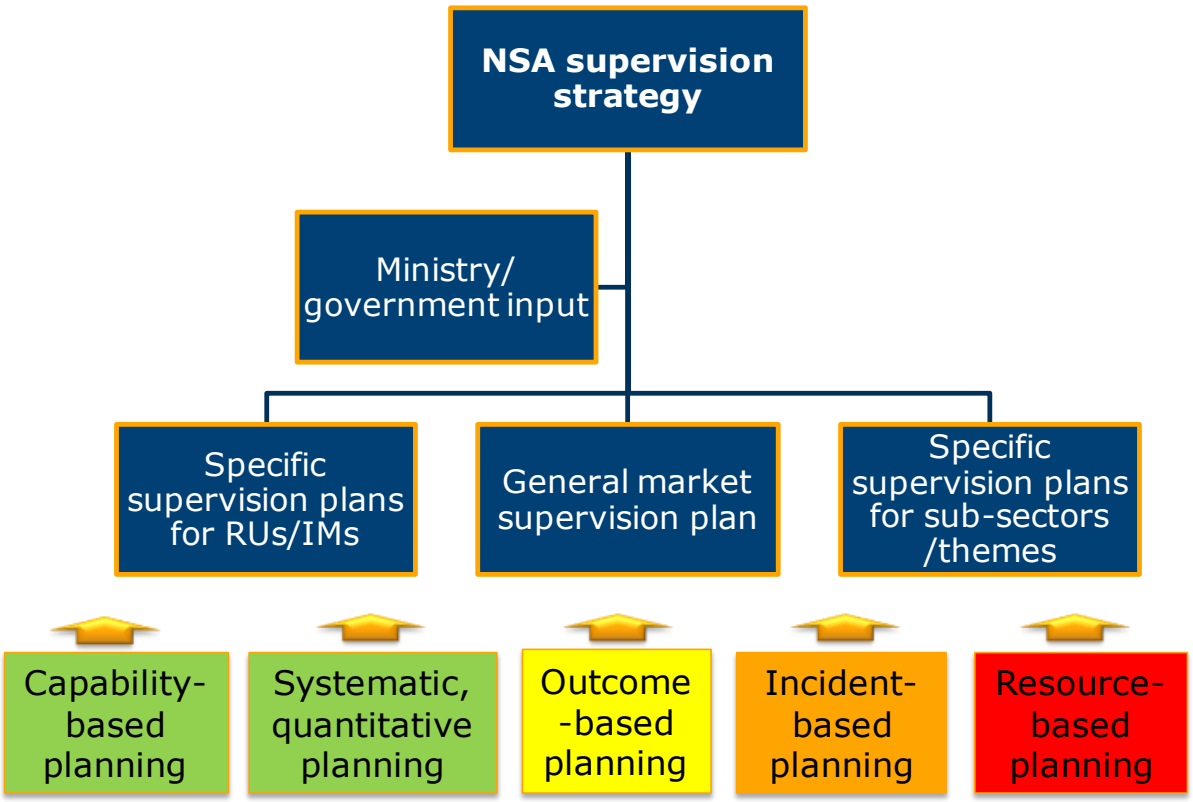


Figure 3.4: Good practice structure for planning supervision

Specific supervision plans are often reviewed annually or more frequently; however, several NSA would update plans if an incident or new information required changes. Action taken to update plans was most commonly to change the activities targeted by the plan.

Therefore, to achieve baseline good practice it is recommended that NSA:

- Plan supervision based on an assessment of RU/IM capability.
- Supplement supervision planning by reviewing relevant incident data.

Further good practice could be demonstrated by NSA if they were to:

- Consider distributing planned supervision activities across the periodicity of the certificate/ authorisation to allow more regular supervisory contact with RUs/IMs.
- Implement a systematic, quantitative approach to assessing the capability of an RU/IM, and its risk relative to other RUs/IMs and use this to plan supervision.
- Access models of incident precursors to plan supervision that will address the events and actions that are believed to lead to incidents.

3.5 Supervision practices

This section discusses NSA supervision practices. The subsections are arranged to cover specifically: the frequency of methods used for supervision and enforcement (3.5.1); the frequency and type of checks on the SMS for RUs/IMs (3.5.2–3.5.6); how information is used to benchmark supervision and enforcement activities (3.5.7); and proactive and reactive supervision practices (3.5.8).

A summary and recommendations are provided in subsection 3.5.9.

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV) and 1169/2010 (Annex III):

All principles may apply.

CSM on Supervision (Article 4)

"The NSA shall adopt techniques for supervision activities. Common elements of these techniques are: interviews with people at different levels in an organisation, reviewing documents and records related to the safety management system and examining the safety outcomes from the management system through inspections or related activities.

2. The NSA in its supervision role shall ensure that it conducts

(a) activities checking the effectiveness of the safety management system; and

(b) activities checking the effectiveness of individual or partial elements of the safety management system, including operational activities."

3.5.1 Frequency of supervision and enforcement methods

There is considerable variation in the frequency with which the various methods of supervision are utilised by NSA. The CSM on Supervision and the guidance that accompanies it discusses how supervision practices should be a combination of interacting with staff at an RU/IM (carrying out interviews and discussing documents and procedures) as well as on-site observations, document reviews and analysis of SMS outcomes.

Twelve NSA use all the primary supervision methods (interviews with staff at all levels, document reviews and analysis of SMS outcomes) with some regularity (Table 3.22). No NSA utilises all the methods listed in the table as frequently as the GB NSA. However, the 11 other NSA do use all the methods listed at least as frequently as every 18 months (Romania, Denmark, Latvia, Bulgaria, Portugal, Channel Tunnel, Hungary, Norway, Ireland, France and Italy).

Two NSA (Sweden, Germany) described a risk-based approach where the frequency with which they supervise using the methods listed is not uniform.

The NSA of the Czech Republic and Lithuania only check the SMS once, after the maximum five-year period of validity has passed.

The Spanish, Finnish and Polish NSA appear to be in the infancy of the supervision process, with Spain at the stage of planning audits and Poland not having reached a point where it has reviewed an SMS.

It would seem that baseline good practice is to check the whole SMS at least once in a five-year period of validity for a safety certificate/authorisation, with further good practice demonstrated by more frequent checks.

Table 3.22: Frequency with which supervision methods are used by NSA

NSA	Interviews with staff	Interviews with (SMS) manager	Review SMS documents/ records	Examine outcomes from SMS	Comments
Great Britain	Every month	Every month	Every month	Every month	
Sweden	Other	Other	Other	Other	NSA use risk-based supervision. You never meet everybody, it depends on activity and risk. Some RU/IMs you can meet often, and some you can meet more seldom.
Estonia	Other	Every month	Every month	Every 12 months	NSA will interview appropriate staff at the RU/IM including operational staff and senior management, when it becomes necessary.
Lithuania	Other	Other	Other	Other	NSA checks 5 years after issuing the safety certificate and authorisation.
Romania	Every 12 months	Every 12 months	Every two years	Every 12 months	
Germany	Other	Other	Other	Other	Depends on each individual case, can hardly be answered 'on average'.
Denmark	Every 12	Every 12	Every 12	Every 12	

NSA	Interviews with staff	Interviews with (SMS) manager	Review SMS documents/ records	Examine outcomes from SMS	Comments
	months	months	months	months	
Spain	Other	Other	Other	Other	The audit guide, which is currently under development, will include terms and frequency of the methods adding to audit plans guidelines. Though the matter has to be set, it is estimated to conduct an audit for each RU/IM every 18 months or 2 years. Regardless of the inspections that are delegated to ADIF.
Latvia	Every 12 months	Every 12 months	Every 12 months	Every 12 months	
Poland	Other	Other	Other	Other	See below:
There's no systemic approach to supervision and enforcement in line with CSM requirements yet. The inspection regime based on the old national requirements still plays key role, as the supervision plans for the year 2011 were defined on its basis. The inspections through SMS have just been launched and they exist in parallel with the typical inspection activities. Statement 1: System of market players supervision through the SMS has been established at the beginning of 2011 and works for just 11 months now. Use of the interviews is linked rather with different problems that the NSA identifies than with the defined schedule. It's also limited by the resources we have. Statement 2: The NSA takes part in systematic SMS Managers meetings, organized at least twice a year. Due to limited resources, bilateral meetings are not common. Statement 3: Till now we've never conducted a review of SMS documents or records. This kind of work is foreseen for the future, now we are still dealing with amendments to SMS on the basis of relevant applications from companies. These amendments have to be accepted by our NSA (divergence between the EU and national					

NSA	Interviews with staff	Interviews with (SMS) manager	Review SMS documents/ records	Examine outcomes from SMS	Comments
law). Statement 4: We started examining general outcomes from SMS this year, but due to lack of resources and competences the number of such activities was very limited. Still most of the supervisory activities took the form of inspections not directly linked with SMS.					
Bulgaria	Every three months	Every month	Every 12 months	Every month	
Austria	Other	Other	Other		Currently supervision is done when issuing a SC/SA, or if necessary due to specific circumstances (e.g. incident). In Austria - before issuing a part A by the NSA- a certificate of an accredited body is necessary for the SMS by law. This includes a yearly audit of the SMS during the validity.
Portugal	Every 12 months	Every 12 months	Every 18 months	Every 12 months	
Czech Republic	Never	Other	Other	Other	Once in 5 years.
Netherlands	Other	Other	Other	Other	Our relation towards the IM and towards the RUs differ. We visit the RUs every 3 years. The contacts between us and the IM are more

NSA	Interviews with staff	Interviews with (SMS) manager	Review SMS documents/ records	Examine outcomes from SMS	Comments
					frequent.
Channel Tunnel	Every three months	Every three months	Every three months	Every three months	
Hungary	Every 12 months	Every 12 months	Every 12 months	Every 12 months	
Norway	Every 18 months	Every 18 months	Every 18 months	Every 18 months	These questions are difficult to answer since our supervision plans are risk-based, and RU/IM are not supervised on a defined frequency.
Ireland	Every three months	Every three months	Every three months	Every three months	
France	Every 12 months	Every 12 months	Every 12 months	Every 12 months	
Finland	Other	Other	Other	Other	It depends on RU/IM. Due to the new organisation no average known yet.
Italy	Every 12 months	Every 12 months	Every 12 months	Every 12 months	
It has been foreseen to carry out at least one audit per year on each RU. The documentation review is carried out during the audit (so, at least once a year also if not all the documentation can be subjected to an audit). The frequency of this review can be increased according to any kind of modification or request to update the certification (it depends on the typology of modification or request of updating). Referring to the SMS data, some of them (indicators) are monitored every three months, other kinds of data every six months (i.e. the data about the safety management system status of progress), some different data once a year (i.e. the annual safety report).					

3.5.2 *Frequency of checking effectiveness of SMS for RUs/IMs*

The forthcoming CSM on Supervision will specify that NSA should have a supervision strategy that ensures they check the effectiveness of the SMS for RUs/IMs as a whole

and in individual parts. It is anticipated that partial checks will be undertaken during the validity of a safety certificate or authorisation in order to supervise targeted elements. This approach is thought to be of greatest benefit to NSA with a small workforce and/or a large market as it enables a supervision to cover a wider range of the market over a shorter period of time.

Few NSA have fixed intervals between whole and partial checks of the SMS for each RU and IM. It is not likely that fixed intervals would be suited to all RUs/IMs so this finding supports an adaptive approach to supervision that is based on the activities and capabilities of RUs/IMs. A broad range of intervals and approaches have been adopted when checking the effectiveness of the SMS for RUs and IMs.

From the questionnaire responses (Table 3.23), it is evident that all NSA check the whole SMS for each RU/IM at least every five years (which coincides with the maximum validity of a safety certificate or authorisation). The exceptions at the moment appear to be Romania, Spain, Poland and Portugal which, to date, have not yet started (or have only recently started) SMS supervision and so have not completed any formal checks of an SMS. Spain and Poland both plan to check the whole SMS of each RU/IM at least very two years and propose to conduct partial checks in response to specific concerns or as appropriate.

The planned checks for the other NSA, in order of frequency, are as follows:

- Estonia and Bulgaria – whole SMS checked yearly, parts checked monthly. Most frequent levels of checks.
- Latvia and Hungary – yearly checks for both whole and parts of SMS.
- Norway – checks every 18 months for both whole and parts of SMS.
- Germany – whole SMS checked every 2 years. Parts of SMS checked on a fluid basis.
- Sweden and the Channel Tunnel – both have a fully fluid approach to whole and partial checks of the SMS. The Finnish NSA has also adopted a fluid process that is based on the size of the RU/IM, with the smallest possibly being checked only once in five years and the largest annually.
- Ireland – checks the whole SMS every 3–5 years (when the validity of the certificate or authorisation expires) and parts every 3 months.
- Denmark and France – checks the whole SMS every 5 years and parts of the SMS every 12 months. Italy appears to be implementing a similar approach.
- GB – checks the whole SMS every 5 years and parts of the SMS on a fluid basis.
- Lithuania and the Czech Republic – check both the whole SMS and individual parts every 5 years.
- The Austrian NSA stated that, by law, the SMS for any operator must be certified by an accredited body – and the certification process requires yearly audits of the SMS to remain valid. It is, however, worth exploring whether that legitimately divests the Austrian NSA of some of its responsibility for checking the SMS.

Table 3.23: Frequency of SMS audits

NSA	Check WHOLE SMS	Check INDIVIDUAL PARTS of SMS?	Comments
Great Britain	Other	Every 12 months	Taking the main IM as an example the SMS is fully evaluated every 5 years with individual sections examined frequently in the intervening periods. Our annual work plans will set out the evaluation requirements for each RU/IM.
Sweden	Other	Other	NSA use risk-based supervision. You never meet everybody, it depends on activity and risk. Some RU/IMs can you meet often, and some you can meet more seldom.
Estonia	Every 12 months	Every month	
Lithuania	Other	Other	NSA checks the effectiveness of the whole SMS and/or individual parts 5 years after issuing the safety certificate and authorisation.
Romania	Never	Never	The legislation for the RUs audit, amending the Order of the Minister of Transports no. 535/2007, is in approval course. The legislation for the IMs audit, amending the Order of the Minister of Transports no. 101/2008, will be changed.
Germany	Every 2.5 years	Other	For the whole SMS, there is an audit at the time of the first assessment, there is an audit part-way through the 5-year validity and there is a further audit at the point of reassessment. This may be a full audit or it may be distributed to cover different parts of the RU/IM at different times. For individual parts, this can hardly be answered on average as these could be follow-ups after a full audit or an incident.
Denmark	Other	Every 12 months	We review the effectiveness of the whole SMS within the certificate / approvals duration and when renewed.
Spain	Other	Other	It is expected the effectiveness of the whole SMS to be checked every 18 months or 2 years. This estimated is based on the number of RUs/IMs and the number of staff available

NSA	Check WHOLE SMS	Check INDIVIDUAL PARTS of SMS?	Comments
			for audits. The effectiveness of the individual parts of the SMS will be checked in response to specific concerns/incidents.
Latvia	Every 12 months	Every 12 months	
Poland	Other	Other	As the system of supervision via SMS isn't fully in force right now, we can share only our plans in this field. Frequency of these activities depends on our resources (number of staff and their availability) as currently the staff responsible for supervision deals also with other tasks, like issuing certificates, safety reporting etc. It's also related to the number of undertakings on the market (currently more than 60). Our plans in this field are following: 1. Effectiveness of whole SMS: every two years. 2. Effectiveness of parts of the SMS: when needed, generally at least once within 1 - 2 years.
Bulgaria	Every 12 months	Every month	
Austria	Other	Other	In Austria -before issuing a part A by the NSA- a certificate of an accredited body is necessary for the SMS by law. This includes a yearly audit of the SMS during the validity.
Portugal	Never	Every 18 months	Never - Has not performed yet because the safety certificates and authorisation are quite recent but we will do it in coming years.
Czech Republic	Other	Other	Once in 5 years.
Netherlands	Other	Other	
Channel Tunnel	Other	Other	Effectiveness is checked through planned inspections and audits through the lifespan of the authorisation.
Hungary	Every 12 months	Every 12 months	

NSA	Check WHOLE SMS	Check INDIVIDUAL PARTS of SMS?	Comments
Norway	Every 18 months	Every 18 months	
Ireland	Other	Every month	Check parts every 3 months but annual statistical review looks at safety performance. Whole SMS would be over the periodicity of the safety cert or authorisation (3 years for IE and RPSI). Individual parts checked with inspections, audits, etc.
France	Other	Every 12 months	The notion of "individual part" does not exist in the regulations. We interpret this as "great theme" contained in a file security (technical rules and maintenance of rolling stock, control of suppliers and subcontractors, and professional fitness training. At least a systematic audit is conducted every year with the RU / IM on a theme that changes each year (based on five themes contained in a file security). With this principle, the SMS is "controlled" in its entirety every five years. After issue of the safety certificate, the RU is the subject of an initial audit within 6 months after the first train traffic.
Finland	Other	Other	Depends on RU/IM. The biggest companies once a year, the smallest once in five years.
Italy	Other	Every 12 months	Following our experience, if no modification has occurred the whole SMS has been checked at the expiry of the safety certificate. It has been foreseen to carry out at least one audit/follow-up per year on each RU.

3.5.3 Value of checking individual parts of an SMS

Table 3.24 shows that, of the 20 NSA responding to the questionnaire:

- Ten NSA found it 'very useful' to check individual parts of an RU or IM's SMS as it provided a good insight into the general safety culture of the organisation.
- The remaining NSA that responded also appreciated this benefit, but attached less value to it, particularly the NSA of the Czech Republic.
- Denmark was the exception – its NSA did not see this approach as being useful in any way as it does not provide objective confirmation that the whole SMS meets the required standards.
- The French NSA did not fully recognise the concept of partial checks.

Table 3.24: Usefulness of partial SMS audits

NSA	Usefulness	Other/comments
Great Britain	Quite useful	It gives an indication of how the RU/IM is performing and their attitude towards seeking compliance.
Sweden	Very useful	It shows easily, as verification, how the RU/IM is working with the whole SMS. Is it known out in production or is only known by management.
Estonia	Quite useful	
Lithuania	Very useful	Checking individual parts of an SMS can define what should be changed in whole SMS.
Romania		
Germany	Quite useful	
Denmark	Not at all useful	To check a part of a safety management system will not provide an objective testimony about, if the rest of the RU/IM is in compliance
Spain	Quite useful	It may be useful when it is not possible to check the whole SMS effectiveness (as alternative measure).
Latvia	Very useful	
Poland	Very useful	In our opinion, although not based on the practice yet, it is very useful because this enables deeper insight into the SMS.
Bulgaria	Very useful	Checking the individual parts of the SMS of a RU/IM is very useful because it enables the NSA to have a clearer estimation for the implementation of the procedures and interrelations described in the SMS.
Austria	-	Concerning certification by accredited bodies.
Portugal	Very useful	Is useful because they are a sample of the whole SMS, and if an individual part is not working properly than is may be a symptom the organisation is not caring about the SMS, and more in-depth assessment is required.
Czech Republic	Slightly useful	It is only example.
Netherlands	Quite useful	
Channel Tunnel	Very useful	Targeted at specific areas to allow in depth analysis.
Hungary	Quite useful	
Norway	Very useful	
Ireland	Very useful	It is indicative of company, if system issues are identified in a part it is probably company wide.

NSA	Usefulness	Other/comments
France	-	Concept does not exist in regs. All parts of the SMS are important and are audited over a period of 5 years.
Finland	Quite useful	
Italy	Very useful	

3.5.4 Methods of checking effectiveness of the whole SMS

Table 3.25 shows that, of the 20 NSA:

- Seven used a minimum combination of audits, staff interviews and investigations to check the effectiveness of the whole SMS for an RU/IM.
- Several NSA supplemented their approach with inspections. Ireland reported supervision meetings with RU and IM management.
- Four NSA (Estonia, Romania, Finland and Italy) did not carry out interviews with staff, which essential highlighted as an element of effective supervision in the CSM on Supervision.
- Poland has not yet gained experience of applying these methods so its NSA responded based on intentions.

Table 3.25: Methods used to check the whole SMS of an RU/IM

NSA	Audit	Interviews with staff	Investigation	Other	Other, please specify:
Great Britain	Yes	Yes	Yes	Yes	Inspections.
Sweden	Yes	Yes	No	Yes	Interview with sub-contracted.
Estonia	Yes	No	No	No	But EE NSA doesn't name it 'audit', it named it 'supervision'.
Lithuania	Yes	Yes	Yes	No	-
Romania	Yes	No	No	No	Legislative draft.
Germany	Yes	Yes	Yes	Yes	Other comprises inspections, I do not know if this is meant to be included in 'investigation'.
Denmark	Yes	Yes	Yes	No	A mix of the above.

NSA	Audit	Interviews with staff	Investigation	Other	Other, please specify:
Spain	Yes	Yes	No	No	-
Latvia	Yes	Yes	Yes	No	-
Poland	Yes	Yes	No	Yes	Till now we haven't practiced it. We plan to use different methods, depending on staff availability and competence. We also plan to review documentation created on the basis of the SMS, carry out audits and interviews.
Bulgaria	Yes	Yes	No	No	-
Austria	Yes	Yes	No	No	Concerning certification by accredited bodies.
Portugal	Yes	Yes	No	No	-
Czech Republic	Yes	Yes	No	No	-
Netherlands	Yes	Yes	Yes	Yes	Inspections.
Channel Tunnel	Yes	Yes	No	No	
Hungary	Yes	Yes	Yes	No	
Norway	Yes	Yes	No	No	
Ireland	Yes	Yes	No	Yes	Supervision meetings with RU and IM management. Sample asset inspections.
France	Yes	Yes	No	Yes	Inspections. The interviews are included in the audits and inspections.
Finland	Yes	No	No	No	-
Italy	Yes	No	Yes	Yes	Audit includes document review. Investigation is interpreted as inspection.

3.5.5 Methods of checking effectiveness of individual parts of an SMS

Of the 20 NSA responding to the questionnaire, Table 3.26 shows that:

- Six used a minimum combination of audits, staff interviews and investigations to check the effectiveness of individual parts of an SMS for an RU/IM.
- Several NSA supplemented their approach with inspections and, in the case of Ireland, supervision meetings with RU and IM management.
- Four NSA (Estonia, Romania, Poland and Italy) did not carry out any interviews with staff. This means that three NSA (Estonia, Romania and Italy) apparently do not interview any staff when carrying out SMS assessments. Poland has not yet gained experience of applying these methods so its NSA responded based on intentions.

Table 3.26: Methods used to check individual parts of an SMS of an RU/IM

NSA	Audit	Interviews with staff	Investigation	Other	Other, please specify:
Great Britain	Yes	Yes	Yes	Yes	Inspections.
Sweden	Yes	Yes	No	Yes	Interview with sub-contracted.
Estonia	No	No	No	Yes	Ordinary supervision.
Lithuania	Yes	Yes	Yes	No	-
Romania	Yes	No	No	No	Legislative draft.
Germany	Yes	Yes	Yes	Yes	Other comprises inspections, I do not know if this is meant to be included in 'investigation'.
Denmark	Yes	Yes	Yes	No	A mix of the above.
Spain	Yes	Yes	Yes	No	-
Latvia	No	Yes	Yes	No	-
Poland	No	No	Yes	Yes	Till now we haven't practiced it. We plan to use different methods, depending on staff availability and competence. In some cases on site visits are planned.
Bulgaria	No	Yes	No	Yes	Thorough inspections.
Austria	Yes	Yes	No	No	Concerning certification by

NSA	Audit	Interviews with staff	Investigation	Other	Other, please specify:
					accredited bodies.
Portugal	Yes	Yes	No	No	-
Czech Republic	Yes	Yes	No	No	-
Netherlands	Yes	Yes	Yes	Yes	Inspections.
Channel Tunnel	Yes	Yes	No	No	
Hungary	Yes	Yes	Yes	No	-
Norway	Yes	Yes	No	No	-
Ireland	Yes	Yes	No	Yes	Supervision meetings with RU and IM management. Sample asset inspections.
France	Yes	Yes	No	Yes	Inspections. The interviews are included in the audits and inspections.
Finland	Yes	Yes	No	No	-
Italy	Yes	No	Yes	Yes	Audit includes document review. Investigation is interpreted as inspection.

3.5.6 Circumstances for partial checks of an SMS

All NSA except Norway would conduct a partial check of the SMS in response to specific safety concerns. NSA were invited to consider other reasons in the questionnaire (Table B.20):

- Except for Norway, none would carry out a partial check to save time, although six NSA would to ensure that more RUs/IMs can be checked within a certain period, which has similar time-saving attributes.
- None would carry out a partial check to save money.
- Ireland carries out partial checks in response to public complaints.

3.5.7 Use of information for benchmarking supervision/enforcement

Table 3.27 shows that, with the exception of Poland and the Czech Republic, all NSA responding to the survey use additional information to assist with benchmarking their supervision and enforcement of an RU or IM's SMS:

- 12 NSA (Sweden, Estonia, Lithuania, Germany, Austria, Portugal, Netherlands, the Channel Tunnel, Hungary, Ireland, Finland and Italy) use the performance and activities of similar RUs/IMs.
- 16 NSA (Sweden, Lithuania, Romania, Germany, Denmark, Spain, Latvia, Bulgaria, Austria, Portugal, the Channel Tunnel, Hungary, Norway, Ireland, Finland and Italy) use the information provided during the assessment/reassessment of an application for a safety certificate or authorisation.

In addition, Sweden and Portugal use incident and safety information (e.g. collected from the NIB or annual safety reports).

The GB NSA benchmarks its SMS supervision on the safety standards that are specified by regulators.

Table 3.27: Information used to benchmark supervision and enforcement

NSA	Use additional info?	Performance/ activities of a similar RU/IM	Information from application/ reassessment of a safety certificate or authorisation	Other, please specify:
Great Britain	Yes	No	No	Safety standards as specified by regulators and NSA
Sweden	Yes	Yes	Yes	Information from NIB
Estonia	Yes	Yes	No	-
Lithuania	Yes	Yes	Yes	-
Romania	Yes	No	Yes	-
Germany	Yes	Yes	Yes	-
Denmark	Yes	No	Yes	-
Spain	Yes	No	Yes	Information gathered during application/reassessment of a safety certificate or authorisation is what it is expected to be used for benchmarking the supervision.
Latvia	Yes	No	Yes	-

NSA	Use additional info?	Performance/ activities of a similar RU/IM	Information from application/ reassessment of a safety certificate or authorisation	Other, please specify:
Poland	No	No	No	-
Bulgaria	Yes	No	Yes	-
Austria	Yes	Yes	Yes	-
Portugal	Yes	Yes	Yes	Analysis of the daily incident/accident reports, Annual Safety Report.
Czech Republic	No	No	No	-
Netherlands	Yes	Yes		This answer does not apply to the IM as there is only one in NL.
Channel Tunnel	Yes	Yes	Yes	-
Hungary	Yes	Yes	Yes	
Norway	Yes	No	Yes	
Ireland	Yes	Yes	Yes	
France	-	-	-	
Finland	Yes	Yes	Yes	
Italy	Yes	Yes	Yes	

When supervision activity identifies an incidence of non-compliance, NSA will issue some requirement for this non-compliance to be addressed. It is encouraging that all NSA stated that they would review non-compliances at least sometimes (the exception was Spain although this may be because its NSA is newly established and has little or no experience in this area). The majority of NSA (12) specified that they would always check whether a non-compliance had been addressed (Table 3.28). Those NSA that may check only sometimes make that decision based on the severity of the non-compliance and/or the resources they have available to carry out the follow-up checks. The majority of NSA would typically follow-up a non-compliance within 4 weeks, although several did state that it would depend on the severity of the non-compliance.

Table 3.28: Reviewing non-compliances in an SMS

NSA	Review whether non-compliance has been addressed?	After how many weeks typically?	Under what circumstances?
Great Britain	Yes - always	3	Always for an enforcement notice. Other issues will be decided on based on the level of risk perceived by the NSA.
Sweden	Yes - always	2 – 4 weeks	-
Estonia	Yes - sometimes	2	It depends on how serious was the non-compliance.
Lithuania	Yes - always	1 week	NSA always reviews whether non – compliance issues have been dealt with effectively.
Romania	Yes - always	1	Depending on severity of the issues.
Germany	Yes - sometimes	No fixed number and no sensible average - it depends on each individual case	It is really depending on severity of the issue and the resources available.
Denmark	Yes - sometimes	?	We approve proposals for action plans and follow up on later review.
Spain	No	-	-
Latvia	Yes - always	4	NSA tries to do it always.
Poland	Yes - sometimes	We check this during additional controls that are performed usually after the deadline set by the NSA to correct the RU / IM activity. The review lasts usually 1 - 2 weeks.	In case of identifying serious non-compliances current system entitles NSA to carry out additional controls to check if its recommendations have been implemented. Usually the recommendations cover what has to be done. Amount of time taken depends on resources and importance of a certain case. We do not perform all necessary additional controls due to lack of human resources, that are not adjusted to market needs (20 000 km of the network, about 60 certified undertakings and more than 1500 sidings that we also supervise).
Bulgaria	Yes - always	4 weeks	It depends on the severity of the safety-related issue.

NSA	Review whether non-compliance has been addressed?	After how many weeks typically?	Under what circumstances?
Austria	Yes - always	This entirely depends on the measures, mostly because the measures issued already include a time frame until which the non-compliance has to be dealt with. This time frame depends among others on the urgency, the amount of work involved and the type of work.	
Portugal	Yes - sometimes	4	Severity of the issue and resources available.
Czech Republic	Yes - always	Not defined	The application is not complete.
Netherlands	Yes - always	That depends on the kind of non-compliance. It varies from a few hours to a few years.	We always do.
Channel Tunnel	Yes - always	Depends on circumstances	Dependent on severity of issue.
Hungary	Yes - always	4	During the yearly audit or if the severity of the issue is big than immediately.
Norway	Yes - sometimes	4 to 6	If they are very critical, or when the response from the RU/IM is not fully satisfactory or clear.
Ireland	Yes - sometimes	1 - 2 weeks	Both the above severity and resource.
France	Yes - always	-	Inspections can be triggered specifically by severity, to verify that the resolution of non-compliance is effective.
Finland	Yes - sometimes	2 to 4	It depends on available resources.
Italy	Yes - always	1 week	Always.

3.5.8 Supervision practices: proactive and reactive supervision

Table B.21 provides examples of one distinction that exists in supervision activities. This distinction is between 'proactive' supervision (which is typically described as planned activity) and 'reactive' supervision (which is typically the response of an NSA to incidents or safety risks that occur). A sample of findings from the NSA interviews reveals variation in the proportion of an inspector's time that is allocated to proactive supervision. The proportion of time allocated to proactive supervision is:

- 50% for the GB and Swedish NSA.
- 75% for the Spanish NSA.
- 80% for the Czech, Bulgarian, German and Danish NSA (for Denmark see Table B.21).
- 90% for the Austrian NSA.

The Bulgarian NSA does not make a formal distinction between proactive and reactive supervision but it is assumed that a minimum of 20% of activity is reactive in that inspectors spend this time reviewing incident data.

The Spanish NSA stated that reactive inspections may be considered 'aggressive' by its RUs/IMs. The NSA wished to avoid being perceived in this way in case it hindered its current efforts to work with RUs/IMs to improve their compliance with the European regulations.

In summary, the proportion of time allocated to proactive supervision will likely vary; however, 50% of inspection time spent on proactive supervision is a desirable minimum balance given the intended role of NSA according to the European framework. There is an argument that a greater focus on proactive supervision will produce a marketplace that is responsible for its own safety and effectively reduces the number of incidents that require a reactive response. Clearly, the frequency of events requiring reactive inspections will affect the delivery of any proactive targets. Nevertheless, the Swedish NSA (which currently has an equal balance) recognised that there were benefits to a proactive approach and wanted to 'be out there more' supervising the market proactively. It is therefore recommended that:

- Resources for inspection are sufficient to permit at least 50% of the time allocated to inspections to be spent on proactive inspections.
- The allocation of resources for proactive and reactive supervision is a set goal that is defined in the NSA strategy.
- If all reactive inspections account for less than 50% of the overall time allocated for inspections, the proportion of time spent on proactive inspections should increase accordingly.
- A goal for an NSA would be to have proactive inspections accounting for 80% of all time allocated to inspections, whilst still being able to reactively inspect and investigate cases as necessary.

3.5.9 Summary

The forthcoming CSM on Supervision is expected to require NSA to use a range of supervision methods (interviews with all levels of staff, document reviews, examining SMS outcomes). Most NSA already use this range of methods with some regularity. The regulation is also expected to require NSA to consider how they will check the effectiveness of each SMS as a whole and in individual parts, where appropriate. No NSA reported that it would check the effectiveness of the whole SMS for an RU/IM more frequently than once every year — and all NSA would do so at a maximum of every five years (coinciding with the maximum validity of a certificate/authorisation). Partial checks are every 3–12 months, or on a fluid basis according to risks and incidents. NSA generally agreed that a partial check of an SMS was at least 'quite useful'; several of those in favour of partial checks reported that it did enable NSA to check more RUs/IMs within a certain period of time, or to respond to specific public complaints. However, a couple of NSA noted that such checks were not a reliable, objective indicator of the performance of the SMS in its entirety.

There was little difference in the methods used for full and partial checks of an SMS: on the evidence provided, a good practice approach would be to use a minimum combination of audit techniques, interviews with staff at all levels, investigative techniques (e.g. examination of documented SMS outcomes) and inspections (e.g. to observe first-hand the operational performance of the RU/IM). In addition, half of NSA used the performance and activities of similar RUs and IMs as a benchmark for supervision of specific RUs/IMs, and almost three-quarters of NSA use information from assessment/reassessment as a benchmark.

Just over half of NSA always check that non-compliances identified during supervision have been rectified, with the remaining NSA typically deciding whether to follow-up based on the severity of the non-compliance.

NSA typically direct 50-90% of the time allocated to inspections to proactive inspections. Reactive inspections account for the remaining percentage.

Key findings:

- Most NSA use a range of supervision methods (interviews, document reviews, examining outcomes) at least every 18 months. Just over half of NSA do so more regularly.
- Whole SMS checks occur every 1–5 years; partial checks are ad hoc or every 3–12 months.
- Partial SMS checks are at least 'quite useful' but are not an objective indicator of the whole SMS.
- Non-compliances were generally followed up, especially if severe.
- 50–90% of inspections for supervision are proactive.

Good practice recommendations:

- Proactive inspections should be a focus of supervision and account for at least 50% of allocation (ideally 80%)
- NSA to audit using a minimum combination of document checks, interviews with a range of staff and frontline inspections.
- Check the whole SMS for each RU/IM at least once during its validity, and ideally more frequently (even if for individual parts of an SMS).
- Supervision scheduling should adapt to the activities and capabilities of RUs/IMs.

NSA that wish to achieve a baseline level of good practice are recommended to:

- Allocate at least 50% of inspections to proactive supervision.
- Audit using core methods of document checks, interviews with a range of staff and frontline inspections.
- Check the whole SMS for each RU/IM at least once in a five-year period of validity for a safety certificate/authorisation.

NSA can deliver further good practice if they:

- Check at least individual parts of the SMS (if not the whole SMS) for each RU/IM more than once during a five-year period of validity for a safety certificate/authorisation.
- Follow an adaptive approach to scheduling supervision. A broad range of intervals between whole and partial checks of the effectiveness of the SMS for each RU and IM could be adopted based on the activities and capabilities of RUs/IMs.

Additional good practice would require NSA to:

- Plan supervision so that 80% of inspections are proactive.

3.6 Delivering supervision

This section discusses approaches to delivering supervision. Further subsections examine auditing methods (3.6.1); how NSA make decisions (3.6.2–3.6.3); how NSA communicate supervision strategies and plans (3.6.4); and, finally how language differences can affect supervision (3.6.5).

A summary and recommendations are provided in subsection 3.6.6.

Table B.22 provides several examples of how supervision is delivered and the varying approaches adopted by different NSA. Supervision presents NSA with particular challenges regarding how they should resource and deliver different supervision activities. Examples of how different authorities deliver supervision are highlighted below:

- To manage resources, the GB NSA has allocated some of its responsibility for supervising low risk, high frequency activities to a group of staff that have the capability to perform this task without requiring the expertise of fully-trained inspectors. The NSA recognises that targeting supervision at the full range of rail activities exceeds the scope of its core professional workforce; however, to avoid neglecting important issues, it has directed its core professional inspectorate towards supervising activities that are high risk or require a high level of technical knowledge and has a workforce with a different level of training and expertise supervising lower risk activities that are more prevalent (and would otherwise consume the time of its inspectorate or be neglected entirely).
- To collect information during supervision, technology can be used to facilitate the process (e.g. online submissions).
- To help guide dutyholders, special surveillance methods are used by the Danish OSH authority. These methods focus on delivering guidance to specific dutyholders based on risk profiles and then following up to see if guidance has been implemented. The approach does not utilise enforcement measures in these two stages so is very much based on targeted 'influencing' of behaviour. In its more moderate form, this approach establishes dialogue with RUs/IMs, whether it is through audit observations (e.g. Danish NSA) or regular meetings with RUs/IMs (e.g. Austrian NSA).
- To help guide staff in their supervision activities, some NSA have introduced internal advice structures for inspectors (e.g. at the GB NSA, supervision staff can talk directly with a senior inspector during supervision).
- To understand where supervision is required, how it should be delivered and how it is being received, survey methods have been demonstrated. These range from full quantitative surveys of staff in the marketplace by the Irish aviation authority through to mini polls online via the Czech OSH website and an online Q&A forum for the Estonian NSA. Whistle blowing policies can also assist with collecting safety critical information from the marketplace.
- To ensure consistency across different regional structures of an NSA, internal rules may be introduced and published.

In some instances, supervision does not extend as far as exploring underlying SMS failures and then issuing guidance or enforcement measures to address these (e.g. the Czech NSA). There are examples where an NSA may show inconsistency in how it delivers supervision: on the one hand, an NSA may report that it is a drain on resources to address underlying faults in the SMS of an RU/IM and yet, on the other hand, the same NSA may use its resources to carry out its own checks of rail sub-systems because an RU/IM has not put in place an effective SMS. This points toward a wider issue of how NSA manage the transfer to the new SMS-based approach to supervision from whichever system was in use prior to harmonisation. Some NSA (e.g. the German NSA) still expend considerable resources on delivering technical inspections because the market has not adopted fully the SMS-based approach to safety. Others prioritise the SMS-based approach and focus on issuing guidance above other supervision and enforcement practices to assist the market with meeting the new requirements (e.g. the Spanish NSA).

3.6.1 Supervision practices: audit methods

Table B.23 offers examples of the audit processes followed by different NSA. As discussed in Section 3.5.1, there are core methods for auditing RUs/IMs, which are based on a combination of interviews with staff, document checks and frontline inspections. Interviews with staff should be at all levels in an RU/IM and it is good practice for this to be planned rather than to happen by chance, which is why the Dutch NSA requests the organisation chart for each RU/IM so that it can identify who to interview. This contrasts with other NSA that focus on interviewing at management level only (e.g. the Czech and Spanish NSA). The importance of blending document checks with other activities was pointed out by at least one NSA that had noted an SMS may be compliant on paper but the organisation may fail to put it into practice.

Other key findings were as follows:

- Some NSA are transparent about their audit approach. For example, the Danish NSA summarises how an audit will include document checking and functional inspections, which are frontline (to inspect working functions of an RU/IM) and desk-based (to inspect the procedures that are set out). The audit is presented as a learning experience for RUs/IMs and there is a clear link between the process and the strategic goals of the NSA.
- Accredited bodies have been used to supervise the SMS of RUs and IMs (e.g. the Austrian NSA and the Polish NSA). An accredited body may be commissioned to carry out a professional audit of an SMS on behalf of an NSA. This approach may detach the NSA from part of the supervision task and so it is desirable to establish comprehensive links between the process of the accredited body and the NSA. The forthcoming CSM on Supervision requires NSA to exploit the link between assessment and supervision; with the SMS audit being a major element in the assessment, there is a risk that this link may not be strong.
- Audits can be guided using a checklist of required SMS features (e.g. Swedish NSA).
- Audits should not overlook subcontractors as they can provide good evidence as to how effectively an RU/IM implements its SMS (e.g. the Swedish NSA).

- It is prudent to monitor regularly whether planned audits are being delivered. As part of this process, the way in which audits are conducted may be reviewed and discussed amongst staff to develop a harmonised approach.

There was evidence of a range of durations for audits:

- 7–14 hours (Czech and Austrian NSA).
- 60–90 hours (Danish NSA).
- 200 hours with 32 spent at RU/IM premises (Swedish NSA).
- Approximately one month (Spanish NSA).

Clearly the intensity of auditing methods differs between NSA. NSA cannot be criticised for spending too much or too little time on an audit but it is useful to acknowledge that the amount of time and resource that is directed at a single audit covers a broad range. NSA that believe they are under-resourced (and especially those that are unable as yet to implement the full European safety regulatory framework) may wish to consider whether it is possible to be more efficient when conducting audits. NSA that are not implementing the safety regulatory framework as intended (e.g. those that are not interviewing staff at all levels) may wish to consider if more resource and/or time could be allocated to the audit process.

NSA also put forward their views for and against auditing parts of an SMS (discussed earlier in Section 3.5.3).

3.6.2 Decision-making criteria

Accountability is one of the seven principles for supervision specified in Regulations 1158/2010 and 1169/2010. NSA must be accountable for their decisions, which means that they must have policies and principles by which they can be assessed (e.g. a decision-making policy) and they must have a complaints procedure (section 3.1.7). The forthcoming CSM on Supervision will be more specific and will require NSA to "have, publish and apply decision-making criteria".

The majority of NSA responding had developed decision-making criteria regarding how they supervise and enforce compliance, and deal with non-compliances (Table 3.29). Six NSA had not developed such criteria (Spain, Poland, Portugal, Netherlands, Finland and the Channel Tunnel). Spain and Poland are both in the process of developing supervision and enforcement strategies that will include decision-making criteria. The Polish NSA reports that barriers to achieving this exist within national legislation and Poland may overhaul its national rules in response to the forthcoming CSM on Supervision.

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.7) and 1169/2010 (Annex III.7):

"7. NSA shall be accountable for their decisions in accordance with Article 17(3) of Directive 2004/49/EC. NSA shall therefore have policies and principles by which they can be assessed."

CSM on Supervision (Article 7)

"1. The national safety authority shall have, publish and apply decision-making criteria on how it monitors, promotes and, where appropriate, enforces compliance with the safety regulatory framework. This activity shall also include how it deals with non-compliance issues."

Of the 16 NSA that have developed decision-making criteria, three (Estonia, Ireland and Italy) do not publish their criteria, and another (Austria) is still in the process of developing and publishing its criteria. The majority of NSA have published this information on their websites. Some share the criteria during the application and assessment process for obtaining a safety certificate or authorisation.

Table 3.29: Dissemination of NSA decision-making criteria

NSA	Developed?	Published?	How?	Have RUs/IMs been told where to find it?
Great Britain	Yes	Yes	Discussed/issued during applications for safety certification or authorisation.	Yes
Sweden	Yes	Yes	Can also be discussed during supervision and meetings.	No
Estonia	Yes	No	-	-
Lithuania	Yes	Yes	Decision-making criteria are published in the officially published legal acts.	Yes
Romania	Yes	Yes	Discussed/issued during applications for safety certification or authorisation.	Yes
Germany	Yes	Yes	Published on NSA website	Yes
Denmark	Yes	Yes	Published on NSA website	Yes
Spain	No	-	-	-
Latvia	Yes	Yes	Published on NSA website	Yes
Poland	No. There aren't any national rules which set out the decision-making criteria. The basis for the supervision and enforcement processes are mainly regulations in the Railway Transport Act, which are an overall transposition of provisions established in Directive 2004/49. EU regulations, which set details for the supervision and enforcement process set in the Directive, and weren't up till now a reason to modify the national rules. Establishing more detailed rules and decision-making criteria is planned in the form of internal rules, prepared on the basis of CSMs set out in regulations 2010/1158 and 2010/1169 and also the CSM on supervision, which is now during legislation process. Additionally, please find attached the relevant Polish "Regulation on controls carried out by the President of UTK", which is mentioned in some of our answers. This regulation makes us trouble, as it was written under the old regime of supervision and hasn't been updated after entry into force of SMS-based supervision (see comment to question 91).			
Bulgaria	Yes	Yes	Discussed/issued during applications for safety certification or authorisation.	Yes
Austria	Yes	Yes	Under development; intended to be published on the NSA website.	No

NSA	Developed?	Published?	How?	Have RUs/IMs been told where to find it?
Portugal	No	-	-	-
Czech Republic	Yes	Yes	Published on NSA website.	Yes
Netherlands	No	-	-	-
Channel Tunnel	No	No		-
Hungary	Yes	Yes	Discussed/issued during applications for safety certification or authorisation.	Yes
Norway	Yes	Yes	Discussed/issued during applications for safety certification or authorisation.	Yes
Ireland	Yes	No	-	-
France	Yes	Yes	All options - Explained at the opening meeting of each control and are also found in a procedure available on the website of the EPSF.	Yes
Finland	No	-		-
Italy	Yes	No		-

3.6.3 Decision-making in supervision and enforcement

Deciding on a suitable response to supervision findings is a core topic for NSA. How this decision-making process is managed is subject to considerable variation. Table B.24 provides examples of these variations.

One example of a decision-making approach stands out for its semi-structured procedure and its apparent ability to deliver proportionate, consistent and transparent decisions. The 'Enforcement Management Model' (EMM) is a tool developed and used by the GB OSH authority and also the GB NSA (based on both authorities sharing audit techniques). The procedure documented by the EMM is described in the examples in Table B.24. Its key features are that:

- It is systematic; there is a logical progression to each step in the decision-making process and most steps are supported by flow diagrams (and a report form that matches the system) so that inspectors are guided to consider each and every step in turn.
- It always requires inspectors to use their expertise and judgement. The GB NSA summarises the EMM as a way of setting out the processes that must be followed in decision-making without indicating what the decision should be.

- It tries to be proportionate by considering the RU/IM and strategic factors that can influence an enforcement decision (in either direction), although the scope of influence is restricted by the model to ensure consistency.

The EMM process requires the GB NSA to identify first the 'risk gap'. This requires staff to consider the consequence severity and likelihood of the actual risk they have identified, and compare this to the benchmark level of risk for the activity (a process aided by risk matrices). The outcome is the risk gap, which can otherwise be referred to as a 'compliance gap' (i.e. how far the RU/IM has diverged from the typical consequence and likelihood for the activity). The compliance gap then leads to an initial enforcement expectation, which can be moderated by factors relating directly to the RU/IM or to the NSA's strategy.

Other NSA also permit some adjustment of their enforcement decisions in response to other factors (e.g. those that relate to the RU/IM, or perhaps the NSA strategy), which is similar in principle to the approach taken by the EMM. For example:

- Some NSA supervise using generally 'influential' measures. The Dutch NSA described how positive dialogue alone was often sufficient to bring about change in an RU/IM without having to decide on enforcement action.
- The Danish NSA describes how the borders between the different enforcement measures are 'grey areas' that can depend on the inspector's perception of the company. There are no rules to govern how the grey areas should be navigated but it is a subject regularly reviewed and discussed at staff meetings.
- The Austrian NSA also practices a procedure that accounts for other factors when making an enforcement decision. This procedure is currently based on 'experience' but the NSA plans to document it. Often this experience does refer to previous cases with similarities in order to be consistent.
- The Bulgarian NSA does not have a documented decision-making procedure but it too considered risk factors and RU/IM response before making an enforcement decision.
- The Swedish NSA will only consider other factors in its decision-making if the initial recommendations (its usual first-step) were not followed. Only then would further enforcement action be considered and there therefore be a need to modify the response accordingly.

Perhaps a key difference between the approaches that have been described are that some, such as the EMM, may not overlook a transgression even if it has been resolved because it must always consider the initial enforcement response that would be appropriate and this can only be modified afterwards to a certain degree. With other NSA this distinction is not so clear and whether or not the company has dealt with the safety hazard effectively appears able to override any initial enforcement action that may have otherwise been deemed appropriate.

A further consideration for decision-making is the number of staff that are permitted to make an enforcement decision, and their level and degree of autonomy. A range was described by NSA:

- Individual inspectors should have the responsibility for their own cases, according to the GB NSA. Others can be consulted to check the legal rationale, for example.

Giving each inspector this authority is said to empower them and encourage them to ensure they are fully appraised of each individual case.

- One or two inspectors will work on a case and should have the responsibility for decision-making, according to the Danish NSA, depending on where the breach was discovered and what it concerns.
- Two persons will cover each case at the Dutch NSA and will share responsibility for decision-making, with legal support available if required.
- A 'team decision' is made by the Austrian NSA that includes legal and technical experts.
- Regional managers issue any recommendations and the head office issues any penalty decisions for the Polish NSA. However, employees of the NSA are individually accountable for decisions according to Polish law (which was reported to promote inaction).

Who makes enforcement decisions at the Bulgarian NSA depends on who is targeted at the RU/IM; if the decision is expected to require management intervention it will be decided by NSA managers and delivered to RU/IM managers. If it is targeted at lower levels in the RU/IM, inspectors will make and issue the decision accordingly. This approach would appear to neglect that SMS-based enforcement should affect all levels in an RU/IM.

Another consideration is how decision-making should be monitored and reviewed. Examples include the following:

- The GB NSA has a practice of using surgeries for team managers to collate and discuss feedback from inspectors on supervision cases. This process retains the links between all levels of the NSA with regard to decision-making, thus providing some balance to the EMM system, which can be practiced somewhat autonomously.
- Weekly meetings between inspectors (and other regular sessions), as described by the Danish NSA, may be appropriate for NSA with fewer staff who are not distributed throughout the country. The focus of such meetings is discussing the rationale behind recent decisions to ensure all staff have a similar understanding.
- Telephone support for staff to contact senior colleagues and/or the director to check their decision-making is appropriate and follows appropriate procedure (e.g. the Danish NSA).
- At the award stage, a committee can be used to provide an independent and expert review of an application decision (e.g. the Danish NSA).
- The Dutch NSA requires all supervision reports to be checked by a colleague and peer discussions are organised before decisions are issued.

3.6.4 Communicating supervision strategies and plans

NSA are expected to communicate supervision strategies and plans to relevant RUs/IMs and, where appropriate, more widely.

One approach to this would be to make strategies/decision-making criteria publicly available, which 11 NSA have opted to do (Table 3.30). Other options for communication are to have regular meetings and formal discussions with stakeholders, which eight NSA

have opted to do. A further option is to present to stakeholders at conferences and other meetings, which eight NSA have opted to do. Overall, four NSA (GB, Lithuania, Hungary, Ireland) have adopted all three of these communication measures.

Six NSA (Poland, Portugal, Czech Republic, the Netherlands, Finland and Italy) have adopted none of these options; however, the Polish NSA is following a national system that requires communicating supervision plans to the affected party prior to any supervision action taking place. The Polish NSA is looking to bring its policies more in line with the forthcoming CSMs on Supervision and Monitoring once they are officially finalised. The Finnish NSA may also be changing its policy as part of a wider organisational change.

Table 3.30: Communicating supervision activities

NSA	Strategies/ decision-making criteria publicly available?	Regular meetings/formal discussions with stakeholders?	Present to stakeholders at conferences/ meetings	Other, please specify:
Great Britain	Yes	Yes	Yes	
Sweden	No	No	Yes	
Estonia	Yes	Yes	No	
Lithuania	Yes	Yes	Yes	
Romania	Yes	No	No	
Germany	Yes	No	No	
Denmark	Yes	No	No	
Spain	No	Yes	Yes	
Latvia	Yes	No	No	
Poland	No	No	No	National system that was the basis for the supervision plan for 2011 doesn't require that. We are only obliged to inform in advance the entity for which the visit is foreseen that we are going to start supervisory activities. We also inform the market players about the procedure for complaints. The procedure is based on law and common sense for almost all activities performed by the NSA. If a specific case is examined in compliance with the administrative proceedings code, the information

NSA	Strategies/ decision-making criteria publicly available?	Regular meetings/formal discussions with stakeholders?	Present to stakeholders at conferences/ meetings	Other, please specify:
				on the appeal procedure is always placed in the decision.
Bulgaria	No	Yes	Yes	
Austria	Under development according to the draft recommendations of the CSM for supervision. It is intended to be made available to public after finalisation.			
Portugal	No	No	No	
Czech Republic	No	No	No	
Netherlands	No	No	No	
Channel Tunnel	No	Yes	No	
Hungary	Yes	Yes	Yes	
Norway	Yes	No	Yes	
Ireland	Yes	Yes	Yes	Guidance is also available on our website.
France	Yes	Yes	Yes	Through its annual activity reports and safety meetings REX (return of experience/feedback).
Finland	No	No	No	Until now the NSA has discussed supervision only sparsely with stakeholders. However, due to organizational changes this is changing at the moment.
Italy	No	No	No	The supervision strategy is not currently made public. An audit annual plan and some files are drawn up for the Ministry.

The questionnaire invited each NSA to specify which of five different methods it used to disseminate its supervision practices. Table 3.31 shows NSA most commonly share information with RUs/IMs on their general supervision and enforcement strategy in person during supervision activities (this method has been adopted by 14 NSA). The next most common approaches to sharing such information is by website and directly during the process of awarding a safety certificate or authorisation (11 NSA), followed by

during workshops and conferences (nine NSA) and finally by direct letters to RUs/IMs (four NSA). In summary:

- Two NSA (GB and Netherlands) shared information using all five methods.
- One NSA (France) shared information using four of the five methods.
- Four NSA (Estonia, Poland, Hungary, and Ireland) shared information using three of the five methods.
- Nine NSA (Sweden, Lithuania, Romania, Denmark, Spain, Bulgaria, Portugal, Norway and Italy) shared information using two of the five methods.
- Five NSA (Germany, Latvia, Czech Republic, Finland and the Channel Tunnel) shared information using one of the five methods.
- One NSA (Austria) did not share information using any of the methods listed.

Table 3.31: Methods of disseminating supervision practices

NSA	On its website	By letter direct to RU/IMs	At workshops/ conferences	In person during supervision/ enforcement activity	Directly during award of a safety certificate/ authorisation
Great Britain	Yes	Yes	Yes	Yes	Yes
Sweden	No	No	Yes	Yes	No
Estonia	Yes	No	No	Yes	Yes
Lithuania	Yes	Yes	No	No	No
Romania	No	No	No	Yes	Yes
Germany	Yes	No	No	No	No
Denmark	Yes	No	Yes	No	No
Spain	No	No	Yes	No	Yes
Latvia	Yes	No	No	No	No
Poland	No	No	Yes	Yes	Yes
Bulgaria	No	No	No	Yes	Yes
Austria	No	No	No	No	No
Portugal	No	No	No	Yes	Yes
Czech Republic	No	No	No	No	Yes
Netherlands	Yes	Yes	Yes	Yes	Yes

NSA	On its website	By letter direct to RU/IMs	At workshops/ conferences	In person during supervision/ enforcement activity	Directly during award of a safety certificate/ authorisation
Channel Tunnel	No	No	No	Yes	No
Hungary	Yes	Yes	No	Yes	No
Norway	Yes	No	Yes	No	No
Ireland	Yes	No	Yes	Yes	No
France	Yes	No	Yes	Yes	Yes
Finland	No	No	No	Yes	No
Italy	No	No	No	Yes	Yes

Seven NSA (GB, Lithuania, Germany, Denmark, Norway, Ireland and France) had supervision and enforcement strategies that could be viewed by other Member States, RUs/IMs and NSA, even if not directly affected by the content. The other 15 NSA did not have such arrangements.

3.6.5 Language differences between NSA

Only one NSA (the Channel Tunnel) had its supervision strategy and plans available in another language. It invests 'significant resources' to ensure that language differences are never a barrier; such resources include investment in written and oral translation services and language training for staff. For the Channel Tunnel language differences therefore do not create a problem. However, for at least four other NSA, language differences do create problems. Often these problems only arise when dealing with RUs from a different Member State (the Spanish NSA, for example, does not deal with foreign RUs so does not have any language-related difficulties at present). Of the four NSA with language-related difficulties, the Swedish NSA explained that such differences can lead to misunderstanding and wrong decisions being made. Its strategy for dealing with these issues is to use English as a universal language for communication. Staff are therefore trained to speak English if presented with a language barrier and are also required to listen carefully to avoid making any assumptions that might be a result of misinterpretation. The German NSA also has experience of misunderstandings occurring so it has opted to translate documents where appropriate to mitigate such issues. The Dutch NSA has experienced language issues related to train drivers from foreign RUs being unable to speak Dutch, which is the preferred language of the NSA. To overcome such issues it enforces only the Dutch Railway Law, which makes communication in Dutch a requirement. In Poland, the NSA has found that language difficulties are not common at present because many foreign RUs have set up subsidiary organisations in Poland and have employed Polish staff with a command of the Polish language. However, when carrying out activities such as assessments for a Part B certificate, such meetings have required an interpreter, which is typically supplied by the applicant. In addition,

Polish law requires that all documents are submitted by applicants in the Polish language hence translation is often required. With regard to EU legislative documents and guidance, the Polish NSA has had to translate the majority into Polish so that they can be understood by it staff, as those who are primarily responsible for certifications, authorisations and supervision do not communicate in English.

3.6.6 Summary

Auditing of RUs/IMs is a process that seems to vary with intensity between NSA, with some directing substantial resource and time at a single audit and other NSA being more moderate.

An essential outcome from supervision activities is a decision on whether enforcement action is required. In accordance with the principles of supervision, NSA should be accountable for their decisions and one way to achieve this is to develop and implement decision-making criteria. Approximately three-quarters of NSA have developed decision-making criteria and most of these have published them.

The process by which enforcement decisions are made is another area where NSA differ. The number of staff who are able to make a decision and their position within an NSA is one of the decision-making factors on which NSA differ. Decisions may be made by individual inspectors, whole teams or only by managers. A consistent approach in which all evidence is accounted for is desirable and perhaps the simplest way to achieve that is to empower an individual with decision-making. When decisions are being made, NSA may choose to support and review the process; for example, staff may be able to liaise with senior inspectors to check their decision-making. Once decisions are made, NSA may choose to adopt a formal review procedure such as a harmonisation committee or a certification committee and/or they may choose less formal review processes such as peer group discussions or team meetings. Some form of monitoring and review is desirable for ensuring decisions are consistent and proportionate.

A further point of difference is the decision-making procedure itself. The review identified one particular procedure (used by the GB NSA) as a clear example of a consistent and structured approach to decision-making. The essential elements were that it directed users to calculate the 'compliance gap' created by the non-compliance or safety hazard, then decide on an initial level of enforcement before considering whether any factors related to the RU/IM or the NSA strategy would affect the subsequent level of enforcement. These principles were adopted in part by many other NSA although none reported bringing together the principles in a form that was as accessible and structured.

Approximately half of NSA satisfy requirements to be transparent by communicating their decision-making procedures and supervision strategies to the market. Meeting with RUs/IMs is the most common approach to communicating these procedures, followed by presenting at conferences and other larger meetings. When considering sharing more general information about supervision strategies and practices, the most common approach is to do so directly with RUs/IMs during supervision. However, it was also common to share such information through websites, during assessment, during conferences and by letter. Few NSA used more than a couple of methods. Only one NSA had opted to translate its supervision plans and strategy into another language.

When considering recommendations for good practice, decision-making procedures were discussed with the NSA Taskforce on Assessment and Supervision and it was generally agreed that:

- A common, structured approach to decision-making for enforcement is desirable (at national or European level) but it should remain flexible. The approach should calculate the compliance gap and direct NSA toward a proportionate response.
- NSA should be accountable for their decisions and demonstrate transparency. Therefore, the decision-making process should be documented by each NSA. NSA may wish to model their decision-making on established procedures used by other NSA (such as the GB NSA) or safety authorities from other domains but no specific model is recommended.
- A longer term goal may be to develop a detailed European model for decision-making in enforcement.

NSA that wish to further achieve a baseline level of good practice are recommended to:

- Monitor delivery of audits to check they are in line with the planned programme.
- Develop and publish decision-making criteria.
- Plan to interview staff at all levels in an RU/IM when conducting an audit. Planning can be assisted by requesting an organogram or similar from the RU/IM.

NSA can make several further adjustments to deliver good practice if they:

- Survey the marketplace to understand how effective supervision is and how delivery could be improved.
- Consider if technology can facilitate supervision practices by, for example, enabling RUs/IMs to submit information and documents online.
- Consider if supervision methods can give RUs/IMs an opportunity to learn from the expertise of the NSA (e.g. by issuing guidance initially rather than enforcing).

Key findings:

- Single audits can take 7 hours to 1 month, depending on the NSA.
- Majority of NSA have developed and published decision-making criteria.
- NSA may give decision-making power to individual staff or collectively to teams or managers.
- NSA may review decisions formally by committee and/or informally in peer groups.
- Few NSA have comprehensive, structured and fully documented decision-making processes.

Good practice recommendations:

- Develop and publish (using multiple methods) a structured decision-making process (together with decision-making criteria) to provide a proportionate response to any compliance gap.
- Plan interviews with staff at all levels in an RU/IM, and include subcontractors during audits.
- Survey the marketplace to check and develop the effectiveness of supervision practices.
- Facilitate learning through supervision for RUs/IMs.
- Empower individual inspectors to make enforcement decisions. Support inspectors with internal advice structures.
- Match staff expertise with supervision activities to use resources efficiently.
- Implement a whistleblowing policy.

This is especially pertinent when managing the transition to an SMS-based approach.

- Implement an internal advice structure so that NSA staff can obtain senior guidance with ease.
- Include subcontractors in audits to estimate how effectively an RU/IM implements its SMS throughout its operations.
- Empower individual inspectors to make enforcement decisions.

Additional good practice would require NSA to:

- Manage resources in a way that matches staff expertise with the type of supervision activity. This should enable staff with a range of skills to be deployed so that no activities are neglected, whether they are high or low risk.
- Implement a whistle blowing policy to obtain honest feedback from the market.
- Consider multiple methods of sharing decision-making criteria and supervision strategies with the market.

These good practice recommendations for decision-making are summarised in Figure 3.5, which present the six key steps in the decision-making process and the methods to consider at each step.

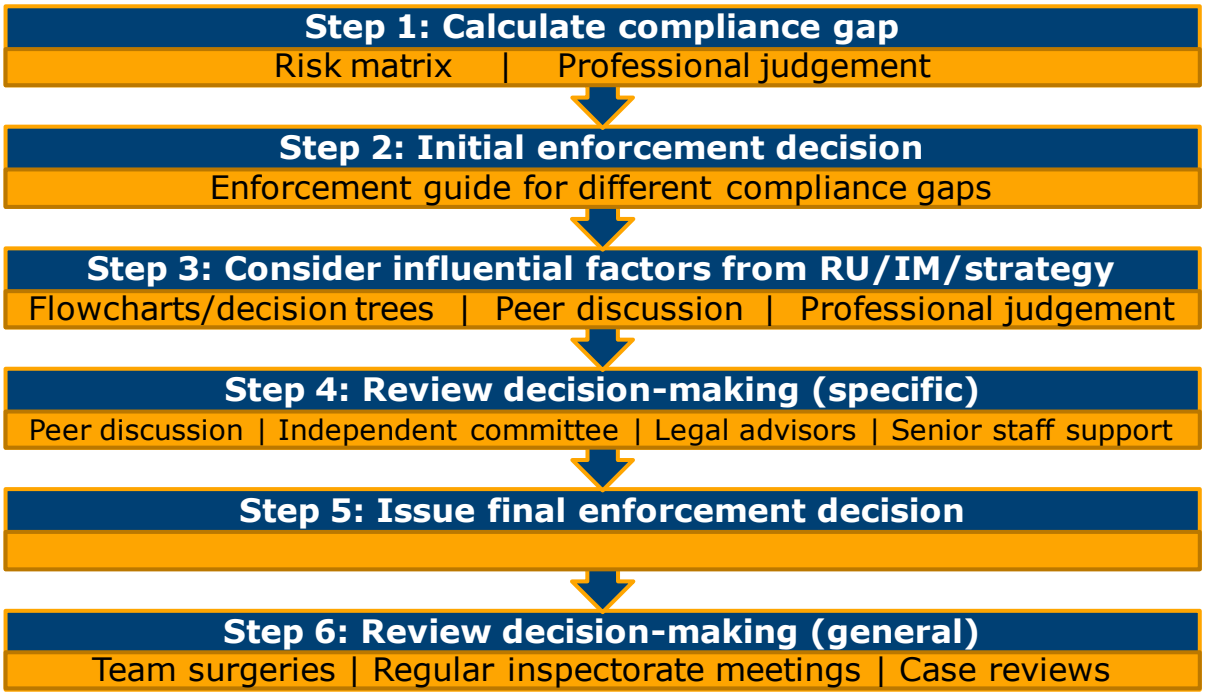


Figure 3.5: A good practice model for making decision during supervision and enforcement

3.7 NSA transparency

Effective communication with the market is embodied in the principle of transparency. In order for NSA to assist RUs/IMs in understanding what they are expected to do (and not do) and what the market can expect of the NSA in return, communication must be a priority for each NSA.

3.7.1 Self reported ratings of transparency

Transparency is one of the seven principles of supervision described in Regulations 1158/2010 and 1169/2010. The foundations of the principle are that RUs and IMs should understand what the NSA expects of them and what they can expect of the NSA.

Table 3.32 shows that, with the exception of three NSA (Poland, Portugal and Finland), all of the NSA responding to the questionnaire stated that they were 'very' or 'completely' transparent when it came to RUs/IMs understanding what the NSA expects of them as well as what RUs/IMs can expect of the NSA.

Table 3.32: NSA ratings of transparency

NSA	How transparent is your NSA in helping RUs/IMs understand what the NSA expects of them?	How transparent is your NSA in helping RUs/IMs understand what they can expect of the NSA?
Great Britain	Very transparent	Very transparent
Sweden	Very transparent	Very transparent
Estonia	Very transparent	Very transparent
Lithuania	Very transparent	Very transparent
Romania	Completely transparent	Completely transparent
Germany	Very transparent	Very transparent
Denmark	Very transparent	Very transparent
Spain	Very transparent	Very transparent
Latvia	Very transparent	Very transparent
Poland	Slightly transparent	Slightly transparent
Bulgaria	Very transparent	Very transparent
Austria	Very transparent	Very transparent
Portugal	Slightly transparent	Slightly transparent
Czech Republic	Very transparent	Very transparent
Netherlands	Very transparent	Very transparent

NSA	How transparent is your NSA in helping RUs/IMs understand what the NSA expects of them?	How transparent is your NSA in helping RUs/IMs understand what they can expect of the NSA?
Channel Tunnel	Completely transparent	Completely transparent
Hungary	Completely transparent	Completely transparent
Norway	Very transparent	Very transparent
Ireland	Very transparent	Very transparent
France	Completely transparent	Completely transparent
Finland	Slightly transparent	Very transparent
Italy	Very transparent	Very transparent

To explore further these statements of transparency, NSA were asked if and where such information was publicised. All NSA except for four (Germany, Spain, Portugal and Finland) claimed to publicise information for RUs and IMs to help them understand what the NSA expects of them (Table 3.33). This information was most often publicised on NSA websites, as well as being circulated and discussed during meetings, workshops and visits. Leaflets were rarely used.

Table 3.33: NSA dissemination approaches

	How is information published?						
NSA	Publicise?	Website	Leaflet	Workshop	Visits	Other	Specify
Great Britain	Yes	Yes	No	Yes	Yes	No	-
Sweden	Yes	Yes	No	Yes	Yes	Yes	Meetings with RUs/IMs
Estonia	Yes	Yes	Yes	Yes	Yes	No	-
Lithuania	Yes	Yes	No	No	Yes	Yes	The expectations are listed in the legal acts that are officially published.
Romania	Yes	Yes	No	No	Yes	No	-
Germany	No	No	No	No	No	No	-
Denmark	Yes	Yes	No	No	No	No	-
Spain	No	No	No	No	No	No	-
Latvia	Yes	Yes	No	Yes	Yes	No	-

How is information published?							
NSA	Publicise?	Website	Leaflet	Workshop	Visits	Other	Specify
Poland	Yes	Yes	No	Yes	Yes	No	Main expectations are outlined in the legislation. The NSA provides the legislation on its website or gives the references to legislation published in the Official Journal. Besides this the NSA shares its expectations during bilateral meetings with RUs / IMs during the certification process (i.e. describes what separate parts of the SMS should include). Sometimes the NSA takes part in general workshops and conferences organised by other entities. There it also shares its expectations. The workshops usually aren't organized by the NSA due to lack of financial resources.
Bulgaria	Yes	Yes	No	Yes	Yes	No	-
Austria	Yes	Yes	No	No	No	No	-
Portugal	No	No	No	No	No	No	-
Czech Republic	Yes	Yes	No	No	Yes	Yes	Individual consultation.
Netherlands	Yes	Yes	No	No	No	Yes	Information by mouth by inspectors.
Channel Tunnel	Yes	Yes	No	No	Yes	No	-
Hungary	Yes	Yes	No	No	Yes	No	-
Norway	Yes	Yes	No	Yes	Yes	No	-
Ireland	Yes	Yes	No	Yes	No	Yes	Guidance document.
France	Yes	Yes	Yes	Yes	Yes	Yes	Annual reports, audits opening meetings, REX (return of experience) meetings...
Finland	No	No	No	No	No	No	-
Italy	No	No	Yes	No	No	Yes	Annual Reports/Critical point or areas.

Across all NSA, the information published on what they expected of RUs/IMs included details on:

- Applicable regulations, and guidance on how such regulations would affect RUs/IMs

- The application process and its requirements
- Recent and forthcoming changes to regulations and procedures
- Accident trends and areas where greater supervision may be required
- Supervision strategies
- Contacts at the NSA

Ten NSA had a service pledge or similar to help RUs and IMs understand what they can expect of the NSA (Table 3.34). All of the NSA that did have a service pledge published it via their websites, with additional circulation during meetings, workshops and visits.

Table 3.34: Publicising NSA service standards/pledges

NSA	Service pledge?	Where is the information published?				
		Website	Workshop	Visits	Other	Specify
Great Britain	No	No	No	No	No	-
Sweden	Yes	Yes	No	Yes	No	-
Estonia	Yes	Yes	No	No	No	-
Lithuania	Yes	Yes	No	Yes	Yes	The 'service pledge' is described in the officially published legal acts.
Romania	No	No	No	No	No	-
Germany	Yes	Yes	No	No	No	-
Denmark	Yes	Yes	No	No	No	-
Spain	No	No	No	No	No	-
Latvia	Yes	Yes	No	No	No	-
Poland	No	No	No	No	No	-
Bulgaria	Yes	Yes	Yes	Yes	No	-
Austria	No	No	No	No	No	-
Portugal	No	No	No	No	No	-
Czech Republic	Yes	Yes	No	No	No	-
Netherlands	No	-	-	-	-	-
Channel Tunnel	No	-	-	-	-	-

NSA	Service pledge?	Where is the information published? Website	Workshop	Visits	Other	Specify
Hungary	No	No	No	No	No	-
Norway	Yes	Yes	Yes	Yes	No	-
Ireland	Yes	Yes	Yes	No	Yes	RSC-g-023-B Guidance document
France	No	-	-	-	-	
Finland	No	-	-	-	-	-
Italy	-	-	-	-	-	-

The content that could be likened to a 'service pledge' varied. Table B.25 shows examples including:

- Statements of intent from NSA
- Descriptions of NSA services and duties
- Supervision strategies
- Descriptions of NSA activities in authorisation/certification and supervision
- Question and answer fora
- Details of the NSA's own ISO certification

3.7.2 NSA communication with stakeholders

This section explores how NSA communicate with stakeholders using websites and a variety of other methods. Such communications are an essential element of transparency, which is one of the regulated principles of supervision (Regulations 1158/2010 and 1169/2010). The CSM on Supervision also requires communication of supervision strategies and plans whilst the Safety Directive states that NSA must 'promote' the safety regulatory framework and act in a 'transparent way'. Collectively, there are strong regulatory requirements for transparency, many of which can be satisfied by following the good practice recommendations in this section.

3.7.2.1 NSA websites

NSA websites represent one of the fundamental methods of communicating with the market and are utilised to some extent by all NSA. Examples of how authorities exploit their websites for dissemination are outlined in Table B.26. Recommended baseline good practice would be to:

- Publish all key documents and NSA processes, policies, and procedures online. Exceptions to this may include sensitive procedures or plans that may give RUs/IMs information that might enable them to influence supervision findings.
- Provide links to direct RUs/IMs to external information sources that the NSA considers informative.

NSA wishing to develop further their website communications would be advised to consider the following points:

- Resources can be made available for download. These can include tools (e.g. checklists). Resources can be catalogued innovatively to assist users in finding what they need (e.g. Danish and GB OSH authorities).
- Websites can feature information and guidance on key industry issues (e.g. the Austrian OSH authority).
- News and current information about the sector can be publicised. Some RUs and IMs in the market may not be as well-connected as others

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.6) and 1169/2010 (Annex III.6):

"National safety authorities shall apply the principle of transparency to help railway undertakings/ infrastructure managers understand what is expected of them (including what they should or should not do) and what they should expect from the national safety authority."

CSM on Supervision (Annex 1.2)

"2. Communicating and Carrying Out the Supervision Strategy and Plan(s)

The national safety authority shall:

i. communicate the overall objectives of the supervision strategy and overall explanation of the plan or plans to relevant railway undertakings/infrastructure managers and, where appropriate, more widely to other stakeholders

ii. provide an overall explanation to relevant railway undertakings/infrastructure managers how the supervision plan or plans will be undertaken"

Directive 2004/49/EC (Article 16.2(f))

"Monitoring, promoting, and, where appropriate, enforcing and developing the safety regulatory framework including the system of national safety rules"

Directive 2004/49/EC (Article 17.1)

"The safety authority shall carry out its tasks in an open, non-discriminatory and transparent way."

and so a central source of news and information for the market can be valuable.

NSA that wish to demonstrate higher levels of good practice can consider:

- Adopting innovative website structures to catalogue information (e.g. according to themes) in order to assist users when searching for help.
- Providing foreign language translations of all or part of the website and its contents (e.g. the Danish OSH authority) to facilitate users from other countries. Given that language differences can be a barrier to cross-border cooperation, this is one route to improving cross-border links. NSA may wish to prioritise translation for languages of neighbouring Member States or those with which they share the most rail trade.
- Publishing enforcement decisions and actions.

The publication of enforcement action warrants further discussion. Some authorities include enforcement actions in the news items they publish online (e.g. GB OSH authority and GB NSA). It can be considered good practice to publish enforcement action for a number of reasons, such as:

- Visible deterrent: there is an element of public shame associated with enforcement action against a company becoming public knowledge. This activity may be an incentive to other RUs/IMs to work harder towards implementing an effective SMS.
- Commercial loss: publication of enforcement action may affect the commercial competitiveness of an organisation by deterring customers. This outcome does depend on the type of organisation: a RU/IM without commercial competition may not be affected but a freight RU that is competing with others for trade may incur commercial losses. The outcome may depend on how the enforcement action is presented. An example that describes how the company has responded positively and effectively may present it as responsive and aware of its role in improving safety.
- Demonstrate the role of the NSA: the function of the NSA as an enforcer can be demonstrated by publishing its enforcement actions. This message can reach the industry, the public, other NSA and stakeholders, providing a degree of transparency and cooperation in the process. For some cases it may be in the public interest to publish enforcement actions, particularly for high profile incidents, as this may reassure the public that the incident has been taken seriously and has led to corrective action.
- Guide the industry by example: as well as being a visible deterrent, published enforcement action may also serve as guidance to the industry regarding how it should operate – and in particular, the practices that should be avoided.

A note of caution is required. Some authorities, such as the Dutch NSA, may be prohibited from publishing enforcement action by national law. In addition, if the law permits publication, the safety authority would be advised to consider if the overall level of enforcement action will still be proportionate when the effects of publication are included. This may depend on the type of organisation, the type of action taken (e.g. has a fine already been issued), and the style of reporting (e.g. how the publication presents

the facts of the case and the company's response). The safety authority should also consider which levels of enforcement should be published (e.g. only prosecutions) and the format for publishing. Some safety authorities may choose to publish high profile enforcement decisions and/or the more severe cases in a prominent position on their website but place details of more minor offences in a less visible section of the website (e.g. in a searchable database). Finally, if publishing enforcement actions, NSA must avoid generating social norms that suggest to the industry that 'everyone is breaking the law'. Violations should be shown as infrequent and unacceptable.

3.7.2.2 Other methods of communication

Websites can also restrict the communication efforts of NSA. In publishing information online, NSA can be of the opinion that dissemination is sufficient and additional communication is not required. There can be value in adopting other approaches, particularly those that enable direct engagement with the market, and NSA that wish to adopt good practice are advised to finds ways of communicating to supplement their online offerings.

Table B.27 provides examples of direct communication with the market, many of which are practiced by safety authorities in other industries. The methods described are all good practice examples of how to satisfy the principle of transparency. In addition, the examples given (such as organising a seminar, conference, workshop or other such course) can be a way to target industry activities that the NSA believes should be a focus for supervision, thus meeting another of the principles of supervision.

The recommended examples of direct engagement with the market are:

- **Conferences, seminars and symposiums.** These events can be organised to bring stakeholders together to inform them of new regulations and guidance, to share and discuss best practice, to discuss key issues, and to develop harmonised approaches. The output of such activities can be shared widely and retained as a reference (e.g. on the authority website) for future use. Seminars are an option for more targeted participation.
- **Workshops and courses.** These can be organised to guide learning of core topics, such as SMS implementation and assessment. They can enable RUs/IMs to access the collective experience of the safety authority and other RUs/IMs on specific subjects. Such workshops are particularly useful for encouraging RUs/IMs to engage with each other to discuss and share practices, with the NSA present to provide a regulator's perspective on the discussion.

Collectively, these methods of communication enable safety authorities to:

- Bring together a diverse range of stakeholders who might not normally share experiences and practices. This may include related authorities (e.g. national investigation bodies).
- Influence behaviour and future practice by providing its own guidance on key issues.
- Develop cross-border relationships and improve harmonisation by inviting stakeholders from other countries to attend.

- Promote central European themes and targets (e.g. those created by ERA) across the marketplace.
- Create a resource bank for future reference by retaining, publishing and disseminating proceedings from the events.

Table B.28 and Table B.29 provide further examples of how NSA communicate.

It is recommended that NSA that wish to develop their communication further should:

- **Meet regularly with RUs/IMs.** The Danish, Swedish and Norwegian NSA (to name just some of several) all have regular meetings with RUs/IMs on a formal and informal basis. Perhaps the most regular and informal of these examples are the 'breakfast meetings' hosted by the Norwegian NSA, where RUs/IMs are invited to come along to talk to the NSA about current operations and issues. All are good practice examples of improving dialogue between the NSA and the market which can be an excellent route to achieving transparency.
- **Assign specific staff as the primary liaison for specific RUs/IMs.** This approach is demonstrated by several NSA including the British and German. Arrangements of this type add another layer to the supervision regime and provide an opportunity for the NSA and individual RUs/IMs to discuss issues that may have emerged, from operational observations or during recent inspections. Frequently changing the point of contact that an RU/IM has with an NSA helps to avoid the difficulties that may arise, such as the potential for bias in the supervision process.
- **Establish ways in which the authority can supervise and enforce with transparency.** This can involve creating and even publishing a set of procedures that staff must follow (e.g. explaining decisions to RUs/IMs, providing written confirmation afterwards).
- **Use a variety of media for internal and external communications**, matched to the needs of the market and to the internal needs of the NSA.
- **Issue monthly incident reports to the market.** This practice (as described by the French NSA) ensures that all RUs and IMs are aware of the latest safety issues in the marketplace, irrespective of whether they were involved directly.

NSA that wish to demonstrate higher levels of good practice are recommended to:

- **Develop a strategy for communication.** A communication strategy is good practice because it provides focus for the NSA; often it is not possible to reach all of the market, all of time so it becomes necessary to segment the market into target groups. The strategy should be reasonably long-term and should identify which stakeholders will be targeted, what the content of the communication will be (and/or the process for developing this content) and how/when the communications will be issued. A strategy should also address any uncertainty within an NSA regarding how it communicates. For example, the question of how widely NSA activity should be disseminated was a consideration for the Dutch NSA. It acknowledged that it was often rather 'silent' when it came to communicating its actions and, when incidents occurred, its engagement with the press was poor. This contrasts with the GB OSH authority, for example, which

uses press coverage of its response to incidents as one of the criteria for measuring the success of its dissemination. This recommendation was agreed with the NSA Taskforce on Supervision.

- **Ensure communication meets the demands of the market.** It is recommended that NSA collect feedback from the market (e.g. via a survey) to identify the most effective methods of communication.
- **Issue leaflets for when there is supervisory contact** to remind RUs/IMs of their rights and obligations during the process (e.g. the GB OSH authority). Even if information is provided elsewhere and at other times, during an inspection it is pertinent to have this information in an accessible format to remind or inform those who are affected by the supervision activity of their rights. It should be considered that those RU/IM employees specifically affected by supervision activities may not be familiar with the NSA's procedures.
- **Update the industry on progress with strategic objectives.** This is particularly relevant for authorities with long-term strategies, as it provides the industry with renewed focus and can also recognise any achievements that have been made over the current period. One of the examples found (from the GB OSH authority) was a compilation of case studies that described how industry stakeholders had adopted good practice.
- **Use posters and media campaigns to highlight important issues** for the industry. Campaigns that target members of the public are more likely to fall under the remit of RUs/IMs or other government departments but campaigns that target RUs/IMs and their employees may be within the scope of an NSA.
- **Offer targeted, in-depth guidance.** An example is the 'CSM School' run by the Danish NSA; RUs/IMs attend to gain a detailed understanding of the CSM on Risk Assessment. This is an example of an NSA recognising market confusion and responding with measures to improve transparency and consistency. It can encourage harmonisation and create a fair market when all RUs/IMs have access to high-quality guidance. Other NSA also issue targeted guidance; for example, the Austrian NSA provides written guidance directly to RUs/IMs to update them on new legislation. Section 3.7.3 provides more information on guidance.

NSA discussions on the subject of communication raised further considerations. One of the points raised was that NSA could use research to promote and encourage safety improvements. The role of research is discussed further in Section 3.7.4. Other discussion points were as follows:

- NSA may wish to consider how other departments within the government communicate with stakeholders; for example, the German OSH authority has established in law an annual forum for stakeholders (see Section 3.1.8) which is a demonstration of good practice that the German NSA could consider adopting for the rail sector.

- It was suggested that meetings with RUs/IMs that occur outside of supervision activities should be an opportunity for the stakeholders to bring up the topics that interest or concern them.
- Communicating with the market has the potential to consume considerable resources that are disproportionate to the expected benefit: NSA are advised to consider the target audience and tailor communication accordingly (this can be supported with a communication strategy). It was recommended that communicating information to segments of the market that are less likely to benefit should not be prioritised over core supervision activities.

3.7.2.3 Summary

In summary, a key finding is that some NSA will claim to be 'very transparent' but then show little evidence of engaging with stakeholders beyond perhaps providing a website. The CSM on Supervision is clear that the supervision strategy and plan should be communicated to RUs/IMs and other stakeholders (e.g. rolling stock manufacturers, ECMs). It seems that many NSA have adopted an approach whereby publication is seen as the primary means of being transparent. There are a number of ways in which NSA can demonstrate good practice through their website communication, such as focusing on key industry issues, providing online resources, publishing industry news and translating parts of the website into foreign languages.

The additional activities of some NSA suggest that a good practice approach to being transparent can involve more than simply providing documents online. Direct dialogue with RUs/IMs is a valuable element of transparency and there are many ways in which this dialogue can be structured. NSA that wish to adopt good practice are advised to first consider organising and participating in conferences, seminars and workshops with their market. Recommendations for NSA that wish to take good practice further include meeting regularly with RUs/IMs, developing a communication strategy and offering targeted guidance.

Key findings:

- NSA primarily communicate with the market through their websites, by publishing documents and information.
- News, industry features, resources, foreign language support and innovative search features have been used to enhance safety authority websites.
- Publishing enforcement decisions may be effective but controversial.
- Conferences, seminars, workshop and courses provide opportunities for targeting communication at specific market segments.
- Some NSA encourage direct and relatively informal dialogue with individual RUs/IMs.
- Examples of good practice include developing a communication strategy that meets the demands of the market and offering targeted, detailed guidance.

Good practice recommendations:

- NSA communication with stakeholders should expand beyond hosting a website.
- NSA should develop a communication strategy. The strategy should ensure that resources that are directed towards communication are proportionate to the size of the market and fit with the other activities of the NSA. This recommendation was agreed with the NSA Taskforce on Supervision.

3.7.3 Guidance

A specific part of communication is issuing guidance. Table B.30 provides examples of guidance from a range of authorities. Key points to consider are:

- It is not good practice to charge for guidance as it will change the perceived status of the guidance and create potential conflicts of interest for future supervision and enforcement.
- Guidance can be collated to form packages or 'kits' to assist with specific topics (e.g. a new application, an audit). The Danish OSH authority offers an example.
- Guidance can use case study examples (e.g. French aviation authority). Real world examples of how individual RUs/IMs have met the requirements of the safety regulatory framework can be useful to share amongst other RUs/IMs.
- Guidance can comprise 'tools' for use by RUs/IMs, such as checklists and even online courses (e.g. Latvian NSA, Irish OSH authority).
- Detailed audit guidance can include sharing the questions and requirements that will be used for SMS auditing and providing accompanying tools such as forms for creating hazard logs and carrying out gap analysis.
- Guidance can direct the market towards the pertinent points in the regulatory framework by issuing summaries.

3.7.4 Research

Competent authorities in other sectors can play a part in directing and even funding industry research. Table B.31 describes examples from the OSH sector.

NSA have a remit to make proposals to overcome deficiencies in the safety regulatory framework, and should also target supervision and enforcement action according to the principles. Research may assist with these goals if it can explore emerging problems and help identify priorities.

If the NSA does have sufficient funds—or believes there is value in doing so—it could follow some of the examples provided and commission research into relevant topics. However, care should be taken to avoid funding research that could create market inequalities (e.g. the example from the Belgian OSH authority) or encroach on the responsibility of RUs and IMs to manage their own risks (e.g. the Italian OSH authority).

It would be good practice for NSA to define how RUs/IMs may lobby for access to research funding. That is not to say that NSA should follow the examples given here and create their own funds for research—rather assist with directing research needs to bodies that may have funding available (be it at a national or European level, e.g. ERAC). Presenting information on how to access such funding (e.g. via the NSA website) is good practice. If NSA do have sufficient resources to fund research, it is important that the research either assists the NSA with targeting its supervision and enforcement activities or explores potential safety benefits that would apply to the whole market rather than specific RUs/IMs.

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.4/5) and 1169/2010 (Annex III.4/5):

"National safety authority supervision activity shall be targeted primarily at those activities which a national safety authority believes give rise to the most serious risks or where the hazards are least well-controlled.

National safety authorities shall decide on priorities to use their resources effectively but the decision on how best to do that should rest with each individual national safety authority."

CSM on Supervision (Annex 1.4)

"Based on experience gathered during supervision activities, the national safety authority shall at regular intervals

iv. make any necessary recommendations to the Member State to overcome any deficiencies in the safety regulatory framework."

Directive 2004/49/EC (Article 16.2(f))

"Monitoring, promoting, and, where appropriate, enforcing and developing the safety regulatory framework including the system of national safety rules"

3.7.5 Awards

One practice used by authorities in other sectors is to award dutyholders for specific achievements (Table B.32). Typically these awards are safety related, and draw attention to those examples that represent good practice in the opinion of the authority. Whilst such awards may have a place in other industries, they are not considered good practice for the rail industry. It is likely that awarding certain RUs/IMs for achievements could polarise the market and have a negative effect on market harmonisation and openness. If NSA wish to promote examples of good practice, conferences, case studies and other means of neutral communication would be more appropriate.

3.8 Enforcement powers and penalties

This section discusses the enforcement powers that NSA have and the penalties that they can impose. The range of powers is explored in greater depth in subsection 3.8.1 and the methods of enforcement are covered in greater detail in subsection 3.8.2. Recommendations are provided throughout and a summary is given in subsection 3.8.3.

Table 3.35 shows that, of the 20 NSA responding to the questionnaire:

- Four (Germany, Spain, Netherlands and Finland) have the legal powers to take a full range of action to require RUs/IMs to rectify deficiencies, to revoke safety certificates/authorisations, to prosecute in court and to impose financial penalties.
- Ten (Sweden, Romania, Latvia, Poland, Bulgaria, Austria, Portugal, Czech Republic, Hungary, Norway) lack the powers to prosecute an RU or IM in court.
- Four (GB, Denmark, Channel Tunnel and Ireland) lack the powers to impose financial penalties.
- Estonia can only impose financial penalties and Lithuania can impose financial penalties as well as revoke a safety certificate or authorisation.
- France can require RUs/IMs to rectify deficiencies and it can revoke safety certificates/authorisations. In some very specific circumstances it can submit a case for the public prosecutor to consider. The Italian NSA also has the same powers although these are set to expand in the near future with the introduction of new, national legislation.

In addition, GB, Latvia, Netherlands and the Channel Tunnel can use further powers to halt rail traffic or certain vehicles if there is evidence that they pose a health and safety hazard. In GB, such powers are assumed under the EC's Regulation on Accreditation and Market Surveillance which raises the question as to whether other NSA should have equivalent powers.

Table 3.35: NSA enforcement powers (questionnaire findings)

NSA	Require RUs/IMs to rectify any deficiencies	Revoke a safety certificate or authorisation	Prosecute RUs/IMs in court	Impose financial penalties	Other, please specify:	Comments
Great Britain	Yes	Yes	Yes	No	Powers under the EC's Regulation on Accreditation and Market Surveillance to: withdraw, prohibit or restrict certain products which are unsafe; recall, withdraw or prohibit products which present a serious risk; and destroy or render inoperable products presenting a serious	-

NSA	Require RUs/IMs to rectify any deficiencies	Revoke a safety certificate or authorisation	Prosecute RUs/IMs in court	Impose financial penalties	Other, please specify:	Comments
					risk.	
Sweden	Yes	Yes	No	Yes	Leave information to prosecutor for their decision of going to court or not.	Financial penalties are only "submit to the penalties". (If you don't fix the non-compliance as agreed – penalties can be forced to RU /IM)
Estonia	No	No	No	Yes	No	Of course NSA wouldn't exert strong legal power all the time; it maybe happens 3–4 times a year.
Lithuania	No	Yes	No	Yes	No	Right to revoke a safety certificate or authorisation is settled in 'Rules on safety Certification of Railway Undertakings and Infrastructure Managers', adopted in 2011. Right to impose financial penalties (levy fines) is settled in Article 112 (1) of the Administrative Code.

NSA	Require RUs/IMs to rectify any deficiencies	Revoke a safety certificate or authorisation	Prosecute RUs/IMs in court	Impose financial penalties	Other, please specify:	Comments
Romania	Yes	Yes	No	Yes	No	-
Germany	Yes	Yes	Yes	Yes	No	-
Denmark	Yes	Yes	Yes	No	No	-
Spain	Yes	Yes	Yes	Yes	No	-
Latvia	Yes	Yes	No	Yes	Stop movement of trains, stop utilisation of rolling stock or railway infrastructure	-
Poland	Yes	Yes	No	Yes	No	Although the list of NSA enforcing tools specified in the act on railway transport is rather wide (financial penalties, closing the line or excluding the vehicle from operation), their execution is not very common. Financial penalties are applicable, when the supervised entity is not going to comply with NSA decisions. The system is a bit complicated as it's always linked with the administrative procedure, which is very formalised.

NSA	Require RUs/IMs to rectify any deficiencies	Revoke a safety certificate or authorisation	Prosecute RUs/IMs in court	Impose financial penalties	Other, please specify:	Comments
Bulgaria	Yes	Yes	No	Yes	No	-
Austria	Yes	Yes	No	Yes	No	-
Portugal	Yes	Yes	No	Yes	No	-
Czech Republic	Yes	Yes	No	Yes	No	The administrative process is very complicated. The NSA has to bring evidence that something is against legislation. This is very difficult.
Netherlands	Yes	Yes	Yes	Yes	Yes – halt the rail traffic.	
Channel Tunnel	Yes	Yes	Yes (GB only)	No	Yes. In respect of the GB half of the channel tunnel: there are full 'Health & Safety' enforcement powers as health & safety law – including enforcement that can be applied.	
Hungary	Yes	Yes	No	Yes		
Norway	Yes	Yes	No	Yes		
Ireland	Yes	Yes	Yes	No		Two levels of fines levied by Courts on conviction (summary conviction and indictment). Legislation enables us to serve improvement and prohibition

NSA	Require RUs/IMs to rectify any deficiencies	Revoke a safety certificate or authorisation	Prosecute RUs/IMs in court	Impose financial penalties	Other, please specify:	Comments
						notices.
France	Yes	Yes	No	No	Yes. EPSF may establish records that provide a basis for criminal prosecution (after transmission to the public prosecutor). This includes: - The fact that an RU/IM operates a motor vehicle in violation of provisions relating to registration or authorisation of commercial operations. - The act of driving a train without being the holder of the license and the documents required by safety regulations or the conduct of a person who trains others but does not hold these documents.	
Finland	Yes	Yes	Yes	Yes	No	All four mentioned above (NSA will of course not itself be the prosecutors). The financial is a penalty fee.
Italy	Yes	Yes	No	No	Yes	Not yet, a Legislative Decree about Penalties is currently in progress and it is expected to be adopted within a few months.

NSA must submit to the European Commission a list of penalties that can be applied under Article 32 of Directive 2004/49/EC.

Table B.33 describes these penalties for some NSA alongside the frequency of application. Six NSA report issuing at least one penalty in the last 12 months (time period is approximate and in some instances based on the last full annual reporting period). Of those NSA that did report financial penalties, the highest number was reported by the GB NSA (although these penalties were all associated with prosecutions – the GB NSA has no powers to issue penalties itself). Only Bulgaria, Poland and the Channel Tunnel imposed no penalties.

3.8.1 Range of enforcement powers

This section explores further the range of enforcement powers available to NSA, whilst the subsequent section considers how enforcement measures are applied (Section 3.8.2). A range of enforcement powers is desirable in order to fulfil the principles of transparency and consistency (Regulations 1158/2010 and 1169/2010). Specifically, without a reasonable range of powers, it is questionable as to how proportionate an NSA can be given that violations of increasing severity could require enforcement action to escalate proportionately. The Safety Directive makes further reference to the range of enforcement powers.

The desktop review of other authorities and the follow-up interviews with NSA produced further details on the range of enforcement methods available.

Table B.34 shows that examples of the widest range of enforcement powers can be found at the Dutch NSA (which has nine enforcement methods in a hierarchical pyramid of response) and the Danish OSH authority (seven courses of action which enable it to vary its response considerably when addressing a breach of the regulations).

A more typical range that is representative of many NSA (as shown earlier in Table 3.35) is demonstrated by the GB NSA (which draws comparisons with the enforcement measures used

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.2/3) and 1169/2010 (Annex III.2/3):

"National safety authorities shall apply the principle of proportionality between enforcement and risk. Action taken by a national safety authority to achieve compliance or bring railway undertakings/infrastructure managers to account for not meeting their legal obligations shall be proportionate to any risks to safety or to the potential seriousness of any non-compliance, including any actual or potential harm.

3. National safety authorities shall apply the principle of consistency of approach to ensure… a similar approach in similar circumstances to achieve similar ends.

Directive 2004/49/EC (Article 16.2(e/f))

"the… amendments and revocation of relevant parts of safety certificates and of safety authorisations"

"Monitoring, promoting, and, where appropriate, enforcing and developing the safety regulatory framework including the system of national safety rules"

(Article 32)

The Member States shall lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate, non-discriminatory and dissuasive.

by the GB OSH authority) and the Danish NSA. However, the Danish NSA describes its range as "quite out of proportion".

A wide range is not necessarily of value if some of the measures are difficult to enforce. Although the Polish NSA has similar scope for enforcement as other NSA, it reports a situation where fixed financial penalties would be an appropriate additional measure—not only to provide consistency with other Polish authorities but also because some of its existing enforcement methods (especially financial penalties) are difficult to access. It is worth noting that not all NSA believe that financial penalties are a necessary enforcement tool; the GB NSA provided a considered argument against such methods (although the same NSA can access financial penalties through prosecutions).

3.8.2 Use of enforcement methods

Table B.35 offers examples of how different authorities have applied the enforcement measures available to them.

Some are examples that show how NSA may not yet be meeting the principles of supervision when it comes to their enforcement activity. Three key findings were considered as not meeting a baseline level of good practice:

- An insufficient range of enforcement measures can lead to NSA making compromised decisions that have the potential to violate the principles of supervision. For example, the Danish NSA is wary of revoking certificates/authorisations due to the inevitable disruption yet it is aware that lesser measures may not be sufficiently harsh for some breaches.
- Inflexible and overwrought administrative procedures may, in extreme cases, protect the rights of RUs/IMs at the expense of railway safety. The Czech NSA describes complex administrative procedures that can severely restrict its ability to take immediate action for safety reasons as the RU/IM has such broad rights for appeal. This effect is compounded by poorly defined regulations that create ambiguity and market confusion.
- Enforcement action can be implemented in a way that does not address the fundamental safety hazard. For example, the Czech NSA described issuing a penalty to an IM but had not taken further measures to ensure that the IM had changed its SMS or even recognised it was at fault.

The following are examples of how authorities can demonstrate baseline good practice during enforcement activities:

- Use a standardised report form for all cases that may lead to enforcement action. A report form can help prompt staff to follow a decision-making process (consistency) and will provide a record of how evidence has been used to support a decision (accountability).
- Report all enforcement action to the executive board of the RU/IM. This will ensure that remedial action can be implemented at all levels in the organisation and is not localised to the part of the organisation where the breach occurred.
- Consider how and when each enforcement measure from the full range may be necessary, even if there have not yet been opportunities to apply all enforcement

measures. Some NSA use only a few of their enforcement powers to achieve market compliance and not all have considered how to apply the full range of enforcement measures (e.g. the Spanish NSA). It is a risk— both to railway safety (due to the unresolved breach) and to supervising in accordance with the principles—not to consider how the enforcement response might be escalated if an RU/IM fails to comply. The principles of supervision would be violated if an NSA used enforcement measures without a clear process or strategy for doing so.

- Explain to RUs/IMs, by way of an enforcement policy statement or similar, the purpose of enforcement action and the principles that will be applied when carrying out enforcement. Although these principles exist in the regulations, there is value in each NSA describing to the market how it will enforce in accordance with these principles (as demonstrated by the GB OSH authority).
- Specify applicable financial penalties (precise amount or range). NSA should define internally the criteria that may affect the size of penalty, if appropriate.

When enforcing, safety authorities can demonstrate good practice that goes further than the baseline if they:

- Combine enforcement measures to increase the available range and proportionality (e.g. prosecuting a dutyholder in conjunction with issuing an improvement notice; GB OSH authority).
- Apply a suitable level of discretion for some enforcement measures due to the wider impact they may have (e.g. prosecutions). The GB OSH authority described how they would use discretion when considering prosecution as it was reported to be an effective way to draw attention to the need for compliance and maintenance of legal standards.
- Engage in dialogue with RUs/IMs. Dialogue is a valuable element of any enforcement action and it can also be an enforcement activity in itself. Authorities may use and promote a dialogue-based approach to develop a 'just culture' in the market that avoids blame and focuses on systems-based safety management (e.g. the Irish aviation authority, the Austrian, Danish and French NSA).
- Consider bringing forward full SMS reassessment for an RU/IM that has committed serious regulatory breaches or non-compliances. The Danish NSA advocates this option when the alternative of revoking the safety certificate or authorisation is too disruptive. It sends a serious message to the RU/IM and still ensures that the organisation makes fundamental changes.

NSA that wish to demonstrate an even higher level of good practice would be advised to consider if it would be feasible to:

- Differentiate financial penalties according to dutyholder factors (e.g. size), as demonstrated by the Danish OSH authority. If the factors on which differentiation is decided are valid, this may be a way of delivering proportionate enforcement, which would also be consistent if it was in accordance with a defined policy.
- Establish a working group to review the existing range of enforcement measures, especially if the current national regulatory framework does not provide a clear,

consistent legal basis for enforcement under the European regime of operations. The working group would include the NSA and the Ministry that has authority for national regulations. The Dutch NSA has adopted precisely this approach in order to update its enforcement measures to reflect changes in railway operations. It is working towards a more transparent enforcement structure where each breach can be accompanied by an administrative fee as a sanction and is supported with a firm legal basis.

- Introduce an innovative system for indicating to the market and to the public the level of compliance each RU/IM has achieved with its SMS. The Danish OSH has adopted a system of coloured 'smileys'. It is important that the process and criteria used are transparent.

3.8.3 Summary

The enforcement powers of NSA vary considerably. NSA appear to differ most with regard to the right to impose financial penalties or prosecute an RU/IM in court. It is recommended that the enforcement tools available to NSA should:

- Cover a range that is sufficiently wide to respond proportionately to different situations. The range should show clear escalation of severity. There should not be 'gaps' in the range of enforcement tools (e.g. there should be sufficient options between the least severe and the most severe penalty to enable a proportionate response).
- Be well-publicised so that the industry is aware of how regulatory violations and non-compliances will be dealt with.
- Be accessible. The procedures for accessing these tools should be well-documented so that staff know how to initiate use of a penalty for any given situation. A system of penalties may not be proportionate or consistent if the difficulty of accessing some tools contributes to them not being used. Complexity of accessing a penalty should not be a disincentive for using it.

Key findings:

- Multiple options for enforcement may be necessary in order for an NSA to enforce proportionately.
- Enforcement measures can be ineffective if not supported by appropriate national legislation.
- Dialogue with RUs/IMs can be an important part of enforcement.
- Enforcement action can be affected by the need to maintain an operating railway and/or government influences.
- Some enforcement action may fail to address the fundamental risk to safety that led to the initial violation or non-conformity.

Good practice recommendations:

- Each NSA should have a range of accessible enforcement powers to enable it to escalate its response to a safety hazard or non-conformity without violating the principle of proportionality.
- Enforcement action should ensure that the fundamental safety risk is addressed. Financial penalties that do not require evidence of corrective action may be ineffective.
- Enforcement policies and processes should be structured and documented publicly.
- Enforcement decisions should be reported to RU/IM executive board.
- NSA may wish to consider if a working group can be formed with relevant government departments to update national legislation so it better supports enforcement.

The range of penalties should also be part of an enforcement system that recognises RUs/IMs are often providing an essential service; penalties that effectively cease operation of an RU or IM should be considered carefully and NSA should have at their disposal tools that enable them to deal effectively with safety hazards whilst maintaining essential services.

The recommended further steps to provide a baseline level of good practice are to ensure that enforcement is structured and defined. This can be achieved by introducing a standardised report form for all case evidence that may lead to enforcement, establishing internally and externally the policies, procedures and measures by which the authority will enforce, and ensuring that enforcement decisions are delivered to the executive board of the RU/IM.

Authorities can exceed their baseline level of good practice by engaging in open dialogue with RUs/IMs to ensure that enforcement action achieves its aim of delivering improvements to safety. Enforcement measures may be adapted for this purpose. Further good practice may involve establishing proportionate and consistent criteria by which penalties may be varied, and introducing innovative public systems for rating RU/IM compliance.

A final point to note is that dissatisfaction with enforcement powers exists across several NSA. The Dutch NSA is demonstrating good practice by forming a working group to discuss improvements with the relevant departments within its government. Other NSA may have concerns about their enforcement powers but do not have an option to discuss them at present (e.g. the Danish NSA) and/or simply have not explored the reaches of their enforcement options as yet (e.g. the Danish NSA and the Spanish NSA).

3.9 Proportionality and consistency in supervision and enforcement

The regulated principles of supervision require that NSA are proportionate and consistent when supervising and enforcing the market. This section discusses how proportionate and consistent NSA rate themselves to be and compares this with responses to case study examples that also test these principles.

Applicable safety regulatory framework:

Regulations 1158/2010 (Annex IV.2/3) and 1169/2010 (Annex III.2/3):

"NSA shall apply the principle of proportionality between enforcement and risk. Action taken by a NSA to achieve compliance or bring RUs/IMs to account for not meeting their legal obligations shall be proportionate to any risks to safety or to the potential seriousness of any non-compliance, including any actual or potential harm.

3. NSA shall apply the principle of consistency of approach to ensure that a NSA takes a similar approach in similar circumstances to achieve similar ends."

3.9.1 Self reported ratings of proportionality and consistency

The majority of NSA (16) reported that the supervision and enforcement action they took was either 'very' or 'completely proportionate' to the type of infringement (Table 3.36). Possible exceptions to this were:

- Denmark, which is openly strict with any "sloppiness and lack of procedures".
- Poland, which is still operating under two regulatory regimes (the EU regime and its own national regime) and is also under-resourced.
- Portugal, Hungary, Italy and the Czech Republic. The latter acknowledges that its state railway "has been operating for many years in the same way" and it would appear that its failure to comply on occasion gives rise to disproportionate action.

A small majority of NSA (14) also reported that their supervision and enforcement activity was 'very consistent' or 'completely consistent'. With the exception of the Czech Republic, which was only 'a little consistent'. All other NSA were 'quite consistent'.

Table 3.36: NSA ratings of proportionality and consistency

NSA	Proportionate (61)	Examples	Consistent (71)	Examples
Great Britain	Completely proportionate		Very consistent	
Sweden	Very proportionate		Quite consistent	Different assessment of RUs and IMs (small IM on sidetracks don't need

NSA	Proportionate (61)	Examples	Consistent (71)	Examples
				full SMS)
Estonia	Very proportionate		Quite consistent	When acts are changes so, that NSA's actions may be not so consistent or look not so consistent
Lithuania	Very proportionate		Very consistent	
Romania	Completely proportionate		Very consistent	
Germany	Very proportionate		Very consistent	
Denmark	Quite proportionate	No	Quite consistent	If we discover an error has occurred by chance, but otherwise there is a procedure that covers this topic, we will give a minor deviation. But if there is sloppiness and lack of procedures, we will be more strict.
Spain	Very proportionate		Very consistent	
Latvia	Very proportionate		Very consistent	
Poland	Quite proportionate		Quite consistent	The problem of consistency arises from the structure of NSA, which is divided into several regional departments. This along with lack of resources complicates the coordination of the decisions among different departments. Bear in mind that the problem of consistency refers mainly to old approach of supervisory activities. There is more consistency in the supervisory activities linked with SMS. It's because the teams established to carry out separate supervisory activities consist always of one or two employees representing the

NSA	Proportionate (61)	Examples	Consistent (71)	Examples
				certification team and one or two employees from the selected regional department of UTK. The problem is also the shortage of resources. Currently only two employees deal with the certification process in total and two people in each regional division. That makes a total of only 16 people available for the supervisory activities.
Bulgaria	Very proportionate		Very consistent	In general the NSA of Bulgaria undertakes the following actions in case of established non-compliance with the safety regulation: It issues penalties and makes formal prescriptions for remedy of the inconsistency. As a follow-up activity the NSA makes more frequent checks of the RU/IM in breach and if there are findings that the non-compliances have not been remedies it may proceed with a procedure for revocation of the safety certificate/ safety authorisation
Austria	Very proportionate		Very consistent	Multiple examples within the same RU/IM will eventually lead to different, stronger measures.
Portugal	Quite proportionate		Very consistent	
Czech Republic	Not at all proportionate	State railways has been operating for many years in the same way, but they do not follow completely all requirements done by legislation.	A little consistent	

NSA	Proportionate (61)	Examples	Consistent (71)	Examples
Netherlands	Very proportionate	No, because if we think the action is not proportionate, we won't take it	Quite consistent	An illegal (unauthorised) vehicle on the main line gets a different penalty to the one which is a few metres outside their company premises on a far away track. Penalty related to risk for others.
Channel Tunnel	Very proportionate		Completely consistent	No enforcement action taken on concession.
Hungary	Quite proportionate		Quite consistent	
Norway	Very proportionate		Quite consistent	
Ireland	Very proportionate	NSA use enforcement powers laid down by legislation.	Very consistent	
France	Completely proportionate		Completely consistent	An internal EPSF helps to qualify the findings of audits ensuring equity between auditees.
Finland	Very proportionate		Very consistent	
Italy	Quite proportionate		Very consistent	Prescriptions on similar safety certificates concerning similar non-compliance that should ask same timing and modalities. Interruption/suspension of the possibility to ask for further services until the elimination of the non-compliances of the safety certificate.

3.9.2 Supervision examples: case studies

To explore the application of the principles of consistency and proportionality, NSA were invited to consider eight case studies in the questionnaire and then indicate the enforcement response that would be issued by their authority to each example. The case studies are presented in Appendix A.

The GB NSA provided the case study examples, a description of the action it took and its reasons for taking such action. Given that the GB NSA was in possession of the evidence in each case, and has demonstrated that it meets several of the good practice recommendations in this report, the action taken by other NSA was compared with the action taken by the GB NSA for each set of examples. Thus, to explore proportionality across the market, the action of other NSA has been considered according to whether it was similar, harsher or softer than the action taken by the GB NSA. Different responses have to be taken in the context of different interpretations of the examples and also what enforcement powers individual NSA may have. Where other NSA differ markedly, consideration will be given as to whether the response to each example demonstrates proportionality.

To explore the consistency with which NSA may enforce, for each of the four main enforcement actions it uses, the GB NSA provided two case studies. These case studies are paired in sections 3.9.3–3.9.6 according to the enforcement action taken. Eight examples were selected so that there would be four pairs of cases with approximately equivalent enforcement responses:

- Case studies 1 and 7 resulted in written guidance being issued.
- Case studies 3 and 6 resulted in verbal guidance being issued.
- Case studies 2 and 5 resulted in prosecution.
- Case studies 4 and 8 resulted in enforcement notices being issued.

For each pair of examples, the consistency with which other NSA responded was considered.

3.9.3 Case study answers – Examples 1 and 7

Table B.36 presents the enforcement responses from NSA to case study 1 (a loose panel on a rail vehicle) and case study 7 (working at height in a station).

For Examples 1 and 7, the GB NSA recommendation was to **'issue written guidance'**.

The answers provided by the GB NSA are the same for both examples. These answers should not be considered as a definitive benchmark—alternative approaches may be justified as more appropriate—but they do provide a point of comparison for other countries.

3.9.3.1 Example 1 – loose panel on a rail vehicle

- Eight NSA (Estonia, Denmark, Spain, Portugal, Austria, Italy, Germany and the Channel Tunnel) would take the same action as GB. Denmark would open a dialogue with the operator to discuss SMS adjustments might be necessary to prevent future occurrences. Austria may also issue a formal enforcement notice.
- Nine NSA would take harsher action than GB (Sweden, Lithuania, Romania, Bulgaria, Netherlands, Hungary, Norway, Ireland and Finland). The Netherlands would expect the operator to issue an action plan to 'prove' it will not happen again. Sweden and Ireland would expect a similar plan as part of its formal enforcement action. Bulgaria would appear to take a phased approach that includes specifying the action that must be taken ("ways of correction of the

problem"). A financial penalty would be applied based on the Member State's own legislation (Railway Transport Act), which would increase if the changes were not made. Romania would issue a fixed fine.

- Two countries would take weaker action than GB (Poland, Czech Republic).
- One country (Latvia) would not investigate the incident at all as it stated that the RU should conduct its own investigation.

3.9.3.2 What does Example 1 show regarding proportionality?

Most countries would take harsher action and in doing so may have overlooked or not accounted for the rarity of the incident, the existing SMS procedures and the technical solution (modified panel fasteners) that had already been implemented. Harsher action is arguably disproportionate.

3.9.3.3 Example 7 – working at height

- Four NSA would take the same action as GB (Estonia, Lithuania, Portugal and Germany).
- Six NSA (Romania, Latvia, Netherlands, the Channel Tunnel, Hungary, and Norway) would take harsher action than GB. The Netherlands would expect the operator to improve its SMS. The other NSA would issue formal enforcement notices, with Latvia seeking to amend procedures that contributed to the event. It is interesting that the Channel Tunnel would seek a formal enforcement notice, which contrasts with the written guidance the GB NSA would issue (note that staff from the GB NSA are jointly responsible for the safety authority of the Channel Tunnel).
- No country would take weaker action than the GB NSA.
- Eleven countries (Czech Republic, Bulgaria, Poland, Spain, Denmark, Sweden, Austria, Ireland, France, Finland and Italy) reported that this example would not fall under the remit of their NSA. Whilst the NSA may play a part in notifying other relevant authorities of the incident, it would not take any enforcement action itself.

3.9.3.4 What does Example 7 show regarding proportionality?

The NSA from most countries would not respond to this incident. This indicates that the remits of NSA differ quite considerably across Member States.

The six NSA that would respond with harsher action may not be acting disproportionately if they believe that the RU/IM's SMS should have prevented the sub-contractor starting work with a safety system that had not been approved. Whilst appropriate action had been taken, the RU/IM had still failed to risk assess properly in the first instance.

3.9.3.5 What do Examples 1 and 7 show regarding consistency?

If the two examples here can be considered equivalent in terms of the action required then it can be reported that GB, Estonia, Portugal, Hungary, Germany and Norway took consistent action.

The consistency of 11 NSA (Sweden, Denmark, Spain, Latvia, Poland, Bulgaria, Czech Republic, Channel Tunnel, Ireland, France, Finland and Italy) cannot be assessed with these examples because at least one of the examples falls outside the remit of each of these NSA.

Three NSA (Lithuania, Romania, and Netherlands) would take different action for each example.

3.9.4 Case study answers: Examples 3 and 6

Table B.37 presents the enforcement responses from NSA to case study 3 (unsafe access to a station roof) and case study 6 (a missing/damaged fence near a platform).

For Examples 3 and 6, the GB NSA recommendation was to **'issue verbal guidance'**.

3.9.4.1 Example 3 – unsafe access to a station roof

- Only Estonia would take the same action as GB.
- Seven NSA (Lithuania, Romania, Latvia, Portugal, the Channel Tunnel, Hungary, and Norway) would take harsher action. All would take formal enforcement action in the form of a notice or other prescription to amend procedures. Again, it is interesting that the response from the Channel Tunnel diverges from the GB response.
- No countries would take weaker action.
- Thirteen countries (Sweden, Denmark, Spain, Poland, Bulgaria, Czech Republic, Netherlands, Austria, Ireland, France, Germany, Finland and Italy) reported that this example would not fall under the remit of their NSA. Whilst the NSA may play a part in notifying other relevant authorities of the incident, it would not take any enforcement action itself. The Polish NSA reported that this division of responsibility for supervision and enforcement was a significant problem. For example, its Building Control Authority is responsible for authorising infrastructure that can be subject to the TSI and yet there is no reference to the TSI in Polish building law.

3.9.4.2 What does Example 3 show regarding proportionality?

Most countries would take no action which highlights how the regulatory regimes in several Member States divide the responsibilities that NSA might be expected to have. Of those countries that have a remit to take action, most would take harsher action than GB and Estonia. It would seem that the tacit agreements to adopt safe systems of work in the example given would not be sufficient reassurance for these NSA, which would seek to support their position with legal tools. This may not help develop less formal, trust-based relationships between NSA and operators—the sort of relationships that could help promote the regulatory framework and encourage operators to follow it proactively. However, it could be argued that formal enforcement action is not disproportionate for a situation where the operator's SMS had not highlighted the problem.

3.9.4.3 Example 6 – missing/damaged fence near a platform:

- Two countries (Denmark, Spain) would take the same action as GB. Bulgaria stated it would make a further inspection to check the fence: it was not clear how it would respond to the outcome of this inspection so this action is considered equivalent in strength to verbal guidance as the NSA has elected to continue monitoring the situation.
- Twelve NSA (Estonia, Lithuania, Romania, Latvia, Portugal, Austria, the Channel Tunnel, Hungary, Norway, Ireland, Germany and Italy) would take harsher action in the form of formal enforcement action, fixed fines or written guidance. Once more, the Channel Tunnel's response is harsher than the GB response.
- The Netherlands would "compliment them [on] a mature safety management system", which may be comparable to verbal guidance if the NSA is simply discussing the positives of the approach that the IM has taken to this problem.
- Four countries (Sweden, Poland, Czech Republic and Finland) reported that this example would not fall under the remit of their NSA. It is potentially a concern that national safety regulatory frameworks in these countries do not cover fenced protection of the railway by the IM(s).

3.9.4.4 What does Example 6 show regarding proportionality?

Those countries that would issue some form of verbal guidance, or would monitor the situation, have clearly recognised that the IM is responding to the situation promptly. It is potentially disproportionate to issue a fine or enforcement notice to an IM that is acting to resolve a problem on the day it is made aware of it—and can show that it has acted similarly in the past. Estonia, Latvia, Portugal, Italy and Ireland would all issue written guidance which does not appear disproportionate but perhaps lacks the immediacy and responsiveness of verbal dialogue between the NSA and IM.

3.9.4.5 What do Examples 3 and 6 show regarding consistency?

Estonia, GB, Romania, the Channel Tunnel, Hungary and Norway are broadly consistent in the severity of their responses. Lithuania, Latvia and Portugal are not consistent in their response to these examples. The remaining countries had NSA without an explicit remit to address one or both examples so consistency estimates cannot be made.

3.9.5 Case study answers: Examples 5 and 2

Table B.38 presents NSA enforcement responses to case study 5 (missing/damaged fence next to a nature reserve) and case study 2 (a loose barrier between carriages).

For Examples 5 and 2, the GB NSA recommendation was to **'prosecute in court'**.

3.9.5.1 Example 5 - missing/damaged fence next to a nature reserve

- Only the Channel Tunnel would take the same action as the GB NSA.
- Sweden, Poland, France and the Czech Republic would not have a remit to deal with the missing trackside fence described in this example. The Polish NSA would try to provide written guidance to help address the problem but ultimately would

have to transfer the problem to a different authority. The NSA of the Czech Republic probably would not even become aware of the problem which is potentially of concern given the chance of a serious incident.

- The remaining 14 NSA would take weaker action than the GB NSA, of which the majority would issue some type of formal enforcement notice. The NSA that would do so were in Romania, Denmark (which would add specific requirements to implement an action plan that would be subject to NSA supervision), Spain (for private IMs only – public IMs would be subject to contractual enforcement action), Bulgaria (including sliding scale of fines depending on how the issue was addressed), Netherlands (which would also require an action plan and may impose a fine for the lack of repair work to date), Hungary, Norway, Ireland, Germany (which would require the fault to be rectified and the SMS updated), and Finland (which would require written confirmation that action has been taken). Fixed fines would be issued by Lithuania, Austria, Italy and Portugal; Latvia would issue other financial penalties for the infringement. Estonia had the weakest response, preferring to send written guidance only.

3.9.5.2 What does Example 5 show regarding proportionality?

Although only two NSA would prosecute in court (GB and the Channel Tunnel), it was evident that the majority of NSA issuing formal enforcement notices or penalties were attempting to reprimand the IM for its negligence whilst simultaneously seeking changes to procedures that might improve future responses to similar incidents. For four NSA, the lack of a remit to deal with such as issue is of concern and it may be worth exploring the implications of this further.

3.9.5.3 Example 2 - loose barrier between carriages

- Only the Channel Tunnel would take the same action as the GB NSA.
- Nine NSA would issue a formal enforcement notice: Estonia, Denmark (which would ban use of the faulty material/equipment until made safe, expect SMS changes to prevent reoccurrence and, if any of the deadlines for these actions are not met, would revoke the RU's safety certificate), Spain (which would focus on improving maintenance plans), Netherlands, Hungary (which would also revoke the safety certificate of the RU/IM, if necessary), Norway (which may report the incident to the police and would also pass it on to the NIB to follow up), Ireland, Germany and Italy.
- Four NSA would take other formal enforcement action – Sweden (which would require an action plan for maintenance and checks, plus investigation of communication between operating staff and maintenance staff), Finland (which would also ask for clarification of action and may investigate if the NIB declines to), Bulgaria (which would prescribe changes and a sliding scale of fines contingent on speed of compliance), and Poland (although this NSA stated that the issue would likely be addressed by the NIB first and then referred to the NSA for enforcement – at which point failure to comply with the notice would lead to prosecution).
- Three NSA would issue fixed fines (Lithuania, Portugal, Romania and Austria) and two would issue other financial penalties (Latvia – which would also implement an

SMS reassessment and Czech Republic – which acknowledged that it may not receive information on such an incident but if it did, it would focus on punishing the operator financially for poor vehicle condition).

3.9.5.4 What does Example 2 show regarding proportionality?

Several NSA were using formal enforcement actions or notices as part of a stepped approach to enforcement (e.g. Denmark, Poland), where there was an initial focus on addressing the immediate problem followed by obligatory requirements to improve procedures. If such activity can achieve the same outcomes as a court prosecution and in the same timescales then it could be argued that this type of response is proportionate. It could be argued that issuing a fixed fine does not help to differentiate an incident of this severity from a more minor incident and nor does it present opportunities to engage the RU in rectifying the procedures that may have led to the incident. In these respects, fixed fines and other financial penalties may not be a proportionate response (although Latvia would at least support such action with an SMS reassessment).

3.9.5.5 What do Examples 5 and 2 show regarding consistency?

Of the NSA that responded to both examples, 15 were broadly consistent in their response to each example (GB, Channel Tunnel, Lithuania, Denmark, Austria, Spain, Latvia, Bulgaria, Portugal, Netherlands, Hungary, Norway, Ireland, Finland and Germany).

Only Romania, Italy and Estonia were not consistent. These findings indicate that NSA had generally recognised similarities in the severity of both examples here and had responded accordingly.

Four NSA (Sweden, Poland, Czech Republic, and France) stated that one of the examples was not within their remit and so consistency could not be established.

3.9.6 Case study answers: Examples 4 and 8

Table B.39 presents the enforcement responses of NSA to case study 4 (poorly maintained road rail vehicle) and case study 8 (excessive working hours by RU staff).

For Examples 4 and 8, the GB NSA recommendation was to **'issue a formal enforcement notice'**.

3.9.6.1 Example 4 - poorly maintained road rail vehicle

- Twelve NSA would take the same action as the GB NSA and issue formal enforcement notices (or similar). Romania, the Channel Tunnel, Hungary and Norway provided no further details on the type of notice. Netherlands, Portugal, Denmark, Sweden, Austria and Latvia would all prohibit use of the vehicles until the faults had been rectified. Bulgaria included prescriptive conditions and a sliding scale of fines if the conditions were not met. Austria included a fixed fine. Germany would require that the fault be corrected.

- Lithuania and Italy would take potentially weaker action than the GB NSA in the form of fixed fines. Estonia would issue other financial penalties but would also remove affected vehicles from rail traffic.
- The Finnish NSA may ask for clarification on the issue and submit written guidance to the organisation at fault.
- Spain would take potentially harsher action than the GB NSA and remove the safety authorisation if the vehicles were being used on the national network.
- Poland, the Czech Republic and Ireland would again find that the incident fell outside the remit of their NSA and would probably be subject to decisions made by another authority. France did not provide a response.

3.9.6.2 What does Example 4 show regarding proportionality?

The findings suggest NSA would generally have a proportionate response to this type of incident and would act to stop further activity until underlying problems had been addressed. Financial penalties may not be disproportionate in such circumstances; however, they could be insufficient (e.g. Lithuania) unless they are delivered alongside other measures to address the underlying cause (e.g. Estonia).

Once again, Poland and the Czech Republic (and also Ireland) categorise such an incident as one that may fall outside the remit of their NSA.

3.9.6.3 Example 8 - excessive working hours by RU staff

- Six NSA (Lithuania, Spain, Latvia, Bulgaria, Hungary, and Norway) would take the same action as the GB NSA and issue formal enforcement notices. Bulgaria would supplement the notice with a fine.
- Estonia, Italy and Portugal would take potentially weaker action than the GB NSA in the form of fixed fines.
- Romania would take potentially harsher action than the GB NSA and remove the RU's Part B safety certificate. Netherlands may take similar action to prevent operation and would punish the RU to "the maximum". The Channel Tunnel would also diverge from the action of the GB NSA and seek a prosecution in court.
- Sweden, Poland, Austria, the Czech Republic, France, Germany, Denmark, Finland and Ireland would find that the incident fell outside the remit of their NSA and would probably be subject to decisions made by another authority. The Polish NSA would have a potential role in checking whether appropriate procedures are in place to control working hours at the RU although direct experience of this uncovered a problem with train drivers working for multiple RUs (therefore making it difficult to control total working time). Denmark reported shared responsibility, which for the NSA's part would focus on enforcing appropriate resource levels at the RU. Although Ireland would refer to the health and safety authority, it might still decide to issue an improvement notice or investigate contravention of an SMS.

3.9.6.4 What does Example 8 show regarding proportionality?

NSA were somewhat divided in their response to this incident. Issuing a formal enforcement notice appears proportionate given the RU's failure to comply with legislation as this would ensure measures were introduced to prevent reoccurrence. Harsher action (especially revoking safety certification) could be considered disproportionate given that no related safety incident occurred. However, the excessive nature of the infringement could warrant a financial penalty in addition to measures to rectify the underlying causes.

3.9.6.5 What Examples 4 and 8 show regarding consistency?

As with the GB NSA, Estonia, Latvia, Italy, Hungary, Norway and Bulgaria were consistent in their response to both examples, which were considered of equivalent severity.

Lithuania, Romania, Spain, Portugal, Netherlands, and the Channel Tunnel were not consistent in their response, primarily because harsher action was taken in response to Example 8.

Sweden, Denmark, Poland, Austria, the Czech Republic, France, Germany, Finland and Ireland did not have sufficient remit to cover both examples so consistency could not be assessed.

3.9.7 Summary

Figure 3.6 summarises how proportionate NSA were in response to the case studies. Those NSA that responded differently to the GB NSA but were considered to have responded proportionately are recorded in the chart as such. Half of the NSA in the survey reported that they would have issued a proportionate enforcement response to five or more of the eight case studies. When compared to how NSA self-rated their proportionality, it is perhaps clear why the NSA of Poland and the Czech Republic rated their proportionality as fairly low; for those case studies where they would issue an enforcement response, it was always softer than what was believed to be proportionate, and all the remaining cases were outside their remit. However, Denmark, Hungary and Portugal also rated that they were less than proportionate and yet the majority of enforcement responses from these NSA were considered proportionate. On balance, Romania, Lithuania and Estonia were the most disproportionate of the NSA and yet all three rated their enforcement activity as 'very' or 'completely' proportionate. Overall, the chart indicates that if NSA are not proportionate, they are more likely to enforce harshly than softly. It also indicates that there are a substantial number of NSA without a remit to supervise and enforce issues related to the workforce on the railways.

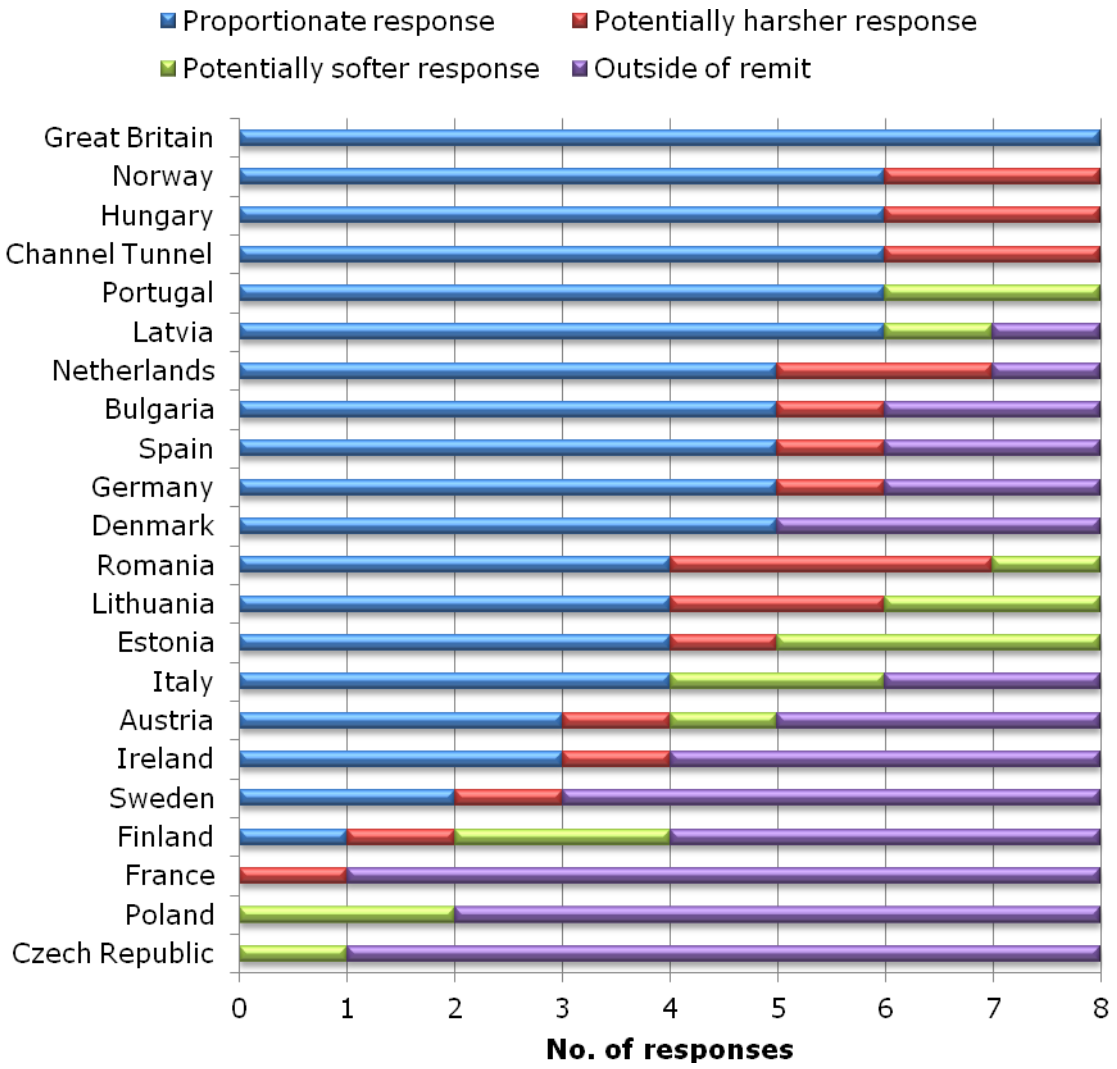


Figure 3.6: Summary of how proportionate NSA were in their enforcement responses to the case studies

Figure 3.7 summarises how consistent NSA were in their enforcement responses to the case studies. The eight examples were selected so that there would be four pairs of cases with approximately equivalent enforcement responses expected[5]. Nine of the NSA were consistent with their enforcement response to at least half of the cases they considered. Three of the NSA that rated their enforcement as rather inconsistent were actually either completely consistent when responding to the case studies (Norway and Hungary) or almost completely consistent (Estonia). The Netherlands was perhaps correct in rating its enforcement as rather inconsistent given that it provided seemingly inconsistent enforcement responses to half of the case studies. The remaining four NSA that rated their enforcement as inconsistent (Sweden, Denmark, Poland and the Czech Republic) could not be as assessed on this principle as the case studies were almost entirely out of their respective enforcement remits.

It should be noted that Romania and Lithuania were largely inconsistent in their enforcement responses and yet self-rated their enforcement as 'very consistent'.

[5] It should be noted that the examples were provided by the GB NSA and the equivalent enforcement decisions were based on the action taken by this NSA when it investigated these cases.

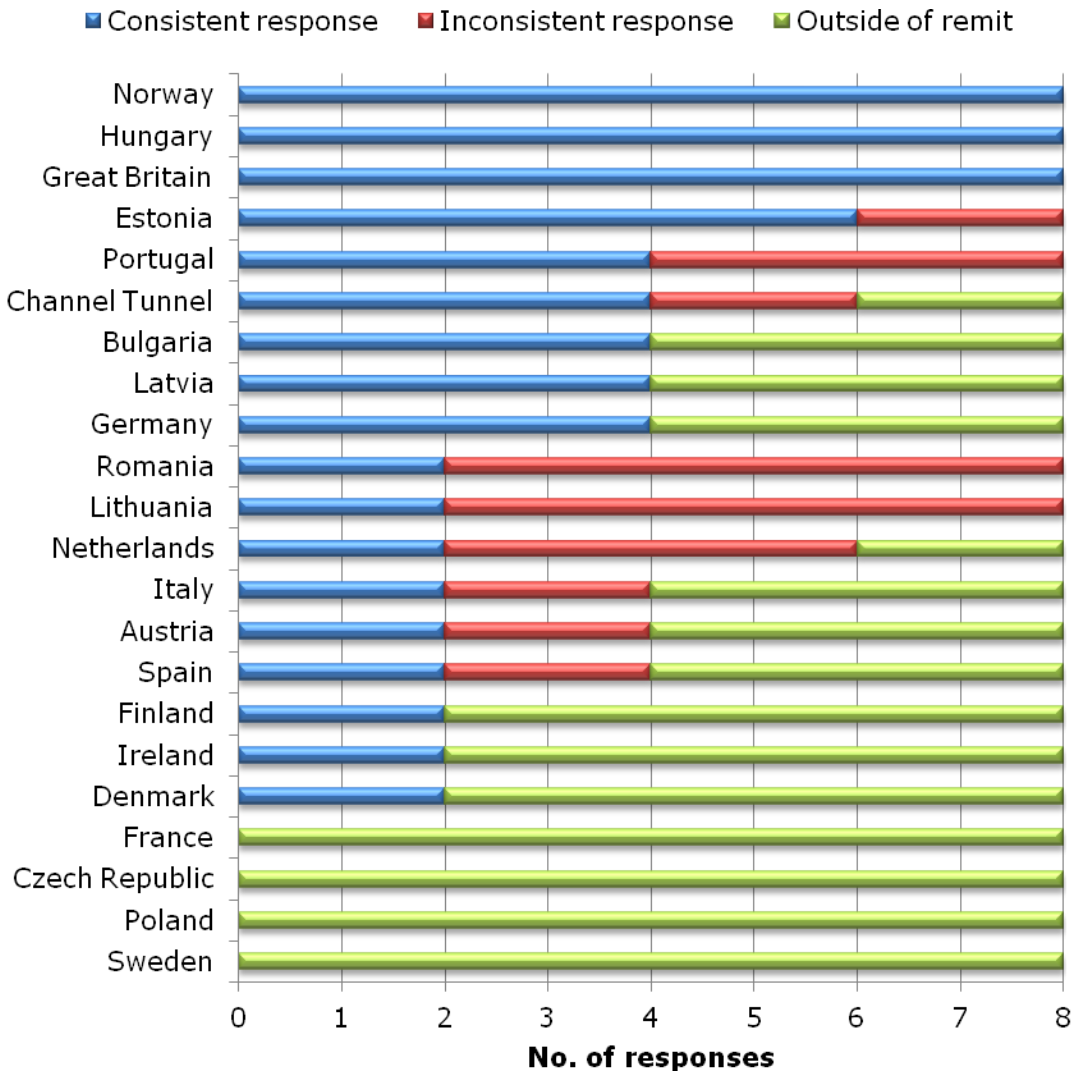


Figure 3.7: Summary of how consistent NSA were in their enforcement responses to the case studies

In summary, there is some disparity between how closely NSA report they are following the principles of proportionality and consistency, and how they responded to the case studies. Some of the findings are clearly affected by the range of enforcement powers available to NSA and the remit within which they operate. Nevertheless, it is evident that the NSA that are most consistent and proportionate in their enforcement are based in GB, Norway, Hungary, Portugal and the Channel Tunnel. When only considering those NSA which report that all of the issues are in their remit. Lithuania and Romania would appear to be the least consistent; the least proportionate would appear to be Lithuania, Romania, and Estonia.

3.10 Evaluating NSA performance

This section explores how well NSA perform the activities of supervision and enforcement, and the ways in which they evaluate their performance and seek to develop in the future. Specific subsections discuss self-reported changes in NSA performance (3.10.1), how performance is reported by NSA (3.10.2), how effective the safety regulatory framework is perceived to be (3.10.3), and how NSA work towards continuous improvement (3.10.4).

A summary and recommendations are provided in subsection 3.10.5.

Applicable safety regulatory framework:

Directive 2004/49/EC (Article 4.1)

"Member States shall ensure that railway safety is generally maintained and, where reasonably practicable, continuously improved, taking into consideration the development of Community legislation and technical and scientific progress and giving priority to the prevention of serious accidents."

3.10.1 Changes in NSA performance

Article 4.1 of Directive 2004/49/EC requires that Member States maintain and continuously improve railway safety. The supervision and enforcement activities of NSA have a role to play in satisfying this part of the Safety Directive. To help understand the extent to which each NSA might be helping its Member State to meet this requirement, the survey invited NSA to rate the change in their supervision/enforcement performance over the last 12 months.

Nine NSA reported that their supervision/ enforcement performance had improved over the past 12 months (Table 3.37). Eleven reported no change in performance and France declined to rate its performance.

The Netherlands reported a decline in performance after its remit was clarified as an enforcer of railway laws rather than having the ability to "promote and develop the safety regulatory framework including the system of national safety rules".

Table 3.37: Changes in NSA performance reported in previous 12 months

NSA	Change of supervision/ enforcement performance	Comments
Great Britain	Yes - performance has improved	We continue to strive to improve.
Sweden	Yes - performance has improved	More structured process- monitoring
Estonia	Yes - performance has improved	We started to use the risk assessment based method.
Lithuania	No - there is no change in performance	-
Romania	Yes - performance has improved	-

NSA	Change of supervision/ enforcement performance	Comments
Germany	Yes - performance has improved	Improvement through process-oriented supervision.
Denmark	Yes - performance has improved	The procedures have not been changed because we are working, we try continuously to improve. We are one of the countries that have been upfront in setting up a regime for a management system. From 2007 we made a legal framework for the RUs/IMs that they had to establish a SMS in line with international standards and we have been working on that path the whole way. So we have elaborated on the procedures but we have not changed them.
Spain	No - there is no change in performance	-
Latvia	No - there is no change in performance	The annual plan is fulfilled.
Poland	Yes - performance has improved	We have no experience in terms of supervision through SMS because of short time during which this supervision system works. We are now trying to shift from a system based on site inspections to the supervision through SMS.
Bulgaria	Yes - performance has improved	We think our performance has improved because of our direct implementation of the requirements of Regulation 1158 & 1169.
Austria	No - there is no change in performance	Due to the supervision/enforcement paper being currently under development there might be a change soon.
Portugal	No - there is no change in performance	-
Czech Republic	No - there is no change in performance	-
Netherlands	Yes - performance is worse	Recently we found out that we are not supposed to do all the tasks of article 16 of the Railway Safety Directive. We are not allowed to "promote and develop the safety regulatory framework including the system of national safety rules". Since then we 'only' enforce railway laws.
Channel Tunnel	No - there is no change in performance	

NSA	Change of supervision/ enforcement performance	Comments
Hungary	No - there is no change in performance	-
Norway	No - there is no change in performance	-
Ireland	Yes - performance has improved	We have a more formal strategy and plans in place. We are doing more now than previously.
France	-	The question is unclear and insufficiently precise. In a quantitative way, the number of tests has increased in recent years significantly.
Finland	No - there is no change in performance	However in future there should be a little increase in the resources of the NSA because of the reorganising of the NSA.
Italy	No - there is no change in performance	The fixed targets have been reached.

3.10.2 Outcomes of supervision plans: summarising safety performance

All NSA specified that they would share the results of supervision activities with affected RUs/IMs.

The forthcoming CSM on Supervision requires that all NSA will have an overview of the safety performance of the RUs/IMs that they supervise and of the Member State as a whole. With the exception of Portugal, all NSA had an overview of the safety performance of some or all RUs/IMs (Table 3.38). Four NSA (Romania, Bulgaria, the Channel Tunnel, Ireland) would share this safety performance data with other stakeholders. With regard to the safety performance of the Member State, all NSA with the exception of Italy had this overview.

Applicable safety regulatory framework:

CSM on Supervision (Annex 4.)

"The NSA shall

(a) share results with the relevant RU/IM of the effectiveness of their safety management system in delivering safe performance, including identifying areas of non-compliance on the part of the RU/IM.

(b) have an overview of the safety performance of the individual RUs/IMs operating in its Member State.

(c) publish and communicate its views on the overall safety performance in the Member State to relevant stakeholders.

(d) publish and communicate its views on the effectiveness of the safety regulatory framework to relevant stakeholders."

Table 3.38: Performance monitoring by NSA

NSA	Have overview of safety performance of each RU/IM?	Share relative safety performance of RUs/IMs with other stakeholders?	Have overview of safety performance of Member State?
Great Britain	Yes - all RUs/IMs	No	Yes
Sweden	Yes - some RUs/IMs	No	Yes
Estonia	Yes - all RUs/IMs	No	Yes
Lithuania	Yes - some RUs/IMs	No	Yes
Romania	Yes - all RUs/IMs	Yes	Yes
Germany	Yes - all RUs/IMs	No	Yes
Denmark	Yes - all RUs/IMs	No	Yes
Spain	Yes - all RUs/IMs	No	Yes
Latvia	Yes - all RUs/IMs	No	Yes
Poland	Yes - all RUs/IMs	No	Yes
Bulgaria	Yes - all RUs/IMs	Yes	Yes
Austria	Yes - all RUs/IMs	No	Yes
Portugal	No	-	Yes
Czech Republic	Yes - all RUs/IMs	No	Yes
Netherlands	Yes	No	Yes
Channel Tunnel	Yes -all RUs/IMs	Yes	Yes
Hungary	Yes - all RUs/IMs	No	Yes
Norway	Yes - some RUs/IMs	No	Yes
Ireland	Yes - some RUs/IMs	Yes	Yes
France	Yes - all RUs/IMs	No	Yes - the annual safety report (produced by the EPSF).
Finland	Yes - some RUs/IMs	No	Yes
Italy	Yes -all RUs/IMs	No	No

For RUs/IMs, all NSA except five (Spain, Poland, Portugal, Hungary, Norway) produce a safety report or rating (or both) for all RUs/IMs (or at least the key ones). France and Italy did not provide a response. It was less common for NSA to rate safety

performance, instead preferring to summarise it in a report (Table B.40). The Polish NSA produces summary data that are presented according to risk themes across its part of the network, rather than for specific RUs/IMs.

With the exception of Norway, each NSA produces a safety report or rating to summarise the performance of its Member State as a whole (Table B.41). Again, safety ratings were far less common (used only by the Netherlands). The Channel Tunnel is unable to produce such a report or rating as has a remit for infrastructure rather than an entire Member State.

Except for Norway, all of the NSA that produce a safety report or rating for their Member State make this information publicly available (Table B.42). Most (excluding Spain, Austria, Finland and the Czech Republic) share this information with stakeholders. A few NSA share this information with other parties.

3.10.3 Effectiveness of the safety regulatory framework

The forthcoming CSM on Supervision expects NSA to be able to use information from supervision and enforcement activity to form an opinion on the effectiveness of the safety regulatory framework as a whole. The question is open to some variation in interpretation as NSA will be subject to both EU and national legislation to varying extents. Table 3.39 summarises the views of NSA regarding effectiveness when responding to the questionnaire.

- Overall, eight NSA (GB, Lithuania, Denmark, Latvia, Bulgaria, Netherlands, the Channel Tunnel, Hungary) reported that the safety regulatory framework was 'very effective'.
- Nine NSA (Sweden, Estonia, Romania, Germany, Spain, Austria, Norway, Ireland and Finland) reported that the safety regulatory framework was 'quite effective'. One of the reasons for this included the inability of the regulatory framework to make timely adjustments in response to issues. Another reason was that supervision activities could take place without problems or hindrance. The Irish NSA stated that the framework's effectiveness has not really been tested as yet.
- Three NSA (Poland, Portugal and Czech Republic) reported that the safety regulatory framework was only 'a little effective'. Poland was clear on the reasons for this: when EU legislation is transposed into national legislation, the translation distorts the meaning and influences the enforcement; some EU legislation contradicts national legislation; RUs/IMs have historic knowledge of the national legislation and have not adapted well to EU additions; and NSA staff lack experience of SMS-based supervision and enforcement. Portugal reported a lack of penalties in its regime alongside a lack of resources to implement the regulatory framework. The Czech Republic also reported resource problems, as well as an NSA that lacked independence.
- France and Italy declined to respond.

Table 3.39: Effectiveness of the safety regulatory framework

NSA	Effectiveness	Comments
Great Britain	Very effective	We consider that the framework encourages RU/IMs to continually review their safety performance.
Sweden	Quite effective	Framework must be changed/revise to follow reality. It not always be done in right time and then you miss some understanding for legislation.
Estonia	Quite effective	
Lithuania	Very effective	Lithuanian legal acts determine the concrete requirements for RUs and RUs are obligated to comply with them.
Romania	Quite effective	Safety rules are still necessary.
Germany	Quite effective	With reference primarily to national regulatory framework.
Denmark	Very effective	On the basis of the annual safety report, we estimate that the safety regulatory framework is very effective.
Spain	Quite effective	
Latvia	Very effective	
Poland	A little effective	Regulatory framework in Poland consists of Polish and European rules. Unfortunately, during transposition process most of the European rules get distorted, which then influences their enforcement. Some of the requirements of EU law are not implemented and the others are in contradiction to national ones that haven't been adjusted to the new requirements. It makes the NSA activity difficult. Additionally, the NSA competences are restricted (we cannot go beyond what's in the detailed legal framework). NSA has also a very limited influence on the development of the legal framework. The role of the NSA in monitoring, developing and enforcing other legal framework (art 16.2.f of the SD) is not properly transposed to our national legal system. The UTK can only take part in general agreements on the drafts of new legislation, but the ministry responsible for transport legislation is not obliged to take into consideration its proposals and opinions. Important problem is also that most of accompanying documents (e.g. guides) are available usually only in one or three language versions. The new requirements (especially the EU ones) are not well known by the market players. In many cases the market players act up to now on the basis of the old national system and therefore have problems with understanding the new requirements. We, as the NSA, are trying to publish all EU acts for railways on our website together with translated guides, but it doesn't help much.

NSA	Effectiveness	Comments
		Generally speaking, it is hard to implement the supervision along with European rules, because of different organisational culture and lack of historical experience in this field both in the NSA and RUs / IMs (systemic approach and management systems).
Bulgaria	Very effective	The safety regulatory framework contributes to improvement of safety performance where this is necessary and is targeted at maintaining at least the same level of safety or its improvement.
Austria	Quite effective	
Portugal	A little effective	There are lack of penalties foreseen in legislation for some infringements and there are not enough people to carry on more inspections and audits
Czech Republic	A little effective	Lack of qualified staff of NSA, ambiguous legislation, lack of independence for NSA.
Netherlands	Very effective	Working with SMSs underlines that there is a lot of responsibility for the RU's and the IM.
Channel Tunnel	Very effective	In the channel tunnel – effective inspections; no deaths during operations.
Hungary	Very effective	
Norway	Quite effective	We are able to perform our supervision activities without any problems/hindrance.
Ireland	Quite effective	Has not really been tested.
France	-	
Finland	Quite effective	
Italy	-	

Table B.43 provides some additional perspectives from NSA on the effectiveness of the regulatory framework. The opinions provide some contrast on how effective it is for RUs and IMs to operate in accordance with an SMS. Specifically:

- The German and Danish NSA both recognised that there was not a universally high level of understanding in the market with regard to operating with an SMS.
- It was recognised that frontline inspections provide an essential level of information regarding the effectiveness of SMSs; occasionally there may be a substantial contrast between how effective an SMS appears on paper and how it is operated in reality. For example, the Swedish NSA noted that the SMS for some RUs/IMs was a rather superficial structure that did not evolve as intended after the award of a certificate or authorisation.

- NSA have a part to play in improving the effectiveness of the safety regulatory framework by guiding the market. In the experience of the Dutch NSA, working with SMSs has provided a platform for generating notable improvement in safety culture – markedly more so than might be expected if the market was simply given a set of rules to follow rigidly.

Table 3.40 shows that these findings on the effectiveness of the safety regulatory framework are typically shared with RUs/IMs, stakeholders and the Agency. Six NSA (Germany, Austria, Portugal, France, Italy and Czech Republic) either did not share this information or did not specify.

Table 3.40: Disseminating NSA views on regulatory effectiveness

NSA	Individual RUs/IMs?	Stakeholders?	ERA?	Other?	If other, please specify
Great Britain	Yes	Yes	No	No	
Sweden	No	Yes	Yes	-	
Estonia	Yes	Yes	Yes	No	
Lithuania	Yes	Yes	Yes	-	
Romania	Yes	Yes	Yes	Yes	Romanian Railway Investigation Body, Romanian Railway Notified Body, Romanian Railway Licensing Body.
Germany	-	-	-	-	
Denmark	Yes	Yes	Yes	-	In the annual safety report.
Spain	Yes	Yes	Yes	-	
Latvia	No	Yes	No	Yes	Ministry of Transport.
Poland	No	No	Yes	Yes	See the answer above. In Poland NSA does not have any special role in assessing the effectiveness of safety regulatory framework (the art 16.2 f of SD has been transposed but UTK doesn't have proper role in this field in national system and doesn't have tools to act). There is a strict distinction - ministry of transport is responsible for preparing the legal regulations and NSA is responsible for enforcing them. We often inform the Ministry about the deficiencies of national legal system, but the Ministry is not eager to correct it. Usually only small corrections are implemented but the whole approach is

NSA	Individual RUs/IMs?	Stakeholders?	ERA?	Other?	If other, please specify
					not changed. Besides this the process takes a very long time.
Bulgaria	Yes	Yes	Yes	No	
Austria	-	-	-	-	
Portugal	No	No	No	No	
Czech Republic	No	No	No	No	
Netherlands	Yes	Yes	Yes	No	
Channel Tunnel	Yes	Yes	Yes		ERA receives IGC's annual report but not individual inspection reports.
Hungary	Yes	No	Yes	No	
Norway	Yes	Yes	Yes		
Ireland	Yes	Yes	Yes	No	Annual statistical review available on website.
France	-	-	-	-	
Finland	Yes	No	No	No	
Italy	-	-	-	-	

3.10.4 Evaluation and continuous improvement

It is desirable for authorities to consider ways to continuously improve how they supervise and enforce. This culture of improvement is a basic good practice requirement for NSA. Table B.44 provides examples of authorities that have evaluated their activities and ways in which they have identified how to improve. There appear to be two key stages in the evaluation or performance. The first is to introduce a basic review process:

- A basic review process appears to be a fundamental part of NSA activity. Regular staff discussions and case reviews (e.g. the Bulgarian NSA) are a desirable minimum objective for NSA.
- NSA reviews can be somewhat reactive. For example, the Austrian NSA reviews it enforcement decisions at least yearly to determine whether there have been any changes, whether sufficient technical consultation has occurred and whether enforcement action is proportionate or could be strengthened or softened. It could be argued that such decisions regarding the proportionality and technical quality of individual cases should be reviewed before a decision is issued rather than up to a year after. A move towards a more proactive review process is desirable for such case-specific goals whereas the goals for evaluating NSA performance and delivering continuous improvement should perhaps be focused

more on the broader objectives of delivering a safer and more accessible rail market.

- Reviews of activity (be it random peer reviews of cases or structured annual reviews) should be targeted, with measurable outcome criteria, and ideally be part of the NSA's strategy. What those criteria should be is something NSA must consider – examples include the number of inspections achieved, the number of audit days delivered or more qualitative measures such as the extent to which inspectors have explored underlying SMS faults.

Once a basic review process is in place, the next stage described by NSA is to survey the effectiveness of the NSA as perceived by the market:

- Surveys of those who were subject to supervision and enforcement (e.g. the Austrian OSH), detailed qualitative interview surveys of stakeholders (by the GB NSA) and more general survey activity to gauge RU/IM satisfaction is one approach to understanding how well an NSA is supervising the market.
- An example of how surveys can be effective was provided by the GB NSA. The findings from its survey provided considerable insight into how its supervision and enforcement activities were perceived by the market. It raised several points of concern, such as bias towards particular RUs/IMs and regions, and an approach to stakeholder engagement that appeared dismissive and routine. By ensuring that the survey had question items related to the principles of supervision, it was possible for the NSA to identify where its supervision and enforcement performance was weak, and where its strengths lay. An example of this was communication with stakeholders, which was reported to be document-heavy and rather inaccessible, with the whole process requiring better targeted communication with more direct contact; the subsequent introduction of 'account holders' was encouraged by this survey. Informal feedback from the market is also valuable.
- When surveying the market or conducting other review processes, it is good practice to publish findings so that the market can see collectively how it has responded. It is also good practice to respond to the issues so that the market can see how they will be addressed (where appropriate) and that the NSA has a specific commitment to change.

Some NSA have taken further good practice measures to evaluate their performance, including:

- Changing procedures that are poorly targeted and unnecessarily burdensome for RUs/IMs. For example, the Danish OSH authority changed the circumstances under which it issued 'consultancy notices' (which were a detailed follow-up to repeat offences) because its initial policy was placing unnecessary burden on some dutyholders that were not going to benefit from the process.
- Monitoring the number of positive and negative media reports related to an NSA's activities and the number of website hits for its online guidance and toolkits. These are both items that the GB OSH uses to monitor its performance.

- Monitor the quality and focus of evidence used to form cases. The GB NSA regularly reviews the content of its case reports and has noted inspectors are increasing their focus on the underlying SMS failures that may lead to problems at an RU/IM. This is considered a performance improvement: it is a better fit with the European approach, it assists the RU/IM with understanding its problems and it ensures the NSA is more accountable for its decisions.
- Link performance evaluation with strategic goals. The Danish NSA describes in its strategy a highly structured approach to self-evaluation that supports both short- and long-term outcome measures specified in its strategy, with a clear link between the two. It is desirable for an NSA to demonstrate a direct link between its activities and broader goals for improving railway safety and market access that will be shared by RUs and IMs. The activity of an NSA may appear more legitimate as a result and such goals may develop a greater sense of the NSA working together with the market.

3.10.5 Summary

In terms of performance, NSA were divided almost equally between those that felt their supervision performance had improved and those that felt it had remained at the same level.

Almost without exception, NSA are using the outcomes of supervision plans to generate an overview of the safety performance of RUs and IMs, and the Member State as a whole. This is most commonly summarised as a report.

Except for France and Italy, all NSA were able to use safety performance data and supervision experience to estimate the effectiveness of the safety regulatory framework. The majority of NSA reported that it was at least quite effective; those NSA that felt the framework was less than effective reported complications arising from transposition of European directives along with incompatible or restrictive national frameworks. The effectiveness of the framework was suggested to benefit from the introduction of the SMS-based approach which encouraged the market to manage its own safety rather than simply respond to a fixed set of rules. However, NSA recognised that they had a role in guiding the market towards adopting this approach, and ensuring that it was followed in practice as well as on paper.

For NSA to be able to rate any change in their own performance, it would be necessary for them to have in place a procedure for self-evaluation and continuous improvement. Most NSA demonstrated that they had a basic culture of improvement. To evaluate how they were performing, several NSA would review their supervision and enforcement activities against common goals, such as delivering a minimum number of audit days. Some went further and surveyed the market to seek feedback. A further development of these measures was to use such evidence to monitor progress with strategic goals.

For NSA that wish to achieve a baseline level of good practice, it is recommended that they:

- Develop a culture of self-evaluation and improvement. This is particularly important for NSA that do not recognise the regulatory requirement for continuous improvement.
- Establish basic review procedures. Supervision and enforcement activities should be reviewed with a set of common criteria in mind – this stage of review should be about evaluating how the NSA is performing as a whole and should not be seen as a replacement for the due diligence that is expected when reviewing individual cases.

NSA that wish to adopt good practice above the baseline level are advised to:

- Survey all levels of the marketplace using a variety of survey methods. It is important for NSA to understand market satisfaction, both in general and after supervision/enforcement has taken place. Surveys can inform the future policies and procedures of an NSA. Survey findings should be published along with a response to core issues from the NSA, with appropriate commitments to action.

NSA that wish to develop their good practice further may wish to:

- Link evaluation data to strategic goals to present a coherent development cycle.
- Respond to market feedback on procedures by changing them if they are overly burdensome and ineffective. NSA may win or lose market support according to how responsive they are to valid market concerns.
- Monitor how NSA activity is presented in the media.
- Monitor usage of NSA guidance and tools that are provided online (e.g. number of 'hits').

Key findings:

- Almost equal numbers of NSA reported improved supervision performance as reported no change.
- Almost all NSA use supervision outcomes to generate an overview of the safety performance of RUs, IMs and the Member State.
- The majority of NSA summarise as a report the safety performance of RUs, IMs and the Member State as a whole.
- The majority of NSA consider the safety regulatory framework to be effective.
- Most NSA are aware of the need to self-evaluate and have review procedures in place.
- Some NSA survey the market to obtain performance feedback.

Good practice recommendations:

- Establish basic review procedures.
- Survey the market and publish the findings together with an NSA response to specific issues.
- Demonstrate a link between evaluation processes and core strategic goals.

3.11 Market regulatory awareness

NSA reported on general levels of awareness of the safety regulatory framework among the RUs and IMs that they supervised. Of the 20 NSA responding:

- Eight NSA (GB, Lithuania, Romania, Denmark, Channel Tunnel, Hungary, Norway, and Ireland) supervised a part of the market that was either 'very' or 'extremely aware' of the relevant safety regulatory framework, in the opinion of the supervising NSA. Collectively, these NSA all actively promote the safety regulatory framework using a combination of websites, letters, meetings, workshops, conferences, leaflets and reports.
- Ten NSA (Sweden, Estonia, Germany, Spain, Latvia, Bulgaria, Austria, Czech Republic, Netherlands and Finland) supervised parts of the rail market that were 'quite aware' of the safety regulatory framework. These NSA used similar methods of promotion to the NSA listed above.
- Three NSA (Portugal, Poland and Italy) supervised parts of the rail market that the NSA believed were only 'slightly aware' of the safety regulatory framework. The Polish NSA explained that some of the reasons for this lower level of regulatory awareness were due to Article 16.2(f) of Directive 2004/49/EC being improperly transposed to Polish law. The transposition allegedly contains errors and "isn't linked with any tools that the NSA can use [for promotion]. In addition, the Polish NSA cannot initiate any changes to its national legislation, which is forecast to become more problematic once the CSM on Supervision enters into force, because it will increase the NSA's responsibilities under EU legislation but this role will not be supported by national legislation. Nevertheless, the Polish NSA has sought to promote the EU legislation via its website and via meetings. Portugal's NSA did not clarify the reasons for low levels of awareness in its part of the rail market although it did state that seminars, working groups and meetings were used to promote the regulatory framework.

Table 3.41: Market size and regulatory awareness

NSA	Awareness of safety reg framework?	Promotion methods
Great Britain	Very aware	Website, letters, in person, workshops.
Sweden	Quite aware	Promote on Website/ Workshops/ Conferences/ Meetings/ and on Audits
Estonia	Quite aware	Workshops and group e-mails/letters
Lithuania	Very aware	Our NSA publishes information about safety regulatory framework on our website.
Romania	Very aware	website www.afer.ro Official Journal of Romanian Railway Authority
Germany	Quite aware	Publish list of NSR

NSA	Awareness of safety reg framework?	Promotion methods
		- Publish relevant legislation - Publish guidance on safety certification / authorisation - Discuss with RU / IM - Workshops / information sessions on new legislation
Denmark	Very aware	Website, conferences, leaflets, etc.
Spain	Quite aware	By means of dissemination workshops.
Latvia	Quite aware	Consultations, workshops, directions
Poland	Slightly aware	It's a weak part of the NSA activity. As it has been stated in previous answers, the art. 16.2.f has not been properly transposed to Polish law. The Polish rule in this field contains some mistakes and isn't linked with any tools that the NSA can use. Besides this the general Polish legal framework doesn't give any special role for the NSA in the field of promotion and development of legal framework. The NSA doesn't have any special right to initiate necessary changes to the legislation. It will be a real problem for us especially after entry into force the CSM on supervision, as we probably won't get any additional tools in this field. Regardless of weak competences in the field of art 16.2.f we are trying to promote especially the EU legal framework, by publishing the requirements on the website (both the laws and the guides), disseminating the knowledge during different meetings and organizing meetings with ERA representatives.
Bulgaria	Quite aware	Website of RAEA i.e. the NSA of Bulgaria. Workshops with the RUs/IMs and other stakeholders, dedicated to the functions of the NSA. Letters to the RUs and IMs.
Austria	Quite aware	E.g. published guidance, meetings, letters, information on the NSA website.
Portugal	Slightly aware	By seminars, workings groups and meetings.
Czech Republic	Quite aware	By certification process.
Netherlands	Quite aware	Pre risc meetings.
Channel Tunnel	Extremely aware	Regular meetings, discussing all aspects of regulatory framework.

NSA	Awareness of safety reg framework?	Promotion methods
Hungary	Very aware	On the website.
Norway	Very aware	Regularly arranging meetings.
Ireland	Very aware	Through its supervision activity. Production of annual statistical report.
France	-	A set of application guidelines and procedures are available on the website of the EPSF. Meetings REX (feedback) are organized. This is to identify and share to all operators with common problems: to monitoring of events involving safety on the network; to the holding of a database of these events; to the publication of a monthly newsletter describing the main incidents of the past month; to the organization of quarterly meetings for exchange and discussion of audit findings and lessons from incidents. Finally, meetings and dissemination of the regulation of European work is organized (topic general, specific (MSC), ...) several times a year with all stakeholders.
Finland	Quite aware	By regular meetings, ad hoc meetings, seminars, guidance, webpages and direct communication.
Italy	Slightly aware	

4 Summary and discussion

This study presents a comprehensive review of how NSA supervise and enforce the European railway market. The coming into force of the Common Safety Method on Conformity Assessment (Regulations 1158/2010 and 1169/2010) generated the impetus for this study; these Regulations introduced principles to govern how NSA supervise and enforce the market. These principles have established within the European safety regulatory framework a set of requirements that will be a growing focus in the quest for harmonisation. With the opening up of the European rail market, such principles have an important part to play in developing trust and consistency between NSA for cross-border operations. A Common Safety Method on Supervision is forthcoming (recent drafts were a frame of reference for this study) and the European regulatory framework has ambitions to move towards a single safety certificate by 2020 to replace the current two-part system. From these regulatory developments comes a pressing need to understand the pace of compliance across the market currently so that ERA may plan its future guidance and activity with regard to supervision and enforcement practices. This activity will be assisted by establishing a baseline level of good practice that the Agency may wish to recommend to NSA, along with higher levels of good practice for the further development of NSA that may already be meeting or exceeding the baseline.

Throughout this report, the activities related to supervision and enforcement by NSA have been explored and discussed according to the core activities and attributes of NSA that are related to supervision. These activities and attributes are to:

1. Structure and organise the NSA and its general policies/procedures
2. Develop staff competences for the activities of supervision and enforcement
3. Plan supervision activities
4. Deliver supervision activities
5. Make and deliver enforcement decisions
6. Evaluate and continuously improve NSA performance

Each of these NSA activities and attributes has a series of good practice recommendations associated with it. These are summarised and discussed in the following subsections.

4.1 NSA structure and organisation

How NSA structure their organisations for the purposes of supervision and enforcement has shown itself to be critical to how effectively these functions are delivered. Staffing divisions are one of the structural factors that can have an influence. This study has shown that for assessment and supervision tasks, the majority of NSA have a partial division of staff, with a small number having a full division or no division at all. Other divisions were reported according to whether an NSA is supervising an RU or an IM.

Accepting that all NSA are free to adopt different staffing structures (and may be forced to do so, given that half of the surveyed NSA had fewer than 10 staff for supervision and enforcement), this report recommends a number of ways in which NSA can manage

different staffing structures to ensure that supervision and enforcement is not unduly affected. Recommendations for good practice focus on:

- Good internal communication between assessment and supervision teams, facilitated where possible by systems for information storage and exchange.
- An independent and/or peer review process for assessment/supervision decisions.
- A consistent knowledge base amongst staff.
- A consistent and universal decision-making process.

A further route to delivering effective assessment and supervision is to ensure that each NSA has a strategy to guide it. Strategic direction, particularly for supervision, may help to override the potential bias that can emerge from particular staffing structures (e.g. when NSA staff become 'too close' to an RU/IM through repated regulatory contact). Recommendations for an effective strategy focus on:

- A long-term strategy, that is at least published online, and outlines clear strategic goals and a plan for achieving them.
- A wide range of data inputs to the strategy that combine data-led approaches ('top-down') with information from NSA staff and even market participants ('bottom-up').
- Reflecting the European safety regulatory framework.

Once a strategy is developed, its dissemination and delivery (beyond simply making it available online) can affect the influence it has. This study provided examples of authorities using innovative media and events to encourage the market to engage with the strategy so that its success becomes a joint commitment. To facilitate the implementation and delivery of a strategy, some authorities even assign working groups and committees to take responsibility for delivering part or all of the strategy.

However, when strategic decisions regarding the resources, policy and remit of an NSA are made by government departments that are somewhat separate from the daily activities of the NSA, this can bring further challenges. It is therefore desirable if NSA:

- Cooperate with other government safety authorities to provide a consistent level of market supervision and enforcement. This is particularly valid for NSA that do not have a remit to enforce on labour issues directly related to railway operations.
- Appoint a single committee to represent all levels and supervision activities of the NSA.

The difficulties that can arise when an NSA is not able to cooperate seamlessly with other government departments are best represented by examples of poor transposition of the European safety regulatory framework. Such difficulties had led to NSA being unable to supervise and enforce fundamental elements of the European framework, such as the requirement for RUs and IMs to operate with a compliant SMS. Further regulatory conflict was reported when the requirements of European legislation were found to be

incompatible with the requirements of national legislation: in the best case, these legal conflicts had been noted but not yet tested by the market; in the worst case these legal conflicts had led to substantial market confusion.

There are further ways in which an NSA can structure itself to deliver supervision and enforcement that meets the requirements of the regulatory framework. A policy and procedure to enable an RU or IM to complain effectively is one such requirement and the majority of NSA have this in place. Recommended good practice for a complaints policy and procedure is to:

- Ensure the market is aware of it. Publishing online is a minimum recommendation and this can be supplemented by providing the same information during any supervision or enforcement activities.
- Facilitate access to the complaints procedure with online forms and accessible contact information.
- Implement a clear process for escalating complaints if they cannot be resolved initially.

Another way in which supervision and enforcement can be structured to meet the legislative requirements is to have cooperation agreements with other NSA. Just over half of the NSA surveyed had such agreements in place but they were largely informal and used primarily to exchange a fairly restricted range of information. It would seem that what NSA most want to discuss is the assessment and supervision of foreign RUs operating under a Part B safety certificate. A few NSA reported that they had started to broach this issue with cooperation agreements that included open, proactive exchange of information regarding RUs that were operating across borders, and joint auditing and supervision activities for such RUs. Recommended good practice for cooperation agreements between NSA is to:

- Assign a point of contact for cooperation. One of the reported barriers to cooperation was when an NSA did not know how to make initial contact with another NSA, particularly if there had been no previous communication between them. Assigning an email or telephone number for cooperation enquiries would facilitate the process.
- Be ready to exchange information openly and proactively about RUs operating across borders. Some NSA have already initiated cooperation along the 'axes of need' (i.e. key cross border routes) although it may be helpful to review whether all such routes are subject to cooperation between relevant NSA before then promoting wider cooperation across the NSA network.
- Work with other NSA to arrange joint supervision and enforcement procedures.

There was some evidence to suggest that two matters may require further European guidance. The first was the timing of reassessments for Part A and Part B safety certificates. Given that these certificates are interdependent but may be issued by more than one Member State, there is a concern that timing the process of reassessment to fall within the periodicity of a certificate may require careful cooperation between NSA to ensure that there is resource to deliver reassessments without service interruptions. The

second issue was that of language differences when attempting to supervise and enforce RUs that operate across borders.

Finally, it is recommended that cooperation does not stop at other NSA. Each NSA is recommended to cooperate with other competent authorities within its own government, and in other countries where there may be a shared interest. Cross-governmental cooperation has the benefit of providing a consistent approach to supervision and enforcement, which is particularly valuable given that railways operations may be subject to enforcement by other bodies (e.g. labour inspectorates) or that an NSA may wish to coordinate its response to an incident with such authorities. It is also recommended that cooperation include a broad range of stakeholders. There were examples of competent authorities in other sectors participating in regular stakeholder conferences, some of which were even established by law.

4.2 Competency for supervision and enforcement

The forthcoming Common Safety Method on Supervision is expected to require NSA to have systems in place that will ensure supervision activities are undertaken only by competent persons. The majority of NSA already have some formal system in place to train new staff for supervision and enforcement activities. There was a tendency for staff to be trained on-the-job rather than through formal courses; this was particularly true when staff received training on the safety regulatory framework. However, even though the majority of NSA were engaged with competence development there was scope for continued improvement in this area.

Several measures were identified as good practice for competence development. In summary, competence development should:

- Focus on training essential skills first, such as auditing techniques. Senior staff can shadow new staff until they meet a desired level of competence.
- Be a strategic goal and training should be targeted to help staff deliver the current strategy. Efficient staff training can be delivered using in-house expertise, market expertise and by consolidating provisions across similar government safety authorities.
- Be monitored to ensure continuous improvement. Internal online systems may facilitate this process.

4.3 Planning supervision

The majority of NSA have at least a general strategy for supervision and, by their own reckoning, are very targeted. Some NSA provided insight into how they set targets for supervision. One of the approaches described was to target areas of railway operation that would help to avoid catastrophe. However, the amount of resource invested into supervision could depend on the NSA's assessment of how well the railway already manages risk in those target areas. For example, a track or rolling stock failure may lead to the greatest type of catastrophe but the market may be managing those risks well, in which case greater resources may be directed at supervision of level crossings, where the risks are not managed as well. Understanding these issues is an essential part of planning supervision and a key reason for having a strategy.

Planning and allocating resources to supervision provide further justification for a supervision strategy. It was reported that most NSA allocated less than half of their available staff and budget to supervision, and three of the four NSA that allocated the least did not have a strategy for supervision. NSA that did have strategies reported that these were a useful tool for discussing with government budget holders what resources were necessary to deliver the required level of supervision and enforcement.

Moving on from general strategies, about two-thirds of NSA reported that they had specific supervision plans for specific RUs and IMs, which meets the requirements of the current and forthcoming safety regulatory framework. NSA reported that a range of methods were used to develop supervision plans, some of which were more appropriate than others. In conjunction with the Taskforce on Assessment and Supervision, it was agreed that the ideal approach to planning supervision was primarily driven by an assessment of RU/IM capability and relative risk, with secondary inputs from an assessment of incidents and/or their precursors. It was agreed that supervision should not be planned by simply distributing resources equally.

4.4 Delivering supervision

4.4.1 Methods and decision-making

Most NSA use a range of supervision methods regularly (interviews with all levels of staff, document reviews, examining SMS outcomes), many of which were also deployed when checking the SMS of an RU or IM. On the evidence provided, a good practice approach would be to use a combination of: audit techniques; interviews with staff at all levels in an RU/IM; investigative techniques (e.g. examination of documented SMS outcomes); and, inspections (e.g. to observe first-hand the operational performance of the RU/IM). Of the overall time allocated to inspections, NSA typically direct 50-90% towards proactive inspections (which is a desirable range), with the rest of the time being used for reactive inspections. It is recommended that NSA aim for 80% of inspections to be proactive (and certainly no less than 50%).

NSA must routinely decide whether enforcement action against a particular RU/IM is required as a result of supervision findings. Approximately three-quarters of NSA have developed and published decision-making criteria to guide this process. One such process was singled out as a clear example of a consistent and structured approach to decision-making. It directed users to calculate the 'compliance gap' (i.e. the extent to which the risks presented by a specific case deviate from the accepted benchmark level of risk for that activity) created by the non-compliance or safety hazard, then decide on an initial level of enforcement before considering whether any factors related to the RU/IM or the NSA strategy would affect the subsequent level of enforcement. Although other NSA had adopted similar processes in part, none reported bringing together these principles in a form that was as accessible and structured.

In collaboration with the NSA Taskforce on Assessment and Supervision it was agreed that a prescriptive decision-making model would be not be appropriate for the sector at present (although it could be a future goal for the European network to develop one). However, a common approach to decision-making was desirable and the Taskforce agreed that the commonality should focus on making decisions according to a 'compliance gap' model. Further agreement was reached with the Taskforce on recommending that each NSA documents and publishes its decision-making process.

NSA that wish to demonstrate further good practice are advised to:

- Work with the market to develop effective supervision. By surveying the market and engaging with RUs/IMs, NSA can develop a better understanding of what supervision techniques work best for all parties and, importantly, what methods enable RUs and IMs to learn from the experience.
- Develop internal structures and practices to facilitate supervision and decision-making. These could include electronic document management systems, internal communication to connect inspectors with senior staff when advice is needed, and team structures that empower individuals to make decisions with appropriate technical and legal support.

4.4.2 Transparency and communication

Current and forthcoming European legislation is specific about the need for NSA to communicate with the market in a way that makes each NSA's expectations transparent and also specifies what the market can expect of each NSA in return. The majority of NSA reported that they were very transparent and yet the findings indicated that there was an overdependence on NSA websites as a means of communication with the market, perhaps reflecting that NSA held unrealistic expectations of how much transparency they could deliver through websites alone. Whilst it is baseline good practice to publish online key NSA documents, processes, policies and procedures, some NSA did not necessarily utilise this resource as effectively as others. NSA could better exploit their websites by including tools to assist RUs/IMs (e.g. checklists for audits), innovative cataloguing and search mechanisms, information and guidance on key industry issues, news and current industry information and foreign language support.

To develop their communication further, it is recommended that NSA find additional ways to communicate with the market. For example, NSA can meet regularly with RUs and IMs outside of formal supervision activity, they can assign specific staff to specific RUs/IMs as a primary liaison, and they can host and participate in conferences with stakeholders. All of these activities raise the profile of an NSA across the market and provide interaction between NSA and RUs/IMs that is not constrained by the formalities of supervisory contact.

However, it is recognised that engaging in wider communication may be resource-intensive and for some NSA it might not be feasible to follow good practice in this area without sacrificing resource in a different area. Communication should therefore be planned as part of the NSA's strategy (or even have a strategy of its own). A strategy should identify which stakeholders should be targeted, what communication they should receive and how/when it will be issued. NSA can then plan to communicate on the most important issues for their market and ensure these messages reach the correct segments of the market with the resources they have available.

4.5 Delivering enforcement

When it comes to enforcing a decision, NSA vary considerably in the measures they have at their disposal. The majority have the power to issue formal enforcement notices to RUs/IMs that require them to rectify an issue, often by a deadline. Some NSA can take a softer approach where appropriate and issue such requirements as guidance, whilst other NSA can take a firmer approach where appropriate and issue financial penalties,

suspend or revoke the use of equipment or even a safety certificate/authorisation, and even prosecute via the courts.

Such decisions regarding the severity of the enforcement action should be guided by the decision-making process used during supervision. However, a sufficient range of enforcement measures should be readily available to NSA so that proportionate action can be taken. Some NSA did report a poor range of enforcement measures and/or inflexible and overwrought administrative procedures that dissuaded the use of some measures. A baseline requirement for good practice is that such circumstances should not exist. NSA that are faced with such difficulties are recommended to form an internal working group with relevant government departments to address concerns with available enforcement measures. The goal should be for all enforcement measures to be accessible subject to a clear and published procedure that would ideally draw evidence from a standardised supervision report form.

When delivering an enforcement decision, it is recommended that the decision is communicated to the executive board of the RU/IM (so that the organisation implements company-wide solutions). It is also desirable to ensure that there is dialogue between the NSA and the RU/IM when an enforcement decision is issued in case further mitigating evidence needs to be considered.

4.6 NSA self-evaluation and continuous improvement

It is desirable that NSA have a cycle of continuous improvement. Supervision and enforcement activities should be subject to a basic review process that centres on staff discussion and case reviews. Such activity should be guided by strategic goals (e.g. achieving a specific number of audit days) and the review process would ideally contribute towards fulfilling an NSA's core objectives. For NSA that wish to demonstrate further good practice, it is recommended that they survey the market to establish how it perceives the effectiveness of NSA supervision and enforcement. Surveys can provide insight into where an NSA is underperforming with regard to supervision and where it may be best-placed to target future supervision. By publishing survey findings together with a formal response, the NSA can be transparent with the market.

About half of the NSA surveyed did not report any improvement in supervision performance during the 12 months prior to the survey which would suggest a need for evaluation in order to deliver continuous improvement.

4.7 Conclusions and recommendations

This study has provided a snapshot of NSA supervision and enforcement activity during the transition to the new European safety regulatory framework. It marks a point in NSA development where supervision should be in accordance with the SMS-based approach but will be subject to further regulation as the framework expands.

This review indicates that NSA have collectively reached a reasonable level of maturity with regard to adopting supervision and enforcement practices required by the European safety regulatory framework. However, across the network of NSA there are clear differences in the extent to which the regulations are being implemented and this study brings some of these differences together so that NSA can learn from each other and work towards greater consistency in the future.

This study provides baseline recommendations for good practice to be delivered in each of an NSA's core activities related to supervision. Further recommendations are made to encourage NSA to reach progressively higher levels of good practice. A full list of the recommendations is provided in Appendix C. The recommendations are issued to the European Railway Agency with the intention that they will be adopted, either as direct recommendations to the NSA Network or as the foundations for further work at a European level.

Appendix A Case study examples

The eight case study examples were provided by the GB NSA. They are genuine cases and the enforcement action taken by the GB NSA in each example is indicated. In the questionnaire, the following response options were possible:

- Prosecute in court
- Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)
- Take formal enforcement action (other methods to address a non-compliance)
- Issue a fixed fine
- Issue other financial penalties
- Issue written advice
- Issue verbal advice
- Other (please specify)

Example (5) – missing/damaged fence next to nature reserve

ENFORCEMENT ACTION TAKEN: PROSECUTION

A member of the public complained that there was no fence to separate a nature reserve from a railway line. The NSA discussed the problem with the Infrastructure Manager (IM) and was assured that fencing had been repaired. However, the site was visited 2 months later by the same member of the public who reported that the fence had not been repaired. The NSA visited the site and confirmed that long sections of the fence were missing or needed repair. There was evidence of trespass onto the railway.

The investigation showed that:

- The IM had identified damaged or missing fence at the location three years ago and during recent inspections.
- The IM had received complaints about the fence a year ago.
- The IM knew people had trespassed onto the railway at this location.
- The IM had not carried out any repair work at the site.

The NSA concluded that:

- The IM was responsible for preventing unauthorised access to the railway.
- The IM's maintenance regime had failed over a lengthy period of time.
- This was a very high-risk location to which the public had access (100,000 people/year).

Example (2) – loose barrier between carriages

ENFORCEMENT ACTION TAKEN: PROSECUTION

A loose barrier fixed between two carriages to prevent falls struck three passengers as the train departed a platform. Two of the passengers sustained head injuries and the third was struck on the upper arm.

Earlier in the train's journey the barrier had been reported by staff as being loose but had not been removed. After the incident the train was allowed to continue on its journey until the barrier was removed further down the line.

A second barrier was reported as loose on a subsequent date.

The NSA investigation showed that:

- The barrier which struck the passengers was either loose before entering service or became loose during service.
- The cause was either maintenance failure or the failure of the barrier attachments.
- The train remained in service and was not held at an earlier platform so that the barrier could be removed even though the issue had been identified by operating staff.
- A train technician was not called to remove the barrier at the earlier station.
- There was a communication failure between station staff and service control staff that allowed the problem to continue despite the potential risk to passengers.
- The operator had previously identified risks associated with barriers becoming loose, and has specific instructions on the issue.
- There are records and statements from the operator that this was a common occurrence.

The NSA concluded that:

- The incident and injuries to passengers could have been predicted and prevented.
- Although the risk was well known to the train operator, it failed to deliver the required standard of control.
- The train operator failed in its duty to prevent further incidents by stopping the train and removing the barrier.

Example (4) – poorly maintained Road Rail Vehicle (RRV)

ENFORCEMENT ACTION TAKEN: ENFORCEMENT NOTICES

A visual Inspection of Road Rail Vehicles (RRV) prior to deployment focused on the condition and profile of tyres of the road wheels that engage with the rail wheels to provide traction and braking.

Two of the three RRVs inspected had at least two tyres in poor condition (worn down and damaged). The contact of these tyres with the rails was observed to be reduced, resulting in poor traction and, once movement was underway, braking performance was very poor.

The NSA investigation showed that braking performance of these RRVS whilst in rail mode presented a risk of the vehicles not being able to stop and running out of control.

The NSA concluded that there was a risk of serious personal injury to both the RRV operator and other persons in the vicinity.

Example (8) – excessive working hours

ENFORCEMENT ACTION TAKEN: ENFORCEMENT NOTICES

An inspection of Site Access Registers provided by a Railway Undertaking's (RU) safety department identified numerous instances where combined travel time and shift length

for individual workers far exceeded the RU's company standard of 12 hours, as well as the 14 hour door-to-door guidance contractually agreed with the employing Infrastructure Manager. Examples of combined travel and shift length of up to 20 hours were logged. These had not been addressed by the RU's Site Access Controller or other fatigue management procedures in place at that time.

The NSA investigation showed that the RU had failed to monitor and manage excessive working and travelling hours.

The NSA concluded that the RU had not followed legislation that requires systems to ensure that risks to the health and safety of employees or others who may be affected are controlled, so far as is reasonably practicable.

Example (1) – loose panel on a vehicle

ENFORCEMENT ACTION TAKEN: WRITTEN ADVICE

Routine maintenance on a limited availability vehicle required the removal and replacement of a covering panel. The next morning, this panel was found in a car park next to the track. The panel was sheet metal and approximately 4m by 0.3m in size, giving considerable potential for harm. There were no injuries to people or damage to property.

Removal and replacement of the panel is a simple, routine task that is carried out regularly. The panel is secured by three fasteners, one of which would be adequate to retain the panel if properly applied.

After the event the operator was made aware that identical vehicles elsewhere had been fitted with restraining straps following similar incidents. The operator subsequently took action to replace the fittings used.

The NSA investigation showed that the operator had:

- A good health and safety record and operated a safety management system that required all staff to receive relevant training and assessment. Training and competence was demonstrated through company records.
- Clear procedures for securing the panel.
- A system of competence management for staff with relevant records kept.
- Acted quickly to modify the panel fasteners so the issue would not occur again.

The NSA concluded that:

- The operator had a good record in health and safety matters.
- The task was simple and well defined so it was not considered foreseeable that such a straightforward task would be carried out incorrectly.
- The vehicle was of limited availability so the outcome of the investigation would be of little benefit to other duty holders.

Example (7) – working at height

ENFORCEMENT ACTION TAKEN: WRITTEN ADVICE

Work at height was being carried out on a station platform by a sub-contractor. There was no edge protection and the sub-contractor was relying on an inadequate and poorly designed system to prevent workers from falling.

The NSA investigation showed that:

- The safety system used by the sub-contractor had not been set-up with the approval of the Principle Contractor or the client.
- The Principle Contractor and the client both took action to stop all work at the site when the NSA inspector notified them of the risk. No further work was carried out until the sub-contractor's procedures had been reviewed. This action was later confirmed in writing.

The NSA concluded that:

- The Principle Contractor had failed to manage and risk assess the activities of its sub-contractors and had failed to carry out appropriate local site management.
- The Principle Contractor and client had both responded in a way that was appropriate and demonstrated they took the issue seriously.

Example (3) – unsafe access to station roof

ENFORCEMENT ACTION TAKEN: VERBAL ADVICE

During inspection of construction works at a station, the duty holder's project coordinator, expressed concern about the system used by workers to access part of the station roof.

The system was checked by an NSA Inspector who was also very concerned about the condition of the walk boards and the 'safe man' system in place. It was agreed through discussion that no one would access the roof without a safe system of work being agreed. It was agreed that the Station Manager would hold the key to the roof to prevent unauthorised access. The roof was due for maintenance so it was agreed that nobody would access the roof until the works had been completed and a new safe system of work was introduced.

Example (6) – missing/damaged fence near platform

ENFORCEMENT ACTION TAKEN: VERBAL ADVICE

During inspection of a railway platform, an NSA Inspector identified that a large section of fence was missing along a well established trespass route, which would allow unauthorised access to the railway. The Inspector informed the Infrastructure Manager (IM). The IM confirmed to the Inspector that a replacement fence would be completed by the end of the day.

Further NSA investigation showed that:

- The same fence had been reported damaged and repaired two months earlier, along with a request to upgrade.
- The same fence had been inspected 5 days before the latest damage was reported so it was assumed that that the latest damage had occurred after this inspection.

The NSA concluded that the IM's attitude and cooperation was sufficient to address the problem. There was no evidence that this was a systemic problem at this location.

Appendix B Tables

Table B.1: NSA staffing structures for assessment and supervision – interview findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	DK	"One very important point I think is actually the same team that is making the safety certification and the safety authorisation is doing the supervision. So we know the safety management system of the companies from the very beginning and we know the weaknesses and strengths of the system so they will actually not be able to guide us in the wrong direction on purpose or not because we have this continuous line from certification, authorisation to supervision. That's actually not the way it is in all countries that I'm aware of. We have a certifying committee so when a lead auditor finishes an assessment for certification or authorisation he gathers the needed documentation and forwards it to the certification committee." The NSA strategy describes the certification committee as follows: "The certification committee is appointed for the occasion and consists of the head of supervision and authorisation and at least one supervisory member of staff who did not participate in the supervisory team in connection with the corresponding certification inspection. The certification committee thus ensures quality and independence in the case handling and decisions." *Our opinion: It would appear to be good practice to have the same team carrying out assessment and supervision. Caveats to this approach would be ensuring there are some checks and balances in the process to avoid regulatory capture or any other bias. The certification committee is the approach used here to ensure quality and independence.*		2		3		2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	E	The NSA has established a flexible workforce and had not segregated the activities of supervision from assessment for certification purposes. "It's not exactly the same people doing the same jobs. We have several areas, but we have flexible staff because the background is bigger than we thought because there are people from our RUs/IMs working with us at different levels and so they can redirect their efforts to supervision or enforcement because they've been working on these areas in a lot of years before coming to NSA staff. So we try to make a flexible framework, staff, and the information and documents are open for every NSA staff member." *Our opinion: It is potentially good practice that the NSA permits open access to information and documents for all staff as this encourages information from assessment to be shared during supervision and vice versa.*		1		1		1	
I	Rail	PL	The NSA has current plans to create separate departments for carrying out the activities of assessment/certification and supervision. The separation is something that the NSA believes has been promoted by participants at ERA meetings. However: "The main problem here is possibly not separation or lack of separation but simply the number of people who deal with those things. If separation is needed, it can also be achieved within one unit, provided we have enough staff to deal with those areas. We assume that it would be very close, the cooperation between these two groups of people, whether or not they are two different units. What we don't exclude is that people responsible for certification might take part in supervision but what has to be avoided is the assessor being the only person responsible, the sole supervisor, because that would violate the basic principle that it cannot be the same person. What would be useful would be a… recommendation on the European level to determine the right approach." *Our opinion: the decision to separate the tasks of assessment and supervision may be driven by the small number of staff that are expected to perform each activity and the desire to ensure that it is not the same person doing both tasks. The NSA is open to having colleagues working closely on both activities. However, the experience of other NSA suggests that separating activities by department can bring problems in the future, particularly if the size of these departments increases in the future and they remain separate.*		1		1			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	NL	Interviewer: "Your NSA indicated that it has different staff carrying out the activities of supervision and enforcement, and the assessment and issuing of certificates and authorisations… and that little information is exchanged between the two teams. Interviewee: "Yes. Too little. The difference between the granting of certificates and the inspections has been too big. We are all filled with the thought that we should talk more often… because there have been big differences between the departments, but we are all convinced that these differences shouldn't be there. The bosses now think that we should talk more often to each other, and four times a year, all rail staff talk to each other. It's not a coincidence that we have different parts in our organisation granting the certificates and for inspections. The enforcer should be independent… they're very loose from the certification department… because that's the independency we work to. We also have that the person who has given a certificate is not the one that did the inspection, and the other way around. So it's divided in persons, and at this moment, it's also divided in department, but it has always been divided in persons." The NSA also explained the exchange of information between the supervision team and the certification team: "Enforcement is very loose from the granting of certificates. They're different roles, which also explains why they're two different divisions. Of course [we exchange enforcement information] but the question is, how far it should influence their inspection, their assessment? There has to be an influence, but how big it has to be, we think it only has to be [a] big [influence] if there is a tendency for the incident to happen frequently. We tell the other division… that there has been an incident and that the inspectorate did something. Not everything [is shared]." *Our opinion: The national laws of this NSA prohibit certification and enforcement being carried out by the same persons. This has been implemented by dividing the two activities into entirely separate departments. This strict division is not considered good practice and Article 6 of the forthcoming CSM on Supervision is clear that information gathered from supervision and assessment should be shared so that both activities can benefit. This NSA has recognised the difficulty that has been created by this division and is working to improve communication between the two departments. However, the two activities are considered separately and this influences the level and amount of information about enforcement activity that is shared with the certification team. This NSA stated that only frequent incidents should have a*		-1		-1		-1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			strong influence on the assessment procedure and indicated that the inspectors will make their own decisions about whether it is relevant to share information. The possible risk with this approach is that the certification team may have specific concerns about the SMS and may benefit from all evidence relating to an RU/IM's performance. Some incidents that were subject to enforcement but not shared with the certification team could be evidence of suspected weaknesses in the SMS.							
I	Rail	S	The Swedish NSA has a department that assesses and supervises RUs and a different department that assesses and supervises IMs. With regard to consistency, "There we have a problem. We try; we think it's very important to be consistent to have similar decisions and acts to similar RUs/IMs, but that's the problem with that, because we are organized in different departments. We have one department working with supervision and the certification for RUs, and another department working just for Infrastructure Manager. We have not the same guideline. We have not so many meetings to collaborate between these different departments, so we have some problems. We are aware of the problem that we have a way to go there." Historically, the NSA was structured differently: "Earlier we have one department for supervision and one department for issuing different permits. But… in 2007, when [it was] first… about Safety Management System… our team working with RUs seemed to take that step harder and see it [that] we have to use this. Then it… was only ERA guideline at that time, and the other department have talked to some lawyer and said it's just ERA guideline, it's just a guideline, where you don't need to follow it. But we said from our team that it's better: the point is that everybody do the same, so we have to start using it. And of course it was more important that for us because the point is that a railway company from Germany or Denmark came to Sweden, that we have similar decisions—Infrastructure Managers are all in Sweden so they didn't realise the purpose I think. And the regulation has come, and we are on different steps. Then… about two years ago, the Swedish Transport Agency reorganized and we are put together in one department with road and rail, and somehow to try to make the Agency more effective… the leaders think that it's important to have all staff working with traffic in one department (road traffic or rail traffic) and infrastructure for roads and infrastructure for rail in another department. But it's not so good, I think, because we have these problems just now." The problems are based on different documents covering decision-making and permits and can	-1	-1	-1	-1		-1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			potentially lead to inconsistent outcomes and confusion amongst RUs/IMs: "If the Railway Undertaking is having a certificate and we are going through the whole… regulation and set up demands on different things they have to achieve before they can have their certification, we have to see some evidence [of] how they work with staff and all the Safety Management System. [If that] same company is also Infrastructure Manager (perhaps they have some kilometres of their tracks somewhere)… the other departments go through their application and [decide] 'it's all right if you have such a small infrastructure, if… you're buying your maintenance, you don't need to have a Safety Management System.' [If] we… audit… that company, and… we are seeing… a lot of non-compliance with regulation… we revoke the licence or decide to prohibit them so they cannot have their traffic. But at the same time the infrastructure permit is all right, because we have divisions on different evidence. [We think] if the Safety Management System is not working… it's a problem, that somehow the risk is the same and it should be the same division [controlling this]. So if [one part of] the Agency… revoke your permit it should be consistent [with the other part of the Agency] because it's the same Safety Management System… [RUs/IMs] feel we have a different kind of decision. They think… 'why are you having different decisions; why are you revoking our permit? The other part they didn't say that it was not okay?' So that's something we have to work along to try to have consistent." The NSA is now taking steps to address this inconsistency but it is a slow process: "We are… making audits together to try to learn [sic] each other. We have talked to the CEO… but it's taking too long a time for a reaction, I think, but we have started some project with making audits together and we have suggested that new applicants coming in to the Agency we should try to take a step over the edges between the different departments and issue the certificates together somehow, to learn [sic] each other. So the discussion is on the table very often, but it takes long to action." *Our opinion: This example is a frank account of poor practice. It is against the spirit of the principles to have an RU/IM being subject to conflicting and confusing enforcement action. The NSA recognises that it is the structural organisation of the NSA, and the lack of a coordinated and consistent approach between departments, that has led to this situation. The NSA is demonstrating good practice by trying to address the inconsistency with cross-divisional auditing of new applicants.*							

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	S	The Swedish NSA has prior experience of separating the departments responsible for certification and supervision. It described the difficulties this caused and its reasons for merging the two activities: "The problems… was there was no communication between the supervision team and the certification team, so the staff issuing certificates didn't… know how it is in reality. And then after you have issued a certificate, the supervision team go on an audit and they could see, 'oh my God, this is not good', or, 'oh my God, this is wrong', and the company was very confused because they said, 'but you gave us a permit, why can you say it's not good, why do we have to change a lot of it?' So therefore we put the teams together because it was important to have the acknowledgement on how it is… out… in the companies… and try to look at evidence coming in… to see a way of behaviour in a common way to always make a better system, using and learning yourself. At that time it was also a way of going from supervision details, technical details or something more detailed, and go to check the system: do you have rules for that; do you have communication; do you report this; do you use it for… see if it improves the system? Do you, for instance, have some way or new way of looking at it?" *Our opinion: It would appear to be good practice for assessment and supervision staff to be part of the same team or department and not separated. Experience of the Swedish NSA supports this proposal. Operating the two activities of assessment and supervision separately can lead to situations that are confusing for the RU/IM. It also highlights how an audit can benefit from being more than a document-checking process; if it includes direct interaction with the RU/IM, this can help with understanding how documented systems are practiced.*		-1	-1	-1		-1	
I	Rail	A	The Austrian NSA has partly the same staff undertaking the two tasks of assessment and supervision. The NSA explained this mixed approach: "The first time issuing the safety certificate… was I think September 2010 when we had to change to this new system. At this point [we had] the same person doing the issuing [and] we combined it with supervision activity at this time because we did this for the first time before issuing the first safety certificate from our authority. We also did supervision by these applicants and this was done by the same person. In the future it is possible that we can also change from one person issuing the safety certificate and another person [doing the supervision]… [but] as there is only one division concerned with the safety certificate, it would have to be in the same division. Another person could do the supervision, but it's still… I think it will be a case to case decision who will do the next supervision activity		1					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			All undertakings with new certificates, that means all undertakings which operate in Austria at the moment, have already had one supervision activity. If we continue under the principle of consistency doing the next supervision by the same person or to change to another, or do the first supervision by another, it will be also a continuous change of who will be doing, who in person will do this supervision activity. Each way has its advantages and its disadvantages. So I think that our strategy will be that we mix it. We do it once this time and then change the person. Because the person who has done the issuing has of course the most experience in the processes of this undertaking, and then it could also be of course a good idea to let someone look into the undertaking who doesn't have this experience and just begins… looking from a new point of view. So our decision will mostly be in both ways. It's also quite easy for us in the Austrian authority because of the… limited number of persons… we have an exchange of information within the participants of supervision that are doing safety certificates and this happens in regular meetings. When a supervision activity is planned, there is a more intensive exchange of information." *Our opinion: It has been suggested by other NSA that having the same person assessing an applicant and then supervising them it may lack independence and be subject to bias. The principle of consistency is used to support this decision. The approach described by the Austrian NSA is likely to keep supervision and assessment activities within a small team of people, who will meet regularly to exchange information, especially if different staff are responsible for assessment and supervision.*							
I	Rail	D	"Supervision for us is a continuous task. Certification... Assessment or reassessment of the SMS is more a function of... It's not that continuous as supervision is. So, there are fixed supervision teams and the assessment teams are not permanent, I would say, they are convened or put together when necessary or on a case by case basis. " Interviewer: "And is it that the assessment team is put together from a pool of staff who are responsible for supervision?" NSA: "Yes, for example. There could also be other staff but then I think most or any of them would come from supervision staff."		1		1			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Interviewer: "In the questionnaire we asked about the amount of information that's exchanged between the assessment process and the supervision process for a particular undertaking and the response was that some information is exchanged rather than, say, for example, all information. Could you explain more about how information is exchanged between the two functions? NSA: "Well, the information exchange is mostly, I would say, that the supervision findings or aspects or whatever, the outcome of the supervision, is stored in a central database and is available for the information of the assessment team. If the staff is the same, then one could also have chosen all information and then they know anything and they take their knowledge with them for the assessment. In any case, it's anything that is stored in the central database." Interviewer: "So, could it be that, for example, some undertakings, when it comes time to reassess their safety certificate, that that may be done by someone who is familiar with the supervision of that undertaking and then for another undertaking it could be someone who is only able to use the database because they don't have any familiarity with the undertaking?" NSA: "That should normally not be the case, just someone of that team should be familiar with the supervision of the undertaking." Interviewer: "So, if not everyone in the assessment team would necessarily be familiar, at least one person ideally should be?" NSA: "Yes, and will be. It's something that has to be taken into account when the assessment team is put together, that you have the adequate persons in it." *Our opinion: The NSA organises its resources to deal with the principal task of supervision. It assembles assessment teams from this pool of staff as and when necessary. It sees this as an efficient approach to providing resources for both activities of assessment and supervision. To facilitate exchange of information between the two processes, assessments should almost always include someone from the team that has good knowledge of the RU/IM. The NSA also has a central database system for storing and sharing the information that the NSA has collected on each RU/IM.*							

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	F	The NSA described the exchange of information between assessment and supervision: "It's quite good because when we begin an inspection or an audit, notably systematic audits, we ask our authorisation colleagues if there are any particular subjects they would like us to look at because during the authorisation process obviously there's an exchange, exchanges take place between the person asking for an authorisation and our authorisation department. Our guys in this department say you sent us this document but there are still other documents missing, or, the document you sent doesn't give enough information as to what we need. Some entities send you everything you need and you don't even have to ask them any more questions, from my understanding. Some others will provide what's required but after a lot of to-ing and fro-ing and some obviously are very difficult. So we give our authorisations people the opportunity, notably when we go and do the audit, so we're not just looking at the very pristine document which is the final SMS document, we also get some accompanying feedback from our authorisations people and where they thought there may be a cause for concern. And the corollary to that, an entity comes up for its renewal, the authorisation people will… see on our documentation system… all the inspection reports and audit reports… but they can also come and say… "how is this particular entity - has he carried out all the corrective actions?" The authorisations people come and ask us what's the situation with the non-conformity closure, how far they are with it and have we had any particulars problems." *Our opinion: The exchange between the two activities is facilitated by the electronic document management system but there is also a culture of the two teams discussing particular RUs/IMs at relevant points in the assessment and supervision process.*		1		1		1	
I	Rail	GB	The NSA explained that the benefits of having staff in the same team for assessment and supervision extended beyond the sharing of information: "Otherwise… just because of the geography of where people are based, you'd have a number of people doing a lot of travelling so… from an efficiency point of view, go back to resources, seeing if there's a more efficient way of doing it." Combing the two activities is not only an efficient approach when staff are geographically dispersed, it also helps to smooth the workload. The NSA was keen to point out that staff flexibility is essential							2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			because the workload for assessment and supervision was subject to fluctuations and if staff were only trained and able to carry out one activity, the NSA would have "people sat doing nothing for long periods of time". *Our opinion: It is good practice for the NSA to consider the practical implications of separating activities and to adopt a structure that maximises its available resources.*							

Table B.2: NSA general structure – desktop and interview findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	B	Has a safety committee which is comprised of the Director-General, the directors of the operational departments, the risk manager and the manager of the Accidents and Incidents Investigation Unit. The Safety Committee, which convenes three times per year, is responsible for: • discussing and selecting the aviation risks to be handled with priority • taking corrective actions where necessary • assessing, approving and modifying these corrective actions • validating and amending the Strategic Action Plan • discussing and following up on the bimonthly reports on occurrences that require immediate action *Our opinion: The concept of a committee to oversee the strategic decisions of the safety authority would appear to be good practice. Such a committee has the potential to improve consistency across the different activities of a safety authority.*	2	3	2	3		2	2
D	Aviation	IRL	Outlines structure of organisation, the four distinct departments and the activities they perform, including which are responsible for certification and regulation of different parts of the industry. *Our opinion: It is good practice for the structure of the safety authority to be transparent.*			2				
D	Aviation	IRL	Provides clear structure and objectives for its Safety Regulation Division, including organograms for the departments and sub-departments. *Our opinion: It is good practice for the purpose and structure of the safety authority to be transparent.*			2				
I	Rail	NL	The Dutch NSA is divided into two parts within the Ministry: • Inspectorate: the main part of the NSA is a department within a division that is responsible for inspection and enforcement of environmental issues and road/rail transport. It is responsible for all tasks of supervision and enforcement but it is not responsible for policy-making and decisions. • Ministry: the other part of the NSA sits within the Directorate-General division and is part of the Directorate for Public Transport and Rail. This part of the NSA is responsible for policy-making and policy decisions. Examples of how this organisational structure works in practice:				1		-1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			• NSA 'strategy' document is produced by the Ministry. This document outlines what is important for railway safety over the coming year. Whilst the Inspectorate will contribute information to the document, it is written by the Ministry. • There is a focus on 'enforcement' for the Inspectorate which the respondent felt was "worse for safety" as it took away focus from the tasks of issuing safety certificates/authorisations and supervision. Respondent always assumed that the Inspectorate's role was to "make sure the railway is safe"; the recent remit "to enforce" means that the Inspectorate no longer feels that it is always acting to make the railway safer. "Enforcement of law is not always the best tool for safety". *Our opinion: It is good practice for an NSA to be established so that it is governed by a policy that promotes safety. If an NSA is directed by a policy or strategy that is set by a department that is detached from the daily activities of the NSA, a disconnect can occur as demonstrated by this example. It is not necessarily poor practice for an NSA to exist across governmental departments; however, there should be systems in place to ensure that it can function appropriately. It is undesirable for frontline staff of the NSA to feel that they are following a policy that is inappropriately focussed and unable to deliver the safety benefits that are desired.*							
I	Rail	NL	"The differences in point of view from the safety interest: the people who think safety is the highest good; and the people who think enforcement is the highest good. And the way we are now organised, we are in an inspectorate where most of the law people are in a department that's very very aware of enforcement, so we are pushed into the way of thinking of the enforcement people. So that's why the highest priority is the sanctions." *Our opinion: A further example of how organisational structure can determine the approach taken by an NSA. There appears to be a cultural shift in this NSA that is contrary to the approach favoured by the inspectors who are charged with supervision and enforcement. Whilst NSA should be free to establish their own approaches to supervision and enforcement, the principles of proportionality and consistency should be followed – and the goal should be a safe and accessible railway market. If the inspectors have concerns about the style of enforcement they are being asked to pursue, these concerns should be considered and resolved so that inspectors have confidence in the approach they are following.*						-1	
I	Rail	DK	This NSA, as with several others, has no supervisory jurisdiction over matters of construction and health and safety when a line or site is not connected to the network. "During the construction work it's solely our labour inspectorate. And that includes when they… stop the traffic and they start digging, when they start digging we are out of it. And if they are building a new		-1			-1		

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			track and it's not connected, we don't have anything to do with it." The NSA's involvement begins with the safety authorisation or certification. *Our opinion: It is relatively common for NSA not to be involved in supervision and enforcement when a live link to the network is not present. It is desirable for the RUs/IMs involved to operate to the same standards and use the same SMS that they would for live operations. Cooperation with other regulatory authorities in the Member State, and a common approach, would be good practice.*							
I	Rail	PL	The NSA also functions as the market regulator and the passenger rights watchdog. This can affect where and when resources are required: "For example, there is a winter change of the timetable and then there may be passenger complaints, which means that at a certain time, most – or simply all – of the resources are devoted to dealing with passengers complaining about the new timetable. With the short resources, focusing on one thing means the others are left behind. Performing many inspections means that they'll be less detailed or the quality will deteriorate slightly. There are no clear, fixed or permanent rules or mechanisms of setting priorities… there is… an assumption that safety takes precedence but, again, it may have to be replaced if something occurs, like maybe the winter timetable change happens." *Our opinion: It is good practice for NSA to be able to plan in a way that prioritises safety with no exceptions. The exceptions discussed in this example may not be sufficient reason to divert resources from inspections that are critical to safety. To assist this goal, it is desirable if NSA are not given too many conflicting roles and are structured in a way that enables them to fulfill the tasks assigned to them by the Safety Directive.*		-1		-1		-1	-1
I	Rail	BG	Supervision staff are organised into three regional inspectorates, with five inspectors in each unit. The NSA has proposed to increase each unit by one member of staff to be able to accommodate the extended scope of activities introduced by the European safety regulatory framework. *Our opinion: It is good practice to plan future expansion and balance it across different divisions.*							2

Table B.3: NSA subcontracting – interview findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	E	The Spanish NSA reported subcontracting 'some specific inspection tasks related to rolling stock or staff' to the largest IM in the country (ADIF). The NSA explained that the IM has the necessary experience to carry out these inspections: "ADIF was doing these activities for many years and so we are trying that they continue. They are doing it continuously because they have the experience and we are delegating in them this competence because we don't have sufficient NSA staff to make these activities, such as accident investigations, alcohol controls, etc." The NSA meets monthly with inspectors from the IM to discuss findings and any necessary controls. The inspectors from the IM are given guidelines regarding how they should conduct their activity. The NSA stated that: "They [IM inspectors] have a lot of autonomy to make these activities because they have the specific procedures and they know very, very well the sector and they have sufficient staff to make this." However, this autonomy does not apparently extend to enforcement decisions, which remain under the authority of the NSA. It will apparently use all of the information and evidence provided by the IM to then make an enforcement decision. *Our opinion: Subcontracting of supervision activities is not permitted by the European safety regulatory framework. The point made here is that these are inspections relating to national rules and this is a continuation of an existing process. Nevertheless, there has to be some caution exercised in a process that relies on an RU/IM reporting back to the NSA information it believes is appropriate for the NSA's tasks, rather than NSA staff gathering that information themselves.*				-1			

Table B.4: Examples of strategies from other safety authorities

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	IRL	Has an enforcement strategy and policy document online at: http://www.iaa.ie/index.jsp?p=93&n=97&a=225&pp=516&nn=520&lID=856 The document describes how the IAA will enforce flexibly and fairly, being both practical and consistent. It describes the following approaches: • Contraventions of the regulatory framework when operating under an SMS will be dealt with first by discussing corrective action. • Remedial action will avoid enforcement if the service provider addresses the underlying contravention in a way that is judged to "prevent recurrence and foster future compliance". Enforcement action will only be considered when the service provider fails to provide effective corrective measures. • A flow diagram to describe the steps taken by the safety authority if an audit finds that corrective action is required. The flow diagram shows that service providers are obligated to respond with a corrective action proposal within a given time frame. Failure to comply with the deadline leads to a reminder and then escalation to a proposal for enforcement action. Failure to respond to this may then lead to the proposed action being taken. However, if service providers respond in a timely manner but do not propose appropriate corrective action, there is no alternative escalation policy—the diagram indicates that they will simply be set another deadline to respond—and thus an impasse could potentially occur. • A second flow diagram outlines the procedure to be followed if a service provider disagrees with an audit finding. It is escalated via the Lead Auditor and then Associate Director after which it will enter an appeals process wherein the team of Directors and audit team leader will consult. Independent experts can be called upon if required. The final escalation decision rests with the Director. • A description of enforcement measures, in order of severity. • A third flow diagram to show how dereliction of duty amounting to gross negligence will be considered within a 'just culture' framework. • Suspension or revocation of a service provider's licence is never taken as a punitive measure but only to ensure safety. • Proportionality is based on two sub-principles: ○ take action against those who consistently and deliberately operate outside the applicable regulatory requirements; and ○ educate and promote training or supervision of those who show commitment to	1	2	1	1		-1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			resolving safety deficiencies. • Natural justice and accountability is applied to enforcement by ensuring decisions shall: ○ be fair and follow due process; ○ provide confidentiality as far as practicable; ○ be transparent to those involved; ○ take into account the circumstances of the case and the attitude/actions of the certificate/licence holder when considering action; ○ be consistent with actions/decisions for like/similar circumstances; and ○ be subject to appropriate internal and external review. *Our opinion: The policy document and enforcement strategy offers many examples of good practice. It is published online and was issued for consultation beforehand, which delivers elements of transparency. The inclusion of flow diagrams to describe how the safety authority deals with non-compliances is a clear and accessible method of disseminating aspects of the decision-making process. It also demonstrates consistency of approach. The safety authority enforces in accordance with principles, which are explained.* *Concerns do exist regarding the firmness of the approach: there appears to be an unwillingness to take enforcement action without first exhausting other means of delivering safety. This focus on 'influencing behaviour' rather than 'forcing behaviour' may not discourage service providers from committing breaches, and may not encourage a proactive approach to developing an effective SMS.*							
D	OSH	GB	A national strategy (http://www.hse.gov.GB/strategy/strategy09.pdf) with the following key features: • A clear mission statement describing the authority's intent. • Targeted at all parties in the chain (management, workers, third parties) to show that everyone can play a part in safety. • A goal-based structure, where each goal is a shared objective. • An inclusive approach: entitled 'Be Part of the Solution', the strategy seeks to engage and empower the industry. It emphasises the role of the safety authority in working *with* the industry. *Our opinion: The strategy makes clear to industry and the public the role of the regulator and how it operates, as well as the broad responsibilities of the industry. It is published online to promote transparency. By describing the general approach taken, the safety authority is taking steps to be accountable for its activities. The style of the strategy is commendable for being accessible and inclusive, with clearly defined key messages for the industry.*			1	1		1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	A	Occupational Safety and Health strategy 2007-2012. Strategy led to setting up an expert Committee to compile proposals on 5 subject areas: • Risk assessment and hazard awareness • Accident prevention • Prevention of work-related and occupational diseases • Instruction and advanced training and information concerning occupational safety and health, improving the activities of prevention experts • Raising awareness of occupational safety and health. Each area had a specific working group assigned to it. Abstracts of the projects within each group are listed online. The five working groups are composed of representatives of institutions directly or indirectly involved in occupational safety and health, such as ministries, state governments, accident insurance companies, social partners, stakeholder groups, safety engineering and occupational health centres, research centres, universities, regulatory agencies, companies, associations etc. Issued several promotional materials including: • Poster (http://www.arbeitsinspektion.gv.at/NR/rdonlyres/BB85C7BB-7D69-44DC-ABBC-B4186A33B114/0/Poster_Essentials_Austrian_OSH_Strategy.pdf) • Leaflet (http://www.arbeitsinspektion.gv.at/NR/rdonlyres/FC24E83C-291E-4BC4-8BB2-48AFE8174F0D/0/Folder_AustrianOccupationalSafety.pdf) • Presentation (http://www.arbeitsinspektion.gv.at/NR/rdonlyres/5B493695-177A-4593-9E84-DDC0A80FFB82/0/Presentation_Austrian_OSH_Strategy.pdf) *Our opinion: Strategy has a fixed duration with targets for the activities that will be delivered within the timeframe. Timeframe matches wider strategy set across the EU for OSH.* *Strategy establishes core areas for investigation. By establishing working groups comprising a range of representatives, the authority has put in place a distributed framework for delivering the strategy.* *To ensure that the sector is engaged with the strategy, several promotional materials have been produced. Each working group has been tasked with delivering projects in its respective area and these are made available in brief on the website.*			3	2		3	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	A	Clear set of principles for operation published online: • We act according to principles • We go to our responsibilities before the law and conform to uniform principles. • We act in a non-partisan mediator, fairly and consistently. We are trying to convince. • We respect the trust they placed and observe confidentiality. • We quickly decide a minimum of bureaucratic and, in many essential questions independently and responsibly. • We are in direct contact with the market to offer advice that is practical, free and personal. • For emergencies we are available around the clock. • Cooperation and exchange of experiences in our work take a high priority. • A detailed recording and analysis of our business enables us to set the priorities and specific actions. • We are responsible with public funds by improving work processes and continuously improve the efficiency and quality of our work through the proper use and promotion of our employees. *Our opinion: Key principles are in bold. A promise to minimise bureaucracy is helpful to dutyholders. Setting priorities based on analysis of records shows a data driven approach to supervision/enforcement.*			2	2		2	2
D	Aviation	GB	Enforcement of safety issues through the 'significant seven' safety issues, outlined in the Safety Plan (loss of control, runway excursion, controlled flight into terrain, runway incursion, airborne conflict, ground handling, fire). Outlined actions to mitigate these key risks, which have been validated through consultation with industry. *Our opinion: Another approach to strategy – this time using a thematic approach guided by key industry issues.*			2			2	
D	Aviation	GB	Guiding principles outlined in Safety Regulation Group Code of Practice http://www.caa.co.GB/docs/3/SRGCodeOfPracticeApril2010.pdf: • Fostering a culture where safety is paramount • Operating as a cohesive organisation under the direction of the CAA board • Working together effectively, internally and externally • Developing and empowering our staff, and valuing their contribution • Continuously improving our performance and processes			1	1	1	1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			• Playing a full part in the activities of international aviation organisations in support of the GB's needs • Implementing an open and fair regulatory regime based on robust principles and processes. *Our opinion: Defining and publicising the principles that will guide an authority is good practice. Of note is the commitment to international cooperation.*							
D	Aviation	GB	The Code of Practice covers information and openness (publishing guidance of applying for certificates, safety statistics, annual report); consistency (including liaison with other authorities and enforcement bodies); consultation and communication (inviting the views of individuals and industry before implementing changes, conducting regular surveys with those they regulate); courtesy and helpfulness; value for money; and complaints. *Our opinion: Defining and publicising a code of practice is similar to having a set of principles and is also considered good practice. The range of commitments here includes cooperation with other authorities and regular surveys of the regulated market, both of which are good practice examples. It is desirable to be explicit about such goals.*		2	2	2	2		
D	Aviation	IRL	Includes an Action Plan for the authority. This highlights key industry challenges for the forthcoming period (focuses attention of both the authority and the industry). Actions are described in full with delivery dates. Include activities such as: • Promoting regulatory changes across the industry, engaging in EU-wide central agency activities • Establishing specific action groups to address key industry risks (e.g. runway incursion) • Publishing an enforcement policy demonstrating fairness (Q4 2011) • New website with easier navigation (Q1 2012) • Engaging in reviews of regulatory frameworks in other locations (e.g. USA) to highlight and reconcile any challenging differences (key point here is that NSA appear to be less able to reconcile differences between national and EU regulatory frameworks and may be lagging behind some aviation authorities) • Development of safety leaflets for specific issues. *Our opinion: An action plan helps set the programme for delivering the strategy. It is good practice to inform the market of what specific changes it can expect and when those changes will be delivered.*			3	2	2	3	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	GB	A pledge. Companies were invited to sign up to the following pledge: We, the undersigned: • Agree to play our part in reducing the numbers of work-related deaths, injuries and ill-health in Great Britain. • Call on employers to put health and safety at the heart of what they do and to take a common sense approach to health and safety. • Commit to debunking myths around health and safety that trivialise the impact of injuries, ill health and deaths on individuals and their families. • Recognise the importance of health and safety in difficult economic times and the dangers of complacency. • Pledge to work with the Health and Safety Executive and its partners to Be Part of the Solution. The website then displays the names and logos of all companies that have made the pledge. *Our opinion: This is a novel method to promote the goals of the regulatory framework in a public form and encourage companies to adopt them. The public commitment may increase the obligation and motivation to comply within each organisation. It would be desirable to agree the criteria for such a pledge at a European level to ensure consistency. It could then be administered at a national level by NSA. There may be a cultural difference between OSH regulation and rail regulation that undermines this approach – rail regulation is, after all, driven by a standards and rules. However, management using SMS places greater responsibility for delivering railway safety on the shoulders of RUs and IMs – as such, this type of pledge may help to instil a greater sense of responsibility for delivering this within each RU/IM.*			3				
D	OSH	GB	A delivery/business plan (http://www.hse.gov.GB/aboutus/strategiesandplans/delivery-plans/plan1112.pdfhttp://www.hse.gov.GB/aboutus/strategiesandplans/delivery-plans/plan1112.pdf): Updated annually, hosted online and available for download, the business plan outlines how the authority will deliver its mission statements over the year. Each mission statement has several specific components, below which are listed the milestones and evidence required to monitor progress. *Our opinion: A delivery or business plan of this type makes it clear to staff within the authority, and to all external parties, which activities will be the core focus for the year, how they will be measured and why they are important to the marketplace as a whole.*			3	2	2	3	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	GB	The Code of Practice sets out service standards (similar to a service pledge), specifically: general service standards; finance service standards; and approval, certification and licensing service standards. They aim to achieve their standards on 90% of occasions. *Our opinion: A key element of transparency is for NSA to specify what the market can expect of them. It is good practice to establish the criteria for measuring NSA service performance, set targets and then commit to a high level of performance, as with the example here.*			3	3			
D	Aviation	GB	Documented safety plan including a desired capability outcome for SMS along with actions, deliverables and dates, expected safety benefits, and KPIs. • A high-level governance panel that includes industry managers to 'oversee, steer and challenge' the safety plan. • Wider Agency/industry panel to review progress and provide feedback on plan annually. • Regular working groups, conferences and committees to review whether current risks are still a priority, to discuss and share actions to mitigate risks and to raise any subjects of specific interest. *Our opinion: the first statement suggests the authority could be trying to run the industry. The following statements regarding steering groups may be effective as long as they do not attempt to run the regulator. The general theme of cross-dialogue between the safety authority and the industry is good practice; however, that dialogue does require boundaries to be set on both sides to ensure that the relationship between the regulator and the industry remains appropriate.*			1	1		1	
D	OSH	IRL	A published Customer Charter which describes RSA's principles, namely: • Develop and use best practices and procedures to achieve and maintain high standards of service quality. • Consult our customers to identify their needs and develop our services to meet those needs. • Deal with our customers in a straightforward, polite, helpful, open and professional manner. • Treat our customers fairly and consistently. • Lay the foundations of quality customer service through the provision of good working conditions for our staff. *Our opinion: It is good practice to provide and document a complaints procedure.*			3	3			

Table B.5: Examples of NSA strategies

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	NSA has a vision document and a five-year plan. The plan is a consulted document: "that consultation happens so the industry knows what we are going to do for the incoming year. They will get a report at the end of the year saying, this is what we did with you. This is what we found. These are big issues, going forward. We do the analysis of their compliance through the Railway Management Maturity Model, so that will lead to an important discussion at the end of the year to say, actually, you know, last year we analysed you at X. This year, has it changed? Has it improved? But that again leads to a conversation of, you need to do more here; you need to do less there, or whatever it might be. So again, they've got another mechanism for being updated as to what we think of their performance, and where they can get better." *Our opinion: It is good practice for a strategy to be longer term, with an accompanying supervision plan being released annually. It is desirable to update the industry by way of a report on its progress with meeting the objectives of the strategy. The Railway Management Maturity Model adds further detail to this review process.*			3	3		3	
I	Rail	DK	The Danish strategy and supervision plan is published on its website and is made available to all stakeholders. It states the goals of the NSA, which include: • Supervise the railway undertakings' handling of their responsibilities relating to safety on the railway. • Show trust in the undertakings and carry out less supervision when the undertakings provide documentary evidence that they have 'have control over their affairs' and vice versa. This publication seeks to state specifically how this may be achieved in practice. • Four principles for how the Authority's general supervisory activity would be carried out: a clear distribution of roles between undertaking and authority; efficient utilisation of resources; transparent high-quality supervision; and documented outcomes of the supervisory activities. The document also outlines: • How the NSA will evaluate its performance and that of the sector. • What audits and inspections entail. • How the programme of audits will be prioritised. • The methods of supervision and enforcement that will be used. • Methods of communication and cooperation.	3	3	3	3	3	3	3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: The strategy describes clearly the approach the NSA will take and how it will supervise the sector. It demonstrates good practice by detailing a strategy that follows each of the principles of supervision.							
I	Rail	A	The NSA does not have a supervision strategy currently but is developing a long-term strategy (4–5 years) that will be accompanied by annual action/delivery plans. *Our opinion: This is a good practice approach to developing and delivering strategy.*			2	2		2	2

Table B.6: Strategic inputs - all findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Rail	GB	Targeted plans are top-down and bottom-up: "we plan by looking at the risks, at a high level, but actually, there's a plan from bottom up as well, so the two have to blend". If inspectors at local levels report that they are finding consistent problems with certain activities, this will be fed back to the NSA. If the concern appears to be genuine, and an indication of an emerging problem, it will find its way into the strategic plan for the coming year. NSA acknowledges that some issues are not apparent in the "huge model" that is used for targeting activities but this does not mean they are ignored. The bottom-up approach ensures that the NSA targets fresh issues as they arise as well as ongoing problems. *Our opinion: It is good practice that strategies for supervision are developed using both top-down and bottom-up processes. Top-down processes are commonly described as using national incident statistics and CSIs in order to build a plan of the activities that require supervision. However, top-down approaches may overlook emerging problems—until they become sufficiently frequent to feature in annual statistics. The approach described here is to engage with frontline inspectors to collect information on emerging issues. These issues can then be a focus for proactive supervision in an attempt to address the underlying causes before the issues become frequent incidents. It is important for NSA to be open to emerging patterns of behaviour and the risks associated with them.*						2	2
D	Rail	GB	Prioritisation can be about directing resources at issues where there are concerns: "Track brakes, you know, should we be looking at track brakes as a development of improving rolling stock braking? Discuss. Well, we've actually taken the option this year of going, yes. We're going to devote some resource to having a look at that, because actually we think, given the leaf fall issues and low adhesion, it's the logical next step for improving risk control. None of the duty holders are prepared to touch it with a barge pole. We actually think there's some credibility in there. Right; we'll do some work this year to suss out whether that's got some value or not, and then we'll decide the outcome of that, whether we need to then progress it into a further work stream to push it out to the rolling stock manufacturers, and the TOCs for take up, but it's about trying to say, we think there's an issue there. We think that it needs bottoming out, and actually, no one else is prepared to do it. We've got to get on and do it. So we will put some resource in there. And I see that as prioritisation."						3	3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: The NSA is identifying areas that may not be emerging as a problem currently, but have the potential to. It is directing resources at areas that RUs/IMs may be neglecting, even if this has not led to incidents. It is important to note that strategy decisions are about prioritising issues that may be of future importance.							
D	OSH	GB	A national strategy was developed following three months of consultation, with events across the country. The theme of this event was to invite all interested parties to become 'part of the solution'. This type of proactive language was used to stimulate positive engagement with the regulatory framework, and to show that the regulators were actively engaging with the industry. The strategy was provided online as a document for viewing or download, as a presentation, and also in video format. *Our opinion: Offering multiple methods of dissemination (document, presentation and video) is good practice, especially when trying to engage the industry with important strategic plans.* *The foundation for the strategy approach in this example was a plateau in health and safety performance, which the safety authority attempted to address by engaging directly with the industry via a series of strategy-planning events. There is a risk that industries can become complacent when a satisfactory level of safety performance is attained: this can inhibit further improvements.* *Many NSA may not be in a similar situation but this approach may still provide transferrable benefits. Consultation and positive dialogue with the industry prior to launching a strategy will help build good relationships with stakeholders; this approach may encourage industry members to feel as if they hold a large stake in the safety performance of the Member State. From the outset, RUs and IMs should be encouraged to take responsibility for safety and deliver it how they choose to — the NSA role is to ensure that safety is delivered in the way that is described by each SMS.*			3	2	2		
I	Rail	NL	Targeting areas for supervision is primarily a top-down process, based on risk analysis and an annual report of the network risks. The analysis of risk focuses on violations of law and the likelihood of a dangerous occurrence. More resource is given to supervision and enforcement of the most dangerous areas. The process has limited bottom-up influence. Where this does occur is during assessments and inspections, which can lead to attention being paid to a particular area during subsequent supervision activities. On a more formal basis, there is a yearly meeting of inspectors at which it is possible to discuss emerging issues. Executive management at the NSA can then decide whether the subjects raised should be targeted the following year and "that's the way how the bottom-up						1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			way becomes top-down". In addition, areas are targeted according to whether there are laws that the NSA can enforce. If there are no clear laws to permit enforcement on RUs/IMs, the area is unlikely to be a focus for the NSA. *Our opinion: It is good practice to have an approach to targeting that has multiple inputs, both top-down and bottom-up. This NSA has formalised how it will incorporate a bottom-up approach, the realisation of which could be argued as somewhat inflexible and infrequent. The NSA also seems slightly restricted in what it can target by the need to have enforcement measures available (although it has carried out investigations of issues where it knows there is limited scope for enforcement). It may be better practice to be open to targeting a wide range of areas given that safety hazards might be discovered that should be subject to future enforcement.*							
I	Rail	A	The NSA is awaiting the forthcoming CSM on Supervision before finalising its strategy and supervision plans. "We look forward to the new regulation concerning the provision. So it's the strategy, the supervision strategy, the general strategy, and then we also try to develop of course at the same time the data which we use for coming to a result, which undertaking we should supervise at which time, and… there is different data, like the safety report made by the undertaking, of course the reports by the national investigation bodies, or also complaints, for instance, which are taking into account all the approval, or which approvals and how much they will be undertaking, for instance, as applied for. We also have periodical meetings with railway undertakings, so these are all… is there anything else? Of course the performance supervision results also take that into account. Yes, one could say that's most of the data we think of at the moment." *Our opinion: The NSA is aiming to adopt a good practice approach by aligning its strategy with forthcoming regulations. It currently has a wide range of data inputs that it is likely to use when developing its strategy.*						1	1
I	Rail	PL	The NSA notes that the supervision principles are "just a small part of the fourth annexe to the regulation" and it is awaiting "the more detailed regulation on CSM in the field of supervision". Until it is adopted as a Regulation by the European Commission, the NSA will struggle to construct a convincing argument to increase its resources for this task from the 1–1.5 employees who are currently responsible.						-1	-1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: This report is benchmarking NSA against a set of principles that are soon to be bolstered by the CSM on Supervision being released as an official regulation. Some NSA are restricted in the changes that they can initiate prior to this regulation coming into force.							
I	Rail	PL	The NSA made recommendations for further European guidance on how NSA should conduct supervision: "I believe a common or unified approach is necessary across all the member states to determine what is the necessary level of resources to properly carry out the supervision duties. Without a suggestion, at least, at the EU level, you cannot expect the proper level of implementation of supervision in various member states. For this reason, the SMS maintenance would be insufficient." *Our opinion: NSA strategies for supervision are contingent on having appropriate resources available, which is a Member State decision. Stronger, clearer direction from ERA and the EC on the scope of resources required is desirable for this NSA, but is likely to be contingent on the market for each Member State.*							

Table B.7: NSA without strategies

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	BG	The NSA does not have a formal strategy that is documented as such: "Regarding the fact that we do not have such a formalised sort of strategy, our activity has the nature that we strategically implement our plans, meaning supervision, meaning safety certification, and authorisation. The development of the sector in this aspect of safety. What exactly we do is defined, specifically, the rules of procedures of our agency." The NSA has on its website a list of 'administrative services' that outline its role. It is therefore clear to the market what functions the NSA performs. *Our opinion: Whilst the NSA is clear about its functions, it does not openly explain to the sector how it will strategically 'develop the sector in this aspect of safety'. There is an implicit objective to improve safety but it is not realised into a strategy that extends beyond fulfilling the required functions as an assessor, regulator and supervisor. It is good practice to define a strategy for improving safety that proposes to deploy the functions of the NSA in a way that will develop and improve the sector.*			1	1			
I	Rail	CZ	The NSA has not made any changes to adapt to the principles of supervision since they were introduced. It's strategic priority is to create a system for SMS assessment: "First we have start prepare new methodology for the assessment of safety management system. It is the most important. I think now we have to do very important work to prepare internal rule or questionnaire for issuing safety certificate part A, publish some instruction on the web for the applicant, and develop methodology to assess safety management system of applicant, it is now the very important part. I think that supervision of existing railway undertakings for which were issued safety certificate, but certificate issued not with compliance with this regulation, but only with Czech position of safety director, which was quite different. So I think it's not bad to require these things now, but for the next way for safety certification. To explain you, I think, in 2007 and 2008, there issued vast majority of safety certificates in a very short time. It means the certificates are valid for five years, so it means that in 2012 and 2013 they will be issued again. There will be new certification. So I think in this case, check that consistent with this regulation for these, all certificates, is not		-1	-1	-1		-1	-1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			necessary. We will do it in those second certification." The NSA will create a strategy for the safety certification assessment process, "which is now much more important than supervision." *Our opinion: It is apparent that the majority of operators have not been assessed under the new, SMS-based regime. As a result, this NSA is focused primarily on using its resources to provide this new certification service. It would appear that a coherent strategy for targeting NSA supervision activity is not a current priority and as a consequence, it is unlikely that supervision activity meets the requirements of the safety regulatory framework.*							
I	Rail	E	The Spanish NSA did not report having a formal strategy as yet. However, it did describe its current aims: "We think that we have to change the point of view of our RUs/IMs in involving them in the European regulatory framework… to make sure that the regulatory framework can be adhered to … a better understanding for RUs and so we consider that inform them and make them to understand the European regulatory framework is the most important… That's the main, one of the main activities of [the] NSA." *Our opinion: Although the NSA does not yet have a strategy, it is demonstrating good practice by focusing on supervising in accordance with the European framework.*						1	
I	Rail	E	"Our strategy of this supervision and enforcement, first of all, is to develop completely our procedures, to communicate these procedures to RUs and IMs of the sector, and then we hope next year to make the first audit to one RU and we will try to increase our NSA staff to try to make more audits. First we will start next year with one audit per year and we will try to increase this about four or five audits a year." *Our opinion: The NSA's strategic priorities are to put in place consistent and transparent procedures from which will follow assessment and supervision in accordance with the European framework.*			1	1		1	

Table B.8: Compatibility between national and European legislation

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	GB	"Statutory functions include proposing new or updated laws and standards, conducting research, providing information and advice, and making adequate arrangements for the enforcement of health and safety law in relation to specified work activities." *Our opinion: An important consideration for NSA is that national legislation provides them with sufficient statutory functions. The survey of NSA has highlighted occasions when such functions are incomplete or diluted. The function to propose changes to national/European legislation where necessary is considered desirable, as is the ability to research and advise. The CSM on Supervision will regulate that NSA should make recommendations to the Member State to overcome deficiencies in the safety regulatory framework so this function should be a clear part of an NSA's powers.*						1	
I	Rail	NL	The new regulations (1158/2010 and 1169/2010) ask more of the industry than Dutch law (this is for the CSM-CA element of the regulations, rather than the principles of supervision). The respondent stated that Dutch law needs to find a better way to enforce these regulations because under the current system, if an RU/IM did not comply, the NSA would struggle to refuse an application for a certificate/authorisation on such grounds. In practice this has not happened but it is a risk. *Our opinion: It is good practice for national legislative frameworks to be compatible with the European safety regulatory framework. It is undesirable for there to be any doubt about the NSA's ability to enforce the European safety regulatory framework; such a situation may undermine safety and may also work against a harmonised single market for railway operations.*	-1		-1			-1	
I	Rail	BG	The Bulgarian NSA incorporated the principles of supervision directly into its Railway Act. *Our opinion: European Regulations apply directly and do not need transposition into national legislation. However, it is beneficial to incorporate the principles if it improves compliance.*				2			
I	Rail	CZ	The NSA described poor transposition of Article 8 of the Safety Directive (2004/49/EC). This poor transposition has been noted by the Commission. The fault appears to enable applicants to be issued with a safety certificate without having an SMS that conforms to the national safety rules of the NSA. This may be a reason for the NSA continuing to be responsible for supervising that its national safety rules are adhered to by RUs/IMs. "Bad transposition is a major problem. The Ministry of Transport says everything is correct. We have only say some comments when the new regulations are prepared, but they usually, not everything take into account. That, I think, is not problem only of Czech Republic, it's a problem of many states, the			-1	-1		-1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			transposition." *Our opinion: Significant flaws in the transposition of EU Directives can undermine the role of the NSA and prevent it from adapting to the new regime of supervision that is encouraged by the European safety regulatory framework. It is poor practice for Member States to fail to recognise errors and to disregard feedback from its NSA.*							
I	Rail	PL	"There is a difference between the SMS recommendation and the internal provisions within the railway undertaking that are supposed to be used to manage the enterprise according to the new rules. The consequence of this situation is that the documentation of SMSs prepared by the railway undertakings emphasises the process-based approach and although it is directly determined by the requirements in annexe three to the directive, in practise, because of it being the internal regulations, a lot of the documents are prepared as they were in the old days of the estate on PKP, when there was just one enterprise dealing with all railway issues. There are not sufficient grounds [within the SMS] for distributing first of all the awareness of various facts and responsibility for them between staff members. Those provisions are not sufficient to promote the rules of management, new rules of management so that all staff are aware of them." In order to improve, many RUs have enlisted the assistance of external SMS managers from academic centres. RUs meet with these organisation regularly and on occasion the NSA participates, where resources allow: "We [the NSA] see it as a really positive initiative because with supervision activities alone, we could not bring about a change in approach." *Our opinion: The NSA is aware that RUs/IMs have been slow to adjust to the SMS-based approach and have demonstrated poor understanding of the requirements in some areas. External, professional support has been used to improve the situation. This may be considered good practice as the NSA acknowledges that the pace of change would have been slower if RUs/IMs had relied on guidance from the NSA (with its limited resources).*					2		
I	Rail	PL	"European legislation, even though it is directly effective, it is an addition to what exists in Polish law and now there is this confusion of what to do because if there is partial overlap but the European legislation introduces some new duties, they may clash with the old duties resulting from the Polish provisions.			-1	-1		-1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			In fact, it's creating confusion on all sides because the undertakings don't know which way to go. It is also a problem for the Railway Transport Office because this office has no power of legislative initiative, of whatever kind. They don't issue regulations, they can't propose too much. If you imagine the European approach where supervision is largely based on audits of safety management systems, anything regarding supervision in the Polish law is based on simple inspections and no flexibility is allowed. So you can see how this creates problems." *Our opinion: This is a further example of how regulatory constraints imposed by national legislation can hinder an NSA's ability to carry out supervision. It also hinders an open market because it creates confusion amongst market players regarding the rules that apply.*							

Table B.9: Examples of complaints procedures

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	GB	The complaints procedure is provided in detail online and should accompany any enforcement action. The procedure outlines the legal process to challenge an enforcement action as well as the process for complaining directly to the safety authority. Complaints are initially directed towards the inspector or their manager. If these routes fail to provide a resolution, the next step offers a choice of contacting the head of the safety authority or raising the matter with the Independent Regulatory Challenge Panel. This consists of independent experts. Information is also provided on how to take up the matter with Ministers or, if unhappy with the decision-making process rather than the conclusion, seek a judicial review. *Our opinion: It is good practice to provide and document a complaints procedure.*				3			
D	OSH	IRL	Website contains complaints procedures – clearly explained in terms of how and when they will be responded to and by whom. *Our opinion: It is good practice to provide and document a complaints procedure.*				2			
D	Aviation	IRL	Provides an online complaints form and contact details for all safety regulation departments. *Our opinion: It is good practice to provide and document a complaints procedure, as well as providing accessible options for initiating a complaint.*				2			
I	Rail	BG	The NSA has a general number for complaints from all parties, which the NSA will always explore and react to. *Our opinion: It is good practice to provide accessible options for initiating a complaint. If the facility is open to the public, it can also form a source of safety-related information on how the market is performing.*			2	3		2	
I	Rail	E	The NSA believes that its action can be judged by the public and so it is important for it to have principles against which it can be judged and a complaints procedure, too. However it has not yet developed these principles or procedures and the issue of accountability is not considered as a first priority: "Right now we don't know how we're going to make this accountability. We don't have our procedures developed. But our principles are not clear… we consider that, first of all, our first step must be about to safety and to exchange information with the sector, and perhaps accountability and complaint procedures could be in a next stage. But we haven't developed any procedures about accountability right now."				-1			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: Care should be taken to adopt all principles to some extent. It is good practice to consider how the NSA will be accountable for its decisions from the outset; it could be argued that the principle of accountability is an intrinsic part of any decision-making process that will be established to enable supervision to deliver its goal of a safer railway.							
I	Rail	D	The German NSA considers that the principle of accountability is met by its formal administrative procedures: "Formally, for us, it's fulfilled by obeying these general review procedures prescribed by the German administrative law. There are these feedback talks each year, which for us also provide a possibility to either complain or to say what, in the view of the ones we supervise, was not okay or should be improved. That's not a formal review or feedback cycle but there is always the possibility to do so. That would then be taken into account and maybe dealt with again the next round to see what has improved. In most of the cases it's done in the second step, when it's taken to the court, and then the decision is taken which doesn't comply with the decision we took before because the first step is really for us to look at the case again, review our decision to see if any new aspects have been brought to the table. In most of the cases, there are no new aspects on the table. We review everything again and then come to the same decision that we had before. So this first step and not too often in the second step can lead to changes." *Our opinion: The formal appeal process – and the NSA's initial, less formal process that invites the RU/IM to present their case regarding any enforcement decision – is stated to meet the principle of accountability in this respect. Separately the NSA expressed a willingness to reform its approaches if a particular case highlighted flaws in its procedures although no example could be offered*				1			
I	Rail	F	"It is a fact that we don't send inspection audit reports with the non-conformities; we send a draft report to the entity that has been inspected or audited with, of course, the non-conformities as decided at our harmonisation meetings. Then they have 15 days legally to give comments on the report. This means that they can give comments on the text of the report. If they were unhappy about some of the wording or what was in the report they can also comment on that. And, perhaps more importantly, if they wish to take issue with the non-conformity, either the description or in fact the grading, that is their official legal opportunity to make representations to us. When it happens… the head of the inspection is the liaison… if he finds something which is not easily answerable because… they hadn't understood something or they need a bit of explanation… it may also mean that				2			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			they have to look again at their Safety Measurement System document which they provided in order to obtain an authorisation and if that happens we have to quote their own documents at them. But if, over and above that sort of anecdotal example, they're still not happy with what's being said, if it's an audit we have an official closure meeting because an inspection obviously tends to be lighter, as it were. But then again on inspection we could have something which they just do not agree with our opinion despite different interpretations of their own documents and the legislation in place. At the audit closure meeting we record their disapproval if we maintain, sometimes they point something out to us and perhaps produce information which we didn't actually have during the inspection audit, in which case we take account of it. And we decide, for example, it could happen that we didn't have all the information and we didn't get it on time despite the fact that we were normally auditing people who were supposed to represent the company. But we would certainly look at information that comes before we publish the final report so we have made adjustments; we're not just going to maintain something if they've provided evidence for us to think otherwise. When the final report is done, we will record, if they're still dissenting, we will record the dissention in the minutes of the closure meeting. Apart from that, there is no specific complaint because the complaint is part of the process of the exchange with them. If they still wish to contest then we are now on to a legal procedure which is provided for in the law. Having written to the EPSF still contesting something and we maintain it and we say no we disagree, bearing in mind that our enforcement is what I said there is no direct financial penalty inflicted by EPSF, their recourse provided for in the law is to go to the Regulator. They will make representations to the Regulator and the Regulator can actually overturn a decision made by EPSF. I'm aware that it has never happened. At the moment, we haven't had a legal objection to a decision made after an audit or a supervision in front of the Rail Regulator in France and I think it's because we take the time to explain to somebody that's put in an initial objection to something that's happened; sometimes it's just a lack of communication or we haven't had all the information that we could have had at the time of the audit or inspection." *Our opinion: The NSA's complaints procedure regarding supervision activity could be considered good*							

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			practice in that it has several steps which demonstrate escalation of the complaint. Initially, the RU/IM is provided with a draft of the findings, on which it can comment. This is followed by a meeting with the NSA to close the supervision activity and finalise the report. This can be an opportunity to make representations that can potentially change the outcome. In addition, the NSA demonstrates further good practice by not using these meetings to prescribe a solution but to help RUs/IMs find the source of the problem themselves. Only when this process fails will the complaint be raised as a legal objection on which the Regulator will have to rule: this has never happened.							

Table B.10: Examples of cooperation from non-rail sectors

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	H	Cooperation agreements between the labour inspectorate and other domestic bodies that may benefit (e.g. mining office). *Our opinion: Ensures that OSH guidance is shared with other public bodies that may benefit or have a stake. This approach is particularly pertinent for Member States where the NSA is not responsible for OSH infringements as it would encourage close cooperation between the safety authorities responsible for rail and OSH. This shares elements of other examples where cooperation extends to sharing general policies and procedures.*		2	2		2		
D	OSH	D	Annual forum: OHS annual forum, run for 6 years and now established in the law. The Occupational Safety Forum brings together the social partners, health insurance, other social security institutions, research institutions and professional associations. All proceedings published online. *Our opinion: The forum involves industry and stakeholders in some key strategic planning, such as the goals of the inspectorate. It is good practice to have a structured approach to stakeholder engagement.*			2		3	2	
D	OSH	A	Regional conference with Slovak and Czech labour inspectorates – the Austrian Inspectorate participates in this two day annual conference with its neighbouring states to "share experiences" and continue "traditionally good relations with these neighbouring states". *Our opinion: Such cooperation arrangements, especially in the form of a regular conference, have considerable value. When countries are so close geographically, the workforce can often cross borders so it is appropriate to cooperate with the authorities in these other states to ensure a common approach so that no matter who is working where, they are still treated the same and have the same rights. It is also a common platform for discussing issues of mutual concern, new regulations etc and arriving at a common approach to these, rather than doing so independently. Whether or not formal cooperation agreements are in place, the platform for dialogue in this example demonstrates a good practice approach.*		2			3		

Table B.11: Examples of cooperation between NSA

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	Cooperation: "I think we saw this as maybe mainland Europe where trains are going across borders and stuff but we don't really have a need for it… because we're very much isolated with our own rules and regulations." Reported that other NSA are not particularly interested in what the GB NSA is doing. "We have no real need to go and foist our systems onto anyone else or we've got slightly… we've got a slightly different legal framework to… other parts of Europe and we have no train flow or no real flow into the wider network and… there's limited need to exchange information. It's not that we don't want to. It's certainly not a policy of we're not going to exchange." *Our opinion: Cooperation does not necessarily require commonality between rail systems. Although the GB network is reported to be isolated in this sense from the rest of Europe, there are still commonalities in the approaches used for SMS, supervision and enforcement that could benefit from cooperation with other NSA.*					-1		
I	Rail	NL	Maintenance covenants exist between this NSA and other NSA to acknowledge the standards of maintenance organisations located inside and outside of the Member State. The benefit is that a domestic RU can have its vehicles maintained by a foreign maintenance company to a standard that the NSA accepts, as long as there is a bilateral agreement that covers the specific maintenance company. Likewise, foreign RUs are able to use Dutch maintenance companies with ease if covered by such an agreement. "It makes it easier to cross borders. I think it's totally what the European Union is about, but it's only between two or three countries, so it's not as big as it should be, because I think Europe wants to have… everything the same, so that if one NSA says it's okay, then it should be okay for all NSA. But in acknowledging each other's maintenance companies I think the European Union is not hard enough, or at least the companies want more. They want more than what the European Union gives, and what our Dutch law gives, so we've made agreements between our neighbouring countries, especially Germany." *Our opinion: it is good practice for NSA to proactively cooperate with other NSA on issues that are of mutual benefit and can ease cross-border operations within the rail market. If European regulation on such matters is considered insufficient, the NSA should make recommendations on how to address this via the Member State. However, it is good practice to seek cooperation agreements to cover any such deficiencies in the interim. Where such agreements prove successful, it is desirable to share these examples with the network of NSA so that others can consider the benefits of adopting similar agreements.*					3		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	NL	There is informal cooperation with bordering Member States on cross-border traffic. This includes occasional telephone calls and even visits; for example, the Dutch NSA went to Germany to assist with the investigation of an incident involving a Dutch railway vehicle. However, the Dutch NSA was proactive in this example and, having heard about the incident on the news, offered to assist the German NSA. "It would make cooperation a lot easier, if you have a contact for each other between member states. If you know someone there, if you have a phone number, if you have an entrance, then people do it but, otherwise, they don't." *Our opinion: Informal cooperation helps to harmonise network operations across borders. In the absence of formal agreements, an informal relationship with key NSA (typically of neighbouring Member States) is good practice. A barrier to this type of cooperation can be simply not having a number or contact to call. It would be good practice for all NSA to assign somebody this role and to publish this role on their website and/or through the NSA Network to facilitate cooperation.*					3		
I	Rail	NL	This NSA had questioned an application for a Part B certificate because of uncertainty about the quality of the Part A assessment. "I think because we talked to the company and then we talked to the ERA and they acknowledged that the EBA [German NSA] didn't do an assessment and they worked with a professional... It's in the Railway Act, the way they do it. So they gave me the text of the Act and I read it and I said that that's not an assessment. We are not even talking about how big or small an assessment should be. There is no assessment. No, that's right. So they agreed on the fact that we were not confident. And we reflect that to the company and they were not happy at all because they felt they were ready in Germany and now it's easy to be ready in the Netherlands, and we said to the company, no, you can't get a B certificate over here. First go to your own NSA and ask an A certificate and make sure that you don't get any of those you have now, make sure that you have your assessment. For the companies in Germany that stay only between the borders of Germany it's no problem [until] they wanted to ride trains in the Netherlands. So they shouldn't have been in our country. Even the EBA didn't want that. They only deemed it okay to ride trains in their own country. So it wasn't meant to be an A certificate." *Our opinion: The European safety regulatory framework asserts that NSA should accept the validity of a Part A certificate when assessing an application for a Part B certificate. This example indicates that assessment procedures within NSA can vary to the extent that some RUs may not be operating under a Part A certificate*					2		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			but rather under national safety rules established by the Member State for domestic services only. Such practices are not good practice for developing a harmonised network, particularly if RUs are confused about the scope of their safety certificate. It may be prudent to check Part A validity if the Part B applicant is from a Member State with national safety rules that permit operations within their borders but not outside. Improved cooperation can improve knowledge of these different working practices.							
I	Rail	DK	The NSA explained that cooperation with countries can be complex: "We are aware that the CSM for conformity assessment and supervision addresses the fact… that there should be agreements with other NSA having A and B certificates. We have not established any written agreements yet but… it's quite a big job actually so it sounds easy but it's not. I think that this is one of the items that has not been thought through in the regulations. It's very easy to say NSA should cooperate but on what and what are the conditions for cooperation? What is the legal basis? And that's not visible for the time being so we have to dig into it and find out what is actually the conditions for this cooperation." However, in spite of these complications, the NSA has made steps to cooperate with other Nordic NSA: "We had just started some joint meetings with Norway and Sweden on… all types of matters. We have made verbal agreements with the Swedish NSA that if we issue a B certificate to a company that has an A certificate in Sweden, we will contact them and also we will inform them if there is anything that we find not to be sufficient. But actually this is an item that should not be made on a bilateral basis… It should be the same way all over Europe and not solely an agreement between Denmark and Sweden. There should be common ways of doing this set out actually by the regulation which is lacking for the time being." *Our opinion: In the absence of more detailed regulation on cooperation, it is good practice for NSA to proactively explore ways of working together to cover issues of common concern. Experience of cooperating under verbal agreements may clarify the grounds for a more formal agreement in the future.*					2		
I	Rail	A	The Austrian NSA has established cooperation links with several adjacent Member States: "There is… a formal cooperation between Germany, Switzerland, Austria… concerning rolling stock authorisations which we compare and try [to introduce] cross acceptance. Concerning the safety certificate… we have already experience with [informal] cooperation with Hungary during the safety certification process and which was quite positive I think on both sides, learning and answering questions. The application was for a part B certificate in Austria and we had some open questions concerning part A and the amount of the issued part A, and this was a question from our direction to Hungary. And on the other hand, for instance,					2		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Hungary asked us something about the insurance provisions by an Austrian railway undertaking which applied for a part B in Hungary. I think both sides were quite satisfied with the outcome. Germany, for instance, is another member state we already had contact with, clarifying questions concerning a safety certification process… it will intensify in the future when we now have, for instance, applicants from Poland. I think it [cooperation] will develop [through the process of new certifications] and I think it also would be a possibility [for] ERA… to make… a template, a general paper for all this cooperation." *Our opinion: This NSA is cooperating with other NSA during the process of certification. Whilst the safety regulatory framework requires NSA to accept the validity of a Part A certificate, the principle of cooperation encourages an exchange of information between NSA that are sharing the supervision of a particular RU via Part A and Part B certificates. The positive response reported by this NSA suggests that this approach will meet with acceptance. However, the NSA advocates ERA intervention to formalise the process of cooperation.*							
I	Rail	BG	The NSA has no formal cooperation agreements but it does have experience of cooperation on an informal level with: • The Romanian NSA. • The Austrian NSA – this was during assessment of a Part B certificate for an Austrian RU, when the Bulgarian NSA asked for clarification on some items. The other NSA was cooperative. On this basis, the Bulgarian NSA sees no need for formal cooperation agreements. However, the NSA was keen for there to be cooperation on the exchange of best practices between NSA, "because it's important how, in case of similar issues, how does the different NSA approach is going to finding the solution of this problem". *Our opinion: It is good practice to establish even informal cooperation with other NSA.*					1		
I	Rail	S	The NSA cooperates with other NSA when assessing Part B applications from foreign companies: "If I get an application from a company from Norway who wants a certification Part B in Sweden I… send a letter to my Norway colleagues [asking] is [there] something I should be aware about? And for information for them that this company is applying for certification in Sweden which makes them in Norway think about should they check something in the management system or should be aware about that company is working abroad."					3		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			If the Swedish NSA issues a Norwegian applicant with a letter detailing any non-compliances or weaknesses in its SMS, it will send a copy to the Norwegian NSA for their information. It will draw attention to any lack of awareness of Swedish rules or systems as this would point to a failing in the part A SMS if the company is not able to establish the rules that apply to operations. In addition, the three countries of Sweden, Norway and Denmark are open to auditing together, particularly as a way of overcoming the sometimes unclear links between the SMS that has been audited for part A and the SMS that will be used when applying for a part B abroad. The NSA is also opening discussions with other NSA (e.g. Finland, Germany, Netherlands) about applicants for part B certificates from these countries. However, this has highlighted that, "we don't have a good communication system between different NSA". It had approached one NSA about an applicant but had not received a response and so suggested that all NSA should have a dedicated point of contact for cooperation and such enquiries from other NSA (e.g. a unique email address or telephone number). *Our opinion: The three Nordic countries of Norway, Sweden and Denmark have established a fluid and apparently effective chain of communication and cooperation. Although in its infancy, the goal of joint auditing could be considered good practice. Their current system of sharing information about foreign part B applications shows a mature and safety-conscious attitude. It is unfortunate that attempts to expand this cooperation to include other NSA have proven more difficult.*							

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	S	The Swedish NSA has recognised that there is a potential 'time bomb' for renewals of certificates that could affect RUs/IMs right to operate: "We see when we are renewing certifications, especially Part A, and the company has several partnerships in other countries. The moment you change your Part A, you have to change your Part B in the other countries [in which you operate] because the Part B is responding to the certificate Part A… If you're very, very late in your issuing [of the Part A renewal] perhaps the other countries are not able to manage the new Part B in the short time. If I can explain, you cannot… If a company have a Part A valid for five years to 2015 and then this year they apply for certification Part B in Sweden we only can issue that Part B for three years to 2015 because you can never… have a Part B valid a longer time than the Part A. And suddenly, some moment in 2015 the company's Part A, Part B in another country, say Part B in Sweden is not valid any longer and everybody has to renew them. Sweden can't renew their Part B before they have renewed their Part A. Suddenly you can be in a very short time which could make problems for the company and this is the kind of issue that we are discussing between our countries, Sweden, Norway and Denmark, and now with companies having a new certificate Part A we are starting with this now so they know where in the line we are just now so they can plan their own work." *Our opinion: the NSA has recognised that the timing of renewals for Part A and Part B certificates could be critical for continued market access. Increased cooperation between NSA may be effective in establishing a timetable for renewals that allows continuous market access and does not create any potential disruptions or unexpected peaks in the workload of an NSA.*					1		1

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	CZ	The NSA described how supervision of foreign RUs/IMs operating under Part B was complicated by language differences and having most documents located in a different Member State. "I think we have to go to the organisation, where it is already located, and say in this event, this driver, this loco, and now show me at first the qualification of the driver, the documents about, I think, about training of this driver, documentation about maintenance of this vehicle, documentation I think about how do you check the following permitted speed. But all these documents are not on the train, but they are in the company. And we can't imagine how to go further." Specifically, the NSA has received reports of a Polish RU breaking speed limits in the Czech Republic. "We received information that they don't follow the speed limit. And there was problem, how we could check this, how to get this information? So it means to go to the headquarter of this company, which is in Warsaw… according to Czech law, they are obliged to speak with us in Czech language, but if we go to Warsaw for inspection it's problem of, we're out of Czech Republic. I think, legal process, in different language, not mother tongues, it's so very complicated. Because of translation, all the legal texts is very difficult." *Our opinion: The NSA is uncertain of how to cooperate with other NSA in order to carry out effective supervision. This may be a product of not assessing using an SMS-based approach; this approach would require applicants to provide evidence that they were following the necessary rules and had a system to ensure this. The Czech NSA would then be entitled to request access to evidence of any function of the SMS.*					-1		
I	Rail	CZ	The NSA is arranging to cooperate with the Slovakian NSA: "We agreed that we will arrange some international supervision. We don't have regular meetings, but we plan to have… once in, twice a year, or three times a year... to discuss the legal problem of EU legislation. Which is, I think, the main problem, common understanding of legislation and stage of transposition." Two reasons were given for selecting Slovakia for a cooperation arrangement: the first was the common language; the second was that the majority of cross-border operations were with Slovakia (most of the foreign operators in the Czech Republic have Part A certificates issued by Slovakia). The NSA has no information on which Czech companies operate abroad as they receive no feedback on Part					1		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			B certificates applied for in other Member States. *Our opinion: It is good practice to cooperate with other NSA and the basis for cooperation (based on cross-border operations) is sound.*							
I	Rail	PL	The Polish NSA has a general agreement to cooperate with the German NSA, but not on issues of supervision. It also has no foreign RUs operating within Poland – all are registered as Polish companies. Polish RUs are operating in the Czech Republic, Slovakia and Germany but no cooperation agreements have followed because the NSA has not been approached officially for information. The NSA has concerns about cooperation with other NSA: • "What's… going to be critical in such cooperation is the ability or inability to communicate; those are the problems that are quite likely to make it difficult." • "We assume that there may be problems resulting from the discrepancies in how we define supervision and how it's done elsewhere." • "Today, if we think about our supervision of any enterprise abroad, it would be impossible because of insufficient funds." The NSA would appreciate setting 'general rules' for cooperation between NSA at a European level. *Our opinion: The NSA has expressed a positive approach to cooperation but has concerns about differences in language and supervision processes, as well as funding for such activity. Setting rules for cooperation at a European level may provide a basis for the NSA to secure funding should it be necessary to cooperate and such rules may clarify the grounds for cooperation.*					1		
I	Rail	E	When considering Part B applications from foreign undertakings, the Spanish NSA will, "first of all… analyse documents [then] we have to make several interviews to inform RUs of other member states that they have to adapt their way of operating to Spanish infrastructure." The NSA has been working with the NSA of Portugal and France: "They have approached us and we had several meetings. We have exchanged national regulatory framework information and we have informed them of our specific infrastructure, our specific national regulations to make them easier to operate in our country… it's been easier than we thought it was going to					1		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			be." *Our opinion: the NSA has begun cooperation with neighbouring NSA that have RUs/IMs wishing to operate in Spain. The focus has been ensuring that there is an understanding of the national rules in Spain and the infrastructure (Spain has a dual gauge infrastructure). The cooperation has been positive.*							
I	Rail	D	"We don't have cooperation agreements with each neighbouring NSA or member state. We have some with Poland and with the Netherlands and Switzerland, for some aspects. We do joint supervision activities with our neighbouring countries but that's something to be developed or intensified in the future." The NSA explained why the current cooperation agreements emerged: "It was mostly market-driven, I would say. These are the countries where we have... a high volume of cross-border traffic. There was also a high interest from the marketplace, from railway undertakings, that, for example, in the past authorisations of train drivers, authorisations of rolling stock were mutually accepted. So, we had strong and intense discussions with our neighbouring NSA and resulting from that intense cooperation on these issues. There was also an exchange on items related to supervision and then from that this was developed towards joint supervision activities because they said we share information, we have approximately the same knowledge, why don't we make a joint supervision team and make that together. That in the end helped and we've been sharing information." The NSA elaborated on the joint supervision activities: "[There is] the principle of territoriality. So, if we join a Dutch supervision, for example, in the Netherlands, they would be the ones formally organising it, be responsible for it and we would be visitors or... I don't even know if we could say co-auditors. We would discuss the topics with the NSA colleagues in advance. We would then be visitors. We could ask questions. We could use the findings or the information we gather but the one deciding in the end would be the Dutch colleagues because it's on their territory and it would be their supervision activity. That's the way we would deal with it." For the future, the NSA believes cooperation will and should grow: "We think that, with the coming CSM on supervision, there is more obligation put on the NSA to develop their cooperation. That's something we will do. Formal agreements with every neighbouring NSA or regular yearly meetings to have an exchange on supervision topics and on supervision of the cross-border of the					3		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			respective countries. In any way, it will develop and intensify. The share of information currently is possible on a bilateral basis but it's also possible via the safety information systems of ERADIS, which also have to develop and evolve and things. There is also cooperation on area level and area networks where topics of a general interest can be discussed or brought to the attention of everyone. That's something where there is something at the moment but that has to be strengthened in the future." *Our opinion: The NSA has cooperated selectively on the issues that are priorities for smoothing existing cross-border operations. It is potentially good practice that it is using this cooperation to cross-audit in conjunction with another NSA to share practices as well as information about RUs/IMs. The NSA believes that the forthcoming changes to the safety regulatory framework will drive greater cooperation. It would be desirable for NSA to cooperate in a way that not only deals with issues of current relevance to cross-border operations but also smoothes the path for future cross-border operations to begin. Recognising what barriers may exist to prevent cross-border running and then using cooperation to overcome these issues is as important as cooperating to overcome issues that emerge after cross-border operations are attempted.*							
I	Rail	F	The NSA described its recent cooperation activities: "From a supervision point of view that's just beginning, actually, because there is a joint inspection taking place with our Swiss colleagues; that's actual taking part in an inspection, as it were, and I think it's relatively new for us to do that. But we have had non-inspection exchanges with our opposite numbers in different NSA in that we had an inspector from the British NSA, ORR, he spent two weeks with us but that was a sort of exchange thing where we sent somebody from EPSF who spent two weeks with the ORR. And that was looking at different methods and there has been quite a lot of co-operation with ORR, the Swiss and also the Belgium National Safety Authority. It's not the same as going down on the ground and actually taking part in joint inspections; that's only just beginning. I think the different entities that came to see how we worked were quite impressed by the arrangements we have for the database. It was also interesting for us to see what the definition of inspection is with other National Safety Authorities and it may be that we decide, perhaps in the future, to do more inspections and audits but it's a subject which is still being looked at." *Our opinion: The joint inspections with other NSA can be considered good practice. The French NSA is using cooperation to share knowledge of procedures and processes and some valuable exchanges appear to be taking place – for example, other NSA learning from the French experience of creating a database for its*					3		

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			incidents and the French NSA learning that more inspections may be useful in its future supervision plans. These exchanges exceed the safety-related information that is referred to by the principle of cooperation.							
I	Rail	GB	"I think we saw [cooperation] as maybe mainland Europe where trains are going across borders and stuff but we don't really have a need for it I wouldn't have thought because we're very much isolated with our own rules and regulations that we follow… We would be in a position of quite gladly exchanging information with [other NSA] if they wanted it. I think we see that at the moment we have no real need to go and foist our systems onto anyone else… we've got a slightly different legal framework to other parts of Europe and we have no train flow or no real flow into the wider network… so… there's limited need to exchange information. It's not that we don't want to. It's certainly not a policy of we're not going to exchange. But our information is on the website anyway so they could always get that." *Our opinion: It is good practice to cooperate with other NSA to share procedures and practices as well as safety-related information regarding common rail systems. This NSA describes a positive approach to cooperation but is not proactive in exchanging information; as with most NSA communication, it is delivered passively via a website. The NSA also does not recognise the value of exchanging information about its policies and procedures with other NSA, citing differences in rail systems.*					-1		

Table B.12: Staff skills and competencies required for supervision

NSA	Required skill/competence
Great Britain	The key competencies set out in our Inspector competency framework are: Regulatory Skills - leadership, creating and maintaining effective working relationships, managing people and coordinating teams, planning, organising, managing projects and resources, communication, analysing and using information to make decisions, developing and applying skills and knowledge, specific skills to enforce health and safety law, inspect and investigate, advise and influence, plan organise and prioritise, assess risks, work effectively with business, work effectively with partners and stakeholders. Inspections - undertake effective assessments of stakeholders ability, use knowledge effectively, personal development innovation and learning, IT literacy and numeracy; Knowledge - occupational health, occupational safety, modern rail transport systems including interoperability, legal framework for safety regulation, level crossings, permanent way, structures, stations, light maintenance depots (LMDs) and freight terminals, signalling, railway telecommunications, rolling stock and vehicles, electrification traction and power, general railway operations, operation of train movement control, management systems risk assessments and human factors, heritage railway metro and tramways and personal safety. Each category has a range of topics against which inspectors are assessed to determine whether they meet the competency or further development is required.
Sweden	Higher education /university or other similar education and good knowledge of railway. Exam from quality auditor course (ISO 9001) Good knowledge of legislation and regulations Good at writing and expressing yourself in different situations
Estonia	Personal qualities must be honesty, loyalty, technical (higher) education, independence
Lithuania	Staff are expected to have higher education and experience in railway transport area.
Romania	Railway experience Synthesis capacity

NSA	Required skill/competence
	Good knowledge of legislation/ regulations/ rules Correctness Seriousness
Germany	University or university of applied science degree in the relevant domain or comparable experience Practical experience Analytical skills Management system knowledge Personal skills like negotiating, self-confident manner, sense of responsibility, working autonomously and in teams
Denmark	Our staff are expected to have completed lead auditor training and to have experience with, and good knowledge of management systems.
Spain	Knowledge of Safety Management Systems Experienced in audits Experienced in the assessment of safety certificates and authorisations Open-minded Ethical
Latvia	Knowledge in particular railway field (infrastructure, rolling stock, management of train movement) Knowledge of legislation generally at state level and particularly in railway sector. Experience in profession (at least 5 years) and experience in state administration
Poland	Knowledge of safety regulatory framework (both national and EU), technical knowledge related to infrastructure, rolling stock and maintenance, knowledge about the inspection regime that is currently in force (the old approach regime based on national ordinance sets precise requirements for the inspection process, its documentation and timeframes. The regulation is not in line with the new approach set by the CSM for conformity assessment and CSM for supervision. It's not process oriented and is linked more with conducting audits than planning and documenting the

NSA	Required skill/competence
	supervisory activities). Besides this, skills linked with different supervisory techniques, including audits are expected. We hope that in the nearest future more emphasis will be put on the skills and competencies related to audits rather than inspections. Right now the audit competences are not common in the NSA.
Bulgaria	Qualification for performance of safety-related activities in the field of railway transport Successfully passed examination for knowledge of the national safety rules
Austria	The staff are expected to have knowledge of the general administrative procedures; the relating laws, regulations and rules, as well as skills in negotiating, knowledge and practical experience in the relevant fields.
Portugal	Good general knowledge about railway industry More than three years of experience in railways technology - infrastructure and/or rolling stock Good knowledge about national and European legislation applicable to railways Training on audit techniques
Czech Republic	Working experiences Knowledge of legislation Knowledge of NSA internal rules
Netherlands	Knowledge of rail safety. Ability to express oneself verbally and written
Channel Tunnel	For the GB half of the Channel Tunnel: qualified railway inspectors are assessed for necessary and relevant skills by the ORR (see GB skills). For the French half, qualified inspectors are assessed by EPSF (railways) or relevant ministries (rescue, safety at work, ...)
Hungary	Working knowledge of the railway system. Working knowledge of the EU and national legislation.
Norway	Experienced auditors. Higher education at masters level.
Ireland	Railway experience or high hazard experience. Audit experience desirable but not essential. Clearly skills such as 'ethical', 'thorough', 'organised' etc

NSA	Required skill/competence
	are expected.
France	The criteria that EPSF has chosen to implement for inspectors are: 1. Experience required: At least 5 years of specialty rail system, this period may be reduced or eliminated if the person has received education level of at least + 3 pan and preparatory courses adapted to the job. 2. The inspectors must be empowered. The initial conditions of capacity are: - At least 5 days of audit training - At least two days of safety training of staff vis-à-vis risk rail - Participation in at least: 2 complete controls, under the direction and with the advice of a confirmed Inspector; and 2 controls with the advice of a qualified inspector, not necessarily present during the inspection. The authorisation is valid for 3 years under certain conditions and is renewable.
Finland	Good knowledge on railways in practice and the legislation in regard railways, auditing skills and experience.
Italy	1) Technical and specific skills about on the processes to be evaluated. 2) Specific skills as auditor. 3) Knowledge about the legislative framework to be applied.

Table B.13: Planning training for supervision staff – all findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	Technical training: "I think already we're seeing some improvement in the ability to deliver specific training courses to those people that need training." Training needs identified by team managers and also led by programme of work (i.e. any core areas that the NSA will be targeting in a certain period). Technical training is divided between "run of the mill things" on basic underlying principles of railway operations and more specific training. The NSA is keen for its staff to receive technical training so that they all operate at a 'uniform' standard. This is particularly important when technical issues lead to enforcement action; staff need to be aware of how severe a technical fault may be as this will influence their enforcement decision. *Our opinion: Another example of targeted training. The NSA is training its staff in technical issues so that they can deliver supervision for any current themes in the supervision plan. It is also essential that staff have current technical knowledge so that they can enforce consistently and proportionately by recognising the risks presented by technical breaches.*	2	2				2	
I	Rail	GB	Designing in-house courses for inspectors, run by inspectors. *Our opinion: This is good practice as senior staff are often best placed to identify training needs and then creating training that fills gaps in skills and competencies. It would be better practice if such training was shared more widely, where appropriate. For example, it could be offered to other NSA with a similar need. This would be subject to similar practices being used by staff (although cross-NSA training in itself is a way of harmonising practices).*						2	
I	Rail	GB	Share core training courses with OHS where appropriate (e.g. to train to be an inspector). *Our opinion: This is an efficient approach to training new staff by sharing training with other organisations that have a similar function (e.g. core inspection and supervision skills).*		3					3
D	Aviation	LV	Online summary of CAA training programme which covers safety management, safety regulation, technical instructions for use, and SMS certification and supervision. *Our opinion: provides assurance to the market that inspectors have the required competencies.*			1				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	B	Action Plan specifies that the BCAA will develop safety training courses and safety promotion for employees (e.g. through initial and recurrent training and safety seminars). *Our opinion: it is good practice for strategic planning to include competence development for staff.*			1			1	
I	Rail	NL	There are some efficiencies and benefits for competence development by having the NSA integrated with other government departments for supervision and enforcement. "Some courses can be given to the whole inspectorate, especially the enforcement ones, of course." *Our opinion: Competence development and management can benefit from NSA inspectors working within a government division that includes other inspectorates. There are some competences that are used by all inspectors and initial, refresher and update training can be delivered to inspectors across several domains, including rail. It is good practice to have commonalities in the approach used by inspectors as a way of achieving consistency as well as delivering efficiency and cost savings.*		3					3
I	Rail	DK	The main IM runs a technical training course on operations and signalling that is attended by new staff from the NSA. *Our opinion: It is good practice to seek efficiencies in training and to use external industry courses for relevant technical training.*		2					3
I	Rail	S	The new NSA structure, where supervision of rail, road, air and sea traffic is merged together is helping to deliver a consistent and efficient training programme for new starters: "The total transportation agency is trying to make all decisions consistently and we have the same way of thinking about supervision. So therefore they have started, last year, with this training course and I think it's three or four different steps where you are a new inspector coming, or new officer coming there to learn about authorities and you have to learn about regulations. You have to learn about behaviour at audits. You have to learn about interview techniques. You have to learn about writing down and almost conducting audits and you have to train and discuss with other colleagues in different traffic modes how they see and how they discuss similar items. Then you have also training in quality officer like in ISO 9001 to make quality audits so there is also education in that, in quality systems and making system audits and so on."		3					3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: the NSA has found efficiencies by combining training for common activities of an inspectorate, irrespective of traffic mode. This is good practice in that it not only manages resources more effectively but it also provides consistency across the entire department.							
I	Rail	PL	"There's a proposal to train the employees of the office in conducting audits but there's no reason, there's no grounds for deciding to spend money on that because the Polish legislation does not require them to conduct audits." *Our opinion: This NSA has proposals to train its staff to follow the SMS-based approach but is unable to initiate these proposals due to incompatible national legislation.*				-1			-1
I	Rail	E	There is no formal training programme. The NSA has experienced staff from its national RU in the workforce: "We don't have training because we are learning day-by-day because a lot of things are new for us. So related to RUs we have people from Renfe [Spanish RU] with more than 30 years… background, so they are monitoring and teaching to younger NSA staff. From this we have people with more than 35 years of background and they are making the same activity with people of the NSA that are younger and this is the way of dividing our work areas on the NSA." *Our opinion: the NSA is reliant on a system of mentoring where more experienced staff are passing down experience to other staff. However, there appears to be no clear training process for ensuring that staff have fundamental audit and inspection skills, or that there is a consistent base of experience, knowledge, and practice for all staff.*		-1					

Table B.14: Delivering training to supervision staff – all findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	DK	"It's very urgent that we distinguish between advising and guidance. I'm quite confident that we will only guide during supervision due to the fact that all supervisors are trained auditors. They are not born in the railway industry. Actually… 99% of the experience of the railways they have from the agency. But what is a must is that they have to be examined legal auditors to perform audits or supervisions. So I'm quite confident that we can have audits guided and giving added value to companies without advising and that's… a key issue for our way of supervising big companies." *Our opinion: This NSA demonstrates good practice by showing an awareness of the limitations of its role. Its staff have training that the NSA believes contributes to its neutrality when supervising, and is wholly appropriate to the SMS-based approach.*			2	3		3	
I	Rail	DK	A new member of the supervision team will "start as an observer, go into being a co-auditor and then being a lead auditor under supervision. The person in question has also to feel confident doing it". Judgement is used to decide on the time scale for this process but the typical duration is four months. *Our opinion: Guided development of new staff demonstrates good practice.*				1			
I	Rail	A	The NSA uses a similar approach to training as other NSA, which is to have experienced staff accompany new starters when carrying out supervision activities. However, it re-engages this approach after the new starter has begun supervising alone (usually after about one year) to check on progress: "From time to time there is a possibility that a superior or a more experienced expert accompanies again and see how this has developed and if there are improvements." *Our opinion: The NSA is showing a mature approach to competence management by using experienced staff to guide new staff and then monitor their progress as they begin to carry out supervision alone.*				2			
I	Rail	BG	Bulgarian law requires all new administrative staff to undergo a probationary period of at least a year so new inspectors are not permitted to supervise alone until at least a year has passed. The decision is then made by senior staff based on experience of working with the new starter. *Our opinion: Guided development of new staff demonstrates good practice.*				1			
I	Rail	S	As with other NSA, new inspectors are accompanied for 6–12 months before they are considered capable of acting as a lead auditor. The assessment of their abilities as lead auditor is usually carried out by another experienced colleague, who will shadow them in the role of lead auditor for two or three audits and then discuss their observations in a three-way meeting with the new inspector and their line manager.				2			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: A collaborative approach to deciding when a new starter has reached the required level of maturity is an example of further good practice.							
I	Rail	GB	"I've a three-year training regime where they would go from being treated as a new inspector through to a full inspector and they will have a series of training courses and that will be around concepts such as how to communicate effectively with people through to how to understand the law, how to apply the law properly, how do we investigate properly, how to get people whilst you're doing an investigation, how to put people at ease when you need to put people at ease, and how to get good witness statements through to, you know, being able to conduct face interviews, how to be quite severe in your approach if you need to and they will go on a variety of different technical training courses about rolling stock, power systems, track, structures, signalling. They will have pretty close supervision while they're out on site so they won't just be let loose into network rail. They will be eased in probably over the best part of a year, 18 months so that they feel comfortable, confident and capable of dealing with the types of individuals that they'll be interacting with. I can't give you an exact timeframe because it will depend how quickly the person picks up those skills and how capable they are." *Our opinion: Close monitoring of new starters and assessing maturity based on skill development demonstrates good practice.*				2			
I	Rail	PL	When trying to introduce measures to supervise the SMSs of RUs/IMs, the NSA "met with resistance of inspectors themselves, for whom it was quite a new thing. They simply followed the old approach, the existing provisions" "From 2011… we also control whether the undertakings operate according to the roles consistent with the improved SMS systems. However, for the time being, it is still a superficial sort of control." *Our opinion: NSA that meet with resistance from staff to changes in procedures should consider whether their system of competence management for staff could be improved to ensure that changes are better understood and implemented by inspectors. It is not good practice to be able to introduce only superficial controls.*	-1	-1		-1		-1	-1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	D	"For the ones which do assessments and supervision, they all go through a kind of quality management course from an external provider to give them the necessary input or knowledge on management systems/processes/procedures, how to assess them and so on. That's something not anyone has to have but anyone who does supervision and assessment certification, they get such a course which is an external provider doing this. Well, there might be on-the-job training where, let's say, new colleagues taking over that responsibility...[for mentoring]… Where they're accompanied by experienced colleagues for a period of time in order to learn what they do, how they do it. The usual period is one or two months, so four to eight weeks but there is no fixed period. That is decided in each individual case. Then there are, let's say, internal workshops or training by internal staff where different topics are dealt with by internal experts which are presented and discussed with other colleagues. And there can also be other training by external providers for certain topics/aspects. " *Our opinion: In common with other NSA, the German NSA mentors its staff, although the mentoring period is notably shorter when compared with other NSA. This is supplemented by internal and external training, which would suggest that the NSA makes use of internal skills where possible and turns to external providers for other topics.*				1			

Table B.15: Assessing training provisions – all findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	Annual review of investigation statistics: The NSA explores the performance distribution of inspectors based on criteria such as speed of investigation (typically 11 months, so when it is longer, this is noted), and consistency of decision-making as shown by individual case reports. Focus is on inspectors who are performing least well – the NSA's aim is to bring these inspectors up to the standards of the majority. *Our opinion: NSA should establish some framework for competence that helps them strive for excellence. In this example, the focus on the length of investigations and the decision-making process is likely to deliver an improved service to the market. Aiming to deliver well-reasoned investigations in as short a time as possible demonstrates good stakeholder management: market players will not want to wait too long for a decision, and will appreciate a decision that clearly follows the decision-making process published by the NSA and leaves little scope for alternative interpretations. Other criteria for competence management may be appropriate.*	3	3					3
I	Rail	GB	Staff assessments: "At the end of three years [training] they will be formally assessed by a panel… quizzed on basically any activity of being an inspector and they'll be asked to produce some of their reports and work from that period. They'll be asked to prepare at pretty short notice… two technical presentations. They're put through a relatively robust regime of assessment." Training is also now evaluated by the staff involved rather by HR as it was previously, as this leads to more informed decisions on the value of training and how it can be improved further. *Our opinion: Written examinations are one way of testing staff competence; assessment by presentation of technical material and review of work is another. It is desirable to embed competence assessments in the daily activities of NSA staff and the examples described here show good practice in this area.*	3	3		3			3
D07	OSH	A	In the first two years of service, all employees take part in training courses in the fields of law, technology, medicine and communications work and then take a final exam. *Our opinion: Structured training provision during first 2 years of service with an examination to test competence and understanding. Examinations/formal assessments of staff knowledge and experience may be an appropriate way to ensure staff meet necessary standards.*	2	2		2			2
I	Rail	GB	Online competence management system: "Every year all our inspectors are made to do a competency assessment and that's based on their opinion as to what their skills are, and their managers' opinion as to what their skills and knowledge are, and it's a combination of [these]. It's split into two and it's: regulatory skills, i.e., how to be an inspector; and your technical knowledge of the railway and	3	3		3			3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			occupational health. You get an assessment at the end. You'll know roughly what work you're going to be doing next year, you'll know what your skills are; you should be able to have that conversation with your manager, identify the gaps and then say right, okay, I don't know about lifting with road rail vehicles. Is there a course running? Oh, yes, so it happens, yes. Can I go on that? Or actually do I need to do some guiding reading, or do I need to do some joint visits with inspectors who are suitably experienced?" *Our opinion: It is good practice to have a consistent approach to competence management for inspectors and other staff involved in supervision and enforcement. Deficits in competence follow through to corrective activities such as targeted training.*							
I	Rail	DK	In accordance with line managers, staff agree to regular training updates for continued professional development. *Our opinion: NSA should establish a framework for competence that helps them strive for excellence and that involves staff in making decisions.*	2	2		2			2

Table B.16: Legal training for supervision staff – all findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	"We might try and influence things through the legal training that we do… where we put up an example of an issue and then asked the inspectors what they would have come up at the end of that, what action they would have taken." *Our opinion: Training to achieve proportionality and consistency by using case study examples. This exercise helps staff to understand how and why previous enforcement decisions were made. Use of examples where there was a legal outcome (e.g. a prosecution) helps to develop an understanding of the circumstances in which this approach is suitable.*	3	3					
I	Rail	GB	Annual Legal Update Training Course: refresh various rules on inspector duties and powers, taking into account any new changes. *Our opinion: It is good practice to refresh staff knowledge of the regulatory framework, particularly as it develops.*		2		2			
I	Rail	DK	"We are very aware of new regulations but this is one of the hot points actually; that is how do we transfer the knowledge of the regulations to the staff doing supervision on a level that is sufficient? We are working on that. We have not found a way of elaborating the way of doing it. It's pretty hard because it should not be needed that they know every legal rule in detail but they have to be aware of what to supervise. So we are actually, we have made a new procedure for making the new regulations or rules. That is, in the very beginning of making this new regulation, the legal adviser will have to team up with people that will have an interest in the regulation when it's done and looking into, is there anything in this regulation that will need supervision afterwards? So the supervision is actually incorporated upfront and having an alert that, something will tell you that needs to be supervised." *Our opinion: An example of a good practice approach to responding to new regulations. A far more unified approach can be fostered if staff are guided on the relevance of new regulations rather than being expected to read, interpret and implement changes themselves.*		2		2			

Table B.17: Identifying who is responsible for risk control within an RU/IM

NSA	Aware of who is responsible for risk?	Method of identifying persons responsible
Great Britain	Yes, at all RUs/IMs	SMS and regular contact with RU/IM.
Sweden	Yes, at all RUs/IMs	New RU/ IM notifies information about responsible persons in their application. RU/IM are also responsible to report changes of responsible persons to NSA.
Estonia	Yes, at all RUs/IMs	Via Safety Management System
Lithuania	Yes, at most RUs/IMs	RU/IM inform NSA who are responsible for risk at each RU/IM.
Romania	Yes, at all RUs/IMs	The individuals who are responsible for risk at each RU/IM are designated in the safety certification/authorisation dossiers.
Germany	Yes, at most RUs/IMs	Allocation of responsibilities is shown in the SMS. NSA is in regular contact with RU / IMs.
Denmark	Yes, at most RUs/IMs	Yes
Spain	Yes, at most RUs/IMs	All is centralized by means of contacting the Safety Manager from each RU/IM.
Latvia	Yes, at most RUs/IMs	According to the documents for safety certification.
Poland	Yes, at most RUs/IMs	-
Bulgaria	Yes, at all RUs/IMs	We identify them through contacts with representatives of the above-mentioned structures of the RUS/IM.
Austria	Yes, at all RUs/IMs	The NSA is aware of all individuals responsible for the RU/IM due to the need of notifying a 'Betriebsleiter'/'operating manager', which also has to be present in the organisation chart and is responsible for risks.
Portugal	Yes, at some RUs/IMs	By the direct contact with the safety manager and the description on the SMS Manual
Czech Republic	Yes, at most RUs/IMs	It is a part of organisational structure.

NSA	Aware of who is responsible for risk?	Method of identifying persons responsible
Netherlands	Yes, at all RUs/IMs	Relationship by interaction during issuing and during follow up of measures taken by RUs/IMs.
Channel Tunnel	Yes, at all RUs/IMs	Communication: IGC / CTSA regular meetings; telephone conversations; e-mail etc.
Hungary	Yes, at all RUs/IMs	During the authorization process.
Norway	Yes, at most RUs/IMs	By experience.
Ireland	Yes, at most RUs/IMs	They should be identified in their SMS Safety Case.
France	Yes, at all RUs/IMs	In general, the EPSF contacts the Director General of the RU or IM, depending on the topic that identifies a contact person within the company.
Finland	Yes, at some RUs/IMs	Through SMS
Italy	Yes, at all RUs/IMs	Through the SMS and the Organization provided by the RU/IM

Table B.18: Examples of planning supervision

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	Supervision based on assessment/reassessment process: "What we do in our assessments, every five years or a new assessment is to say what's the capability of this organisation to deliver… you've got nothing to look at other than their procedures so all you can say is are they capable of delivering – yes or no, and then over the following five years you go out and test that that capability is being delivered. Now then when you get to the end of the five-year cycle you've got something on which to base your reassessment and you can say, well, okay, we've looked at driver management every year for the last five years, we're confident that it works well; we're not going to look at that as part of the reassessment; we're going to look at these areas of weakness over the year far more, so you can again start to target your risk." *Our opinion: It is good practice to plan supervision during the validity of a safety certificate or authorisation on the findings from the assessment or reassessment process. This example suggests looking at the capability of the organisation to operate safely; supervision can be planned to cover aspects where there is doubt about that capability. However, at the time of reassessment, if an organisation has shown capability in an area that was a target for supervision, supervision in that area may be scaled back accordingly (although it should never be ignored completely). NSA can target their resources efficiently by using such an approach.* *However, before making a change to a supervision plan for an RU/IM, the NSA should challenge the RU/IM to show how they have improved the SMS for that activity. Supervision and assessment/reassessment should always be linked by the need to demonstrate continuous improvement. NSA should be cautious that the process of supervision of a particular activity may have contributed to improvements and these improvements may not continue if the supervision is reduced in that area (hence the importance of identifying fundamental change on the relevant parts of the SMS).*						2	2
D	OSH	DK	Risk-based supervision model – since 2005, WEA has inspected all Danish companies. It has now adopted a risk-based approach. Selection for inspection is based on the number of FTEs: all companies with at least 2 FTEs will be visited by 2020; half with 1-2 FTEs will be visited. Priority is set according to the company size, the risk profile of its industry sector and results from previous inspections. The Inspectorate will conduct approximately 27,000 inspections in 2012 based on risk profiling and sampling. About 55% will be risk-based, targeted inspections with 45% selected randomly for spot checks.			2	2		2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Inspections are notified 1-4 months in advance but no specific date is given. *Our opinion: Clear selection process. Authority in position to be more targeted now that it has completed initial assessments of all companies. Uses a data driven approach to select dutyholders for inspection but also includes sampling to ensure that others are chosen that may fall outside of the riskier profiles. As with other examples, a target has been set for the proportion of proactive and reactive supervision that will be undertaken by the safety authority, with the balance being slightly in favour of proactive supervision.*							
D	OSH	GB	"Have systems for deciding… priority according to the nature and extent of risks posed by a dutyholder's operations. The dutyholder's management competence is important, because a relatively low hazard site poorly managed can entail greater risk to workers or the public than a higher hazard site where proper and adequate risk control measures are in place. Certain very high hazard sites will receive regular inspections so that enforcing authorities can give public assurance that such risks are properly controlled." *Our opinion: In the context of NSA, it may be important to emphasise that when targeting RUs/IMs, impressions of general competence (e.g. from the SMS) may be a relevant influence when deciding where to target supervision activity. Historical factors (such as poor management of safety) may influence supervision decisions: it is therefore important to establish a system for prioritisation of proactive supervision that account for such factors. In this example, the factors to be considered are: what is the risk that is being controlled and how well has the dutyholder controlled that risk historically; and, what are the political and public priorities for supervision (e.g. prominent high hazard activities).*						2	
I	Rail	NL	"The discussion about safety certificates is always for the duration of the certificate. There is, in the law, a maximum of five years, and before it was three years. It's only a few months since we can give certificates for five years, and that discussion is always about proportionality; shall we give it short, the certificate, and so a year, or a longer period? So there is a lot of discussion about that. "I know that we have a system of risk analysis, so we try to rate the risk (there are three or four kinds: minimal, average, maximum risk). Shortcomings [in an RU/IM's SMS] are put into these risk rates, and then the risk rates stand for a year shorter. There's a time component of the risk category it's put in. So not every shortcoming base is heavy, and not any shortcoming is just as heavy as the other one. Some shortcomings don't have any effect on safety, so they are not important, and they	2	2					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			don't [lead to] shorter duration of the certificate. It's trying to make these risks… to put them into an order so you can see how important they are to the length of the certificate." *Our opinion: When assessing or reassessing an application for a safety certificate, one technique adopted by the NSA as a 'proportionate' sanction is to vary the duration for which the certificate is valid. The NSA has recently had a change of legislation to permit five-year certificates but the law allows durations as short as one year. This is an example of forcing earlier/more frequent supervision on an RU/IM by way of reassessment. Shorter validities are issued when the risks associated with operation are considered to be greater or more numerous.* *The decision regarding the duration is subject to the same 'controls' (colleague and peer group reviews) before it is issued and the NSA is currently attempting to formalise and document this decision-making process. It is based on risk analysis, with different levels of risk equating to different durations of validity.* *It should be noted that this NSA still carries our inspections whilst the safety certificate is valid: the shorter durations are a further safety sanction rather than a replacement for regular supervision. This approach has partly arisen because staff issuing safety certificates for this NSA are not the same as those who carry out inspections and regular supervision.*							
I	Rail	DK	The Danish Transport Authority wishes to target its supervisory resources in a prioritised manner. To ensure the targeted management of resources, the Danish Transport Authority has developed a method, based on a model developed by the Norwegian railway inspectorate, to systematise the prioritisation of audits using the risk picture for the individual undertakings. The method is not a tool to carry out a risk analysis of the Danish railway sector in its entirety, but a risk-based prioritisation tool for use by the supervisory authority. The method is used to prioritise the scope of audit activities with respect to each individual undertaking based on the relative risk for passengers, third parties, and the environment. The method is used to assess the undertakings' relative risk potential in relation to each other, so that they can be sorted into 'priority categories', which in turn will define the number of audits (or audit days).	3	3	3	3		3	3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			All RUs/IMs are required to have at least two audits during the validity of a certificate or authorisation. However, to sort the priority for auditing and the extent required, the following factors are rated: • Train km: give a good picture of the degree to which an undertaking contributes to the overall risk picture and are also used as a basis for Common Safety targets. • Type of RU/IM: the complexity of the operation, organisation and staffing; its interfaces; its exposure to third parties and level crossings; its exposure to other RUs; its infrastructure type and any other special risks. • Prior audit and supervision experience: including any action taken, confidence in the RU/IM's abilities and severity of non-conformities. • Incident data: including minor incidents. Each RU/IM is scored and ranked according to the adjustment factor listed above. The ranking is not published but the process described here is, along with 'focus areas' for the year, which can lead to further audits and inspections independent of those planned annually. Each year, the prioritisation plan is reassessed.							
I	Rail	DK	The NSA has a supervision strategy for the sector, which identifies the proportion of time to be spent auditing each RU/IM based on a ranking system (described separately). Delivery of the planned audit days is then distributed over the year – the NSA does not believe that a single audit for a two-week period, for example, is a worthwhile approach. Instead, "we actually split the [audit] days over the year, having different items for the different supervisions, or different locations". This is supplemented by 100 specific plans to cover the individual RUs/IMs (some are the focus of multiple plans). Each plan is written but is not shared externally. The content follows good auditing techniques: "We are talking about the two main items of the way of working, the horizontal and the vertical. And we ensure, by doing it on a five year basis, that we supervise the whole scope of the management system, that we do it horizontal. And doing it risk based, we identify the items that need special attention and we go deeply vertical into those." *Our opinion: This approach to structuring supervision activities contrasts with that described by other NSA, which will aim for a single visit within a period of time. Distributed supervision may enable an NSA to supervise a wider range of items. It may also decrease the burden on the RU/IM when*						3	3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			compared with a single, intensive audit.							
I	Rail	A	"We have a checklist for the application and this checklist is also taken as a starting point for supervision. So this I would also call a plan, but not in the sense of [the] regulation." *Our opinion: There are elements of good practice in supervision extending items from the initial assessment.*						1	1
I	Rail	A	Supervision priorities are set by the supervision team, which works together to process data from incidents and reports to set priorities. *Our opinion: Baseline good practice is to plan supervision according to incident data and RU/IM capability - in this context, 'reports' are on issues related to RUs/IMs and so meet some of the basic requirements of a capability assessment.*						1	1
I	Rail	BG	Target areas for supervision are selected based on activities where the NSA believes there are risks: this is established by analysis of previous supervision activities, daily reports on the safety of the railway and incident data. "Every day we receive data about different non-compliances… on the national railway network, and these are in the form of messages, telegrams, that we receive. They are analysed, they are collected, and after that we judge in which activities the risk is higher, and which activities have to be supervised, and which [railway] undertaking. So the supervision, sometimes it is immediate control, depending on the degree of risk, or it can be in time, if, for example, we have noticed that there is a repetition of certain identical cases of deficiencies or occurrences. There are deviations which we have found out, we establish, then we can make some extra-ordinary audit of the safety management system of an undertaking, which is not planned, but extra-ordinary, but the judgement is on the basis of expert opinion. We have a monthly plan for the supervision activity for the regional inspectorates that we have. We are speaking about the supervision activities. And also there is a three-month plan. So this is the operational planning, what we have said, that monthly and the three-month plan."						1	1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: The NSA regularly updates its supervision plans in accordance with the latest data. The plans cover not only the areas that are to be supervised but also at which RUs and whether a review of an RU/IM's SMS is warranted. This type of supervision planning is predominantly reactive.							
I	Rail	BG	Financial resources for supervision are, "planned on a monthly basis, and there are cases when they have to be surpassed, but this happens rarely, to spend more resources than usual, and this happens on the basis of approval by the executive director of the railway administration executive agency. And concerning the human resources, we plan, during these actions, and respectively we also plan the reactive activities as every week we spend some time on this activity. With this planning of the budget, monthly, it is distributed evenly throughout the year, and on this stage we manage to cover all these activities." *Our opinion: The NSA demonstrates a fluid approach to budgeting that enables it to react to incidents that may require more resources and then re-distribute these funds throughout the rest of the year. It is good practice to be in a position where all necessary activities can be funded, hence the NSA planning ahead to evenly distribute available resources.*							2
I	Rail	S	"We try to target it like risk-based, and we don't have so much resources that we have to target supervision and we try to target where we see the risks are higher or most effective to do. We have input from a National Investigation Body. We have an accident emergency phone that RUs and IMs could phone [24 hours]… on different matters about serious accidents. We are having meetings every week, discussion what kind of accident or information did we get last week, and if it's something that we should use to change our supervision plan... We have just now [an] issue that… vehicles have problems with the brakes, and it seems the first one [is] a company having a problem with the brakes, and they are taking care of it and they're making a technical investigation. And then… later another company having the same kind of vehicle have the same problems, and they discover that it was problem with the drying the air for the brakes. And there… we have to take sending a letter to every company who has those types of vehicles and inform them about this and make perhaps a special audit about how they take care of their maintenance for the brakes. So that's some kind of the target issue. Other ways we get information from people outside, we get information from other railway companies or Infrastructure Manager… and now we discuss and see should we take this issue to another step or what risk is this in the whole system?"						2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			These inputs are documented in an internal supervision plan that is created annually but updated as supervision priorities develop. If priorities for targeting are not urgent, the output from the weekly meetings will be recorded and fed into planning for the next year of supervision. *Our opinion: The NSA is aware that its resources are limited so it must be selective in how it targets activities for supervision. It describes an approach that looks for emerging problems that could have a wider market impact, rather than being present in a single organisation. Weekly meetings enable staff to consider whether new issues require immediate changes to supervision or can be deferred to the supervision plan for the following year. The use of a 24 hour reporting line for serious incidents encourages RUs/IMs to get the NSA involved at the earliest opportunity.*							
I	Rail	CZ	The Czech NSA has no formal supervision plans. It has 80 RUs/IMs and each has a certificate with a validity of 5 years. The NSA aims to audit each RU/IM once in this period so it is tasked with conducting 16 audits per year, on average. It requires 2-3 staff per audit but has "no capacity to do the audits properly". There are no general rules laid down regarding which RUs/IMs should be audited first, or in what order audits should be executed. One factor that is considered is whether the organisation is completely new or if it is an existing organisation. For example, one applicant comprised staff from the old Czech state railway so as a result of this operational experience, the NSA allowed it to operate for a year before it undertook its first full audit. The safety certificate had to be "issued very quickly" in this example so there was not an opportunity for an audit to be conducted at the same time. To introduce a supervision plan at the time of issuing a safety certificate was reported as "impossible". One of the reasons was that many applicants would not be operational at the time of applying. The application would be in order to obtain a certificate so that the organisation may tender for operational contracts. Thus the certificate will be based on an application that may only involve renting a rail vehicle (e.g. an historical vehicle), which will bear little resemblance to the scope of operations that the company is bidding for. Further to this, after some time (maybe up to two years), the company may, "start operation… in huge… volume - I think five pairs of speed trains on the main line." The RU has no duty to inform the NSA that it has started operations:						-1	-1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			"They have no obligation. They have, if there are some changes, they have to inform us one month after these changes. And in this case, it's possible to go for an inspection. This is good time for going for inspection. But… if we find that something is incorrect, we have to start legal process to withdraw those safety certificate, which is very difficult." Furthermore, the NSA has another type of RU to contend with – the occasional operator: "Some companies operate only rarely. Small companies - we have many companies - I say that they are certificate collectors, more than real operators, who… sometimes, will go for a trip. And in these companies it's very difficult to do some inspection… we sometimes… ask infrastructure manager [to notify us if this company is due to operate]… so we went there for an inspection. But in this case it's very difficult to do for inspection because if something is wrong, you have to find evidence that it is wrong, and they can deny what have happened so it's very difficult to do this in any operation." *Our opinion: The NSA has a no systematic supervision plan. Its audit programme is based on how it can utilise its resources over the life of a safety certificate or authorisation. There is no clear consideration of risk (although this was partly acknowledged by considering the experience of the applicant). It would appear to be poor practice to plan audits in this way, especially as some RUs/IMs may operate for almost the full duration of their certificate/authorisation before being audited for the first time. A distributed audit (as conducted by the Danish NSA) might be a suitable approach here as it would split a single audit into several short audits over the same period and enable the NSA to audit most organisations more than once during the certificate validity.* *However, the NSA also has to consider whether the applicant is currently operating or if they are planning to win a tender or just operate occasionally. In such examples, establishing a supervision plan would be difficult. Nevertheless, the system that is described, and in particular the lack of notice required for starting or changing operation, further complicates the NSA's ability to prepare for supervision. Of significant concern is the reported legal complexity associated with revoking a safety certificate, even if the operations for which it was granted have changed completely.*							
I	Rail	CZ	Supervision is, "concentrating mainly on internal rules, the system of the adhering of internal rules, qualification of staff, qualification of drivers, and internal rules for supervision of drivers." *Our opinion: This focus would suggest that the NSA is following national safety rules rather than the*						-1	-1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			European safety regulatory framework. Rather than targeting supervision at a range of activities across RUs/IMs, it is concentrating on specific areas that relate to its own legislation.							
I	Rail	PL	The NSA described a mixed approach to planning supervision based on established processes and SMS-based supervision: "Our activities; this is the traditional control plus element of SMS supervision. In these activities, we do apply the principle of proportionality – we did apply it before. The main thing is that it's a sort of intuitive assessment of the risks, the threats to safety, depending, for example, on the kind of goods carried by a given undertaking. So if these are dangerous goods, if we assess the risk as higher, there are more detailed and more frequent controls, inspections. This is not fully what the EU supervision is like but still more the traditional approach." Divergence from the European safety regulatory framework was described: "Our understanding of the requirements of both regulations [1158/2010 and 1169/2010] is that there needs to be… specific undertakings being the targets of supervision. Whereas in the traditional Polish model that we still apply, it is not specific undertakings but the global risks within the system." This supervision plan is updated quarterly and has several inputs: • "Global market statistics on safety and the sort of events that occurred." • "Results of the previous years' supervision and feedback from these activities… local branches that know exactly their little regions which they are responsible for… propose the topics, the areas which should be controlled." • The extent to which an RU is engaged in particular operations, such as the transport of dangerous goods, and the amount of experience it has. • History of repeated breaches of the regulations (which will lead to more detailed controls). • Changes in operations reported by the RU/IM (e.g. a new fleet). • Changes reported (or not reported) to the SMS – the NSA is suspicious of RUs/IMs that do not report any changes to their SMS even if new legislation has been issued. • Forthcoming events (e.g. European Football tournament).	1					2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			The NSA described why it has not changed its supervision planning process: "Now the situation is that we have the control reports, both regarding specific topics and specific undertakings. We have those detailed reports and now we have a problem which stops… us moving to the new, European approach because we have not enough resources to select those documents and analyse them so that it's really railway undertaking-specific supervision and not topic-specific. This is generally one of our basic problems, the shortage of staff that prevents us from fully moving into the new approach to safety management." *Our opinion: The factors contributing to the supervision plan were given as examples of a proportionate supervision response. To achieve compliance in the sector, the NSA considers these factors and adjusts its supervision response accordingly. It has a proposal for developing supervision plans for individual RUs/IMs but it does not have resources to deliver these proposals.*							
I	Rail	PL	The NSA elaborated on its mixed approach to supervision: "The Polish experience in applying, preparing, approving SMS is different, it's definitely shorter than in the case of the countries that had them [SMS] before. You could say that we are actually moving towards the SMS-based assessments. It's not there yet, it's not completely implemented. The fact is that once… a dutyholder is provided to have SMS, it doesn't mean that all the railway undertakings suddenly start operating in accordance with the new rules. This also means that our supervision has to be slightly different. We are evolving. We perceive our duty as supervising the enterprises on the basis of or through the SMS systems. However, now it's an element of the [supervision] plan [to control] the degree of SMS implementation. We are only *moving towards* the fully SMS-based approach. However… one of the factors that forced us to operate in that way is the laws changing slowly to full implementation of European legislation." *Our opinion: The NSA is aware that it is unable to make an immediate switch to the new SMS-based approach and so has elected to incorporate an element of SMS supervision to encourage a gradual shift. It is good practice that the NSA has considered how to manage the transition and has a plan of action for doing so, whilst still maintaining safety by continuing its previous role to some extent.*						2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	PL	Supervision plans do exist for individual RUs but these are based on Polish law. They require inspections to check the conditions for issuing a Polish licence. "What we realised is that the expected approach to inspections should be… starting with certificates and not the licences. It's like the legislature still fails to acknowledge a different, more globalised approach to supervision." *Our opinion: There is clearly some duplication in the supervision activities of the NSA (as a result of national legislation). The NSA has recognised that efficiencies could be achieved by combining the approaches and focussing on the requirements for issuing certificates. These potential efficiencies are challenged by national legislation.*						1	1
I	Rail	E	When planning what activities to target for supervision, the Spanish NSA considers inputs from RUs/IMs and from accidents reports: "We determine higher risk by talking and asking questions to gain information from RUs/IMs about the current activity… throughout the past year. So they know better than us which are these higher risk activities. So we produce our assessment and our enforcement in their own knowledge. So we ask them and then we assess the answers of the RUs/IMs. We assess those answers with the NSA staff. We have people in our NSA with more than 30 years valuable background, so we make a supervision of this higher risk based on our own experience and the RUs/IMs experience too." The NSA also considers accident reports from the body responsible for producing them. Collectively, the NSA makes proposals for what should be targeted; these proposals are shared with the accident investigator. *Our opinion: The NSA acknowledges that IMs/RUs are best placed to determine the risk that exists from their activities. The NSA describes a collaborative process where the NSA considers the risks together with each RU/IM in light of its experience and its knowledge of accidents across the whole sector.*			1			1	
I	Rail	E	The NSA has given thought to establishing a set of audit indicators to help it target and evaluate its activity: "We will put in practice targeting by specific areas throughout our NSA to start and where we had safety indicators that include our target areas, preliminary safety, supervision procedures, so we will make and change the monitoring by annual audit. So we hope to, or we expect to get some important information to be able to differentiate target areas from not target areas. But… these audit						1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			indicators are being developed right now, so we hope that this could be a good beginning. These indicators are included in our supervision procedures and… could be of course accidents, activities, technology, maintenance, safety, installations, human errors. So these indicators are directed to have more information about how the RUs/IMs are making development, developing these activities and so we could know what areas are critical or not for our supervision." *Our opinion: It is good practice to define a set of criteria that will be used to measure the performance of NSA in different areas and guide current and future targeting of supervision.*							
I	Rail	S	The NSA plans the distribution of its resources based on the number of certificates it expects to renew each year (which require a full audit) and the number of new companies that require a full audit (delivered in the first 6–12 months of operation), and then whatever staff time remains is used to supervise other risk-based factors. *Our opinion: This is a partial example of resource-based planning although the NSA does use more capability-based assessments to determine how the remaining time for supervision will be distributed. It may be a necessity to consider the effect on resources of carrying out essential activities such as assessments and initial audits.*						1	1
I	Rail	D	"The main aim of supervision should be to… give a reliable picture about safety and safety relevant areas of railways, and that's where we have to focus our supervision. We have a long history of supervision and that's why we think, based on the experience we have and the activities we do, that we have developed a good system for targeting of prioritisation of our supervision." The system for targeting supervision varies with the different structural subsystems: "…in principle, it's a risk based or risk oriented system and, in some areas, based on statistics... It's cases from the past where we draw conclusions from. In principle it's gathering all information we have or we can have from all the sources available and then extracting from that the most risky areas of subsystems or aspects or whatever where we have to put our focus on." Supervision plans can be adjusted on an 'ad hoc' basis but should be reviewed at least yearly: "…if there's an incident, which could lead to an adaption of the supervision plan that this special subsystem or component which led to an incident or accident, proves to be risky which we didn't see						2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			before or have to adapt and concentrate more on that or take that into account. In principle it should be on a yearly basis… there should be a review of the supervision plans or strategy, what to supervise and where to maybe adapt strategy or the priorities." The review process would be a 'roundtable' discussion involving lead auditors and other staff responsible for supervising the different structural subsystems. The lead auditors, with their 'account holder' roles, have substantial input to the process of reviewing supervision plans. *Our opinion: The NSA is clearly targeting supervision activities based on risks observed across the market and within individual RUs/IMs. The NSA will adjust it supervision targets if an incident or a case gives them reason to shift the focus of their supervision; otherwise, reviews are regular and involve the staff who deliver supervision at the frontline.*							
I	Rail	F	"As far as performance of the different entities are concerned, we have a database where we record all the incidents, safety related incidents, and these incidents are reviewed, obviously if there's a major incident we don't wait until the end of the month but these incidents are reviewed on a monthly basis at the departmental meeting. So they're discussed with the head of department and his heads of specialist divisions and we identify those ones which perhaps give us cause for concern based on what we've seen before because our database allows us to either look at incident types or look at the entity that is responsible, was the cause of the incident. So that's basically how we target. But the other thing… we target systematically an entity which has received a new or even renewed authorisation. A new authorisation will always involve an audit taking place six months after the authorisation has been effectively used. So the targeting is based on that. We found it thus far quite effective. [In addition] the ministry requests us to undertake a certain amount of controls every year. And we are given... numbers of the controlled inspections he would like us to do every year. But as far as the selection of which ones are concerned, that's down to us, because we have the expertise on… which entities have had their authorisations granted or renewed, and the database belongs to us and we're the only ones that have access to it as far as the situations we identify as specific risks." This proposed audits and inspections are brought together in an annual supervision plan. There is a monthly meeting at the NSA to discuss and adjust the plan as required (often based on recent						2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			findings/incidents). The plan includes the targets set by the Ministry, which for the current year have been met so the NSA is already starting its programme for 2013. *Our opinion: The NSA is demonstrating good practice by planning its supervision activities. It supplements its obligatory audits/inspections (as set by the requirement to audit new/renewed entities within six months, and the Ministerial targets) with further supervision that is guided by incident analysis and monthly staff discussions. The NSA reports that the Ministry is not prescriptive regarding the targeting and content of supervision, which is desirable given that this should be established using the judgement and expertise of NSA staff.*							
I	Rail	F	The French NSA elaborated on the inputs to its supervision plan: "There's the systematic audit we do. There may be other subjects which… we haven't looked at for some time so perhaps… we want to look at. Plus… the incidents on the database. In the database we don't just have accidents, we do have incidents or near misses... a typical one says that the signal passed at danger but no collision. All the signals passed at danger would be picked up in the database so we will pick up any tendencies or certain things which cause us concern. As the far as the state of the concern we have two levels of inspector; we have 'inspectors', and 'inspectors in charge' of inspections and audits. Inspector in charge will tend to have more experience, certainly in the number of inspections he's already done and that goes on to the competency part. But by definition an inspector in charge will attend the programme meetings [for planning supervision]." *Our opinion: Supervision planning by the French NSA has a range of inputs. The consistent requirement for a timely audit after a renewal or first issue is accompanied by themes from incident analysis. The NSA also utilises what could be described as a 'bottom-up' approach by involving its inspectors in charge in the meetings that are organised to plan supervision activities. These inspectors are the most experienced frontline staff and will have a good understanding of the emerging priorities for supervision to accompany the 'top-down' incident-based inputs.*						2	2

Table B.19: Action taken after reviewing supervision plans

NSA	Changed the...								
	Activities targeted by the plan	Type of data collected to support the plan	Amount of resource allocated to supervision/enforcement of a particular RU/IM	Plan altogether	NSA's general supervision/ enforcement strategy	Recommended Member State take action to overcome a deficiency in the safety regulatory framework	Informed other NSA of the outcomes/actions it is has taken	Informed ERA of the outcomes/actions it has taken	Other, please specify:
Great Britain	Yes	Yes	Yes	Yes	Yes	Yes	No	No	
Sweden	Yes	Yes	Yes	No	No	Yes	Yes	No	
Estonia	Yes	Yes	No	No	No	No	No	No	
Lithuania	Yes	No	Yes	Yes	No	No	Yes	Yes	
Romania	Yes	Yes	Yes	No	Yes	No	No	No	
Germany	Yes	Yes	Yes	Yes	No	No	No	No	
Denmark	Yes	No	Yes	Yes	No	No	No	No	
Spain	No	No	No	No	No	No	No	No	
Latvia	No	No	No	Yes	No	No	No	No	
Poland	Yes	No	No	No	No	No	No	No	Plans are based on old national requirements. The plan for 2011 has not been drafted on the basis of CSM

NSA	Changed the... Activities targeted by the plan	Type of data collected to support the plan	Amount of resource allocated to supervision/enforcement of a particular RU/IM	Plan altogether	NSA's general supervision/ enforcement strategy	Recommended Member State take action to overcome a deficiency in the safety regulatory framework	Informed other NSA of the outcomes/actions it is has taken	Informed ERA of the outcomes/actions it has taken	Other, please specify:
									requirements. The plans are updated due to unexpected events (example: After Viareggio accident we have launched additional supervisory activities concerning axles and wheelsets).
Bulgaria	Yes	No	No	No	No	Yes	No	No	
Austria	No	No	No	No	No	No	No	No	
Portugal	No	No	No	No	No	No	No	No	
Czech Republic	No	No	No	No	No	No	No	No	
Netherlands	No	No	No	No	Yes	No	No	No	
Channel Tunnel	Yes	No	No	No	No	No	No	No	
Hungary	Yes	Yes	Yes	No	No	No	No	Yes	
Norway	Yes	No	Yes	Yes	No	No	No	No	

NSA	Changed the...								
	Activities targeted by the plan	Type of data collected to support the plan	Amount of resource allocated to supervision/enforcement of a particular RU/IM	Plan altogether	NSA's general supervision/ enforcement strategy	Recommended Member State take action to overcome a deficiency in the safety regulatory framework	Informed other NSA of the outcomes/actions it is has taken	Informed ERA of the outcomes/actions it has taken	Other, please specify:
Ireland	Yes	Yes	No	No	No	No	No	No	
France	-	-	-	-	-	-	-	-	
Finland	No	No	No	No	No	No	No	No	
Italy	Yes	No	No	No	No	No	No	No	

Table B.20: Conditions for partial checks of an SMS

NSA	Partial SMS check to ensure that more RUs/IMs can be checked in a certain period	Other	If other, please specify:
Great Britain	No	No	-
Sweden	No	No	-
Estonia	Yes	No	-
Lithuania	Yes	No	-
Romania	No	No	-
Germany	No	Yes	Remark: Question seems to be misleading, as 'partial' does not necessarily mean 'ad hoc' but this is supposed by the way the question is formulated. Partial checks of RU/IM SMS are a vital part of the NSA supervision, be it 'ad hoc', randomly, planned or whatever.
Denmark	No	No	-
Spain	No	No	-
Latvia	Yes	No	-
Poland	Yes	Yes	We haven't conducted any partial checks till now because of short time during which the supervision system through SMS works. As a target solution we plan to use the CSM on supervision as a basis for such actions and to conduct them in response to specific safety concerns/incidents.
Bulgaria	No	No	-
Austria	No	No	See also: Concerning certification by accredited bodies.

NSA	Partial SMS check to ensure that more RUs/IMs can be checked in a certain period	Other	If other, please specify:
Portugal	Yes	No	-
Czech Republic	No	No	-
Netherlands	-		
Channel Tunnel	No	No	-
Hungary	No	No	
Norway	Yes	No	
Ireland	No	Yes	In response to public complaints. Asset inspections are pre-planned not ad hoc.
France	-	-	-
Finland	No	No	-
Italy	No	No	-

Table B.21: Proactive and reactive supervision

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	Targeting: split inspectors' time in half – 50% spent on proactive inspection and 50% on reactive inspection. Proactive inspection is "What do we want to go and inspect? So we will look at the overall risk profile of the railway, risk profile of duty holders, we will analyse what we've done previously with those duty holders and those risks, and say, actually, where we've run the Rail Management Maturity Model, which further enhances our ability to say, actually, what are the strengths and weaknesses of a duty holder? And where should we go and put our noses, for want of a better description, in, to have the best effect on improving safety of those duty holders. So we're very targeted in what we will go and look at." Reactive inspection is: "incidents have happened, and we go and look and learn the lessons of why they happened, and if necessary, adjudicate some justice, for want of a better description… we have a very targeted approach to the investigation process that says we've got a list of mandatory investigations. This is your starting point. These shouldn't be happening. It doesn't mean to say you have to go and look at them and investigate them, but it says you will certainly consider them, and, for example, and trespass will fall into that, or an incident at a level crossing. Now, if you happen to have investigated a very similar situation two weeks earlier, and you know what the outcome was, and the duty holder's already acting, you can literally turn around and say, well, okay, on this occasion there's little value in learning these lessons. We've already started. The duty holder was already acting on the recommendations. We're not going to do it. But otherwise you'd go and investigate and work your way through that." *Our opinion: It is good practice to set targets for how inspectors' time will be divided between these two important functions. An equal balance is believed to be baseline good practice; if an NSA were to spend more than 50% of its time on reactive inspections, this would indicate poor and ineffectual targeting.*						1	1
I	Rail	A	The Austrian NSA typically spends 90% of it supervision time on proactive audits and inspections. More or less will be allocated to proactive supervision depending on the number of incidents occurring that require reactive inspections. The proportion planned for each type of supervision is set out in the strategy. *Our opinion: The NSA has set itself a strategic good practice goal to undertake a high proportion of proactive supervision.*						3	3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	BG	Proactive and reactive supervision is conducted "in parallel": "We cannot say that we separate the time on both activities, so we have to react in all kinds of occurrences, and at the same time we continuously perform preventative activity and supervision. Of course, just practically speaking, we have one day of the week in which we analyse the various occurrences, accidents, incidents, near misses, and this is done continuously and regularly. And when necessary, in case of some more serious incidents or accidents, then we spend more time on such cases. At the same time, the supervision is also a continuous activity." *Our opinion: The NSA appears to allocate at least a fifth of its time (one day per week) to analysis of incidents, which is reactive supervision but which helps to inform proactive supervision. Otherwise it divides its time on the basis of how many incidents it has to react to. Whilst this approach may be borne of necessity, it is useful to set a target for the minimum proactive supervision that the NSA will accept.*						1	1
I	Rail	S	The amount of time allocated to proactive supervision is approximately equal to that allocated to reactive supervision. Overall, about half of an inspector's time is spent is spent on assessment and supervision, with the other half allocated to working groups, project meetings, reviewing procedures (such as the checklists), and issuing guidelines. *Our opinion: The NSA appears to be prioritising the assessments required to issue or renew certification ahead of other supervision activities. It acknowledges that it is currently unable to carry out as much proactive and reactive supervision as it would like. Whilst this situation is undesirable, certification must be timely and thorough in order for there to be a safe, open rail market.*						1	1
I	Rail	S	The NSA stated that its resources were "too small": "We always talked about we should do more supervision. We see every time when we are out in audits, we see evidence of the company not really familiar with… 'system thinking' [use of a SMS]. So I think we have some part of education of the companies when we are out auditing them because they haven't made their own audits, they haven't… they're not really on the track so we see a lot of examples of that - it's very important to be out visiting the companies, learning them how to work with the safety management system. We should be out there a lot more." *Our opinion: The NSA appears to be prioritising the assessments required to issue or renew certification*						1	1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			ahead of other supervision activities. It acknowledges that it is currently unable to carry out as much proactive and reactive supervision as it would like. Whilst this situation is undesirable, certification must be timely and thorough in order for there to be a safe, open rail market.							
I	Rail	CZ	Approximately 80% of supervision activities are proactive. *Our opinion: A high proportion of proactive supervision is considered good practice although this particular NSA was not supervising at all times using the SMS-based approach.*						2	2
I	Rail	E	The Spanish NSA expects that about 75% of the time allocated to inspections will be directed at proactive supervision. "Our inspections will be at the first glance proactive because we consider that to be reactive… could be very aggressive for RUs and IMs, so we will try to be proactive and not make a lot of penalties. Instead of that we prefer to encourage them to improve their procedures in the critical areas. We consider that our sector is composed of very professional RUs and IMs, enterprises, so we are trying not to tell them what to do. We try to learn from each other we can offer them a lot of information about European regulatory framework and they are providing us a lot of information and knowledge about operations and specific activities of RUs/IMs. So we are trying to exchange a lot of information and to make enrichment of each other." *Our opinion: The proactive approach has been prioritised to help develop a positive safety culture. One of the stated goals of this approach is to encourage RUs/IMs to be open with the NSA when exchanging information and knowledge.*						2	2
I	Rail	D	"We maybe leave some room for reactive supervision… 80% or 85% of the resources are allocated to planned or proactive supervision, if you can say that planned is always proactive, and maybe that's some … reserve for reactive supervision, which we know will come but we don't know where and when." *Our opinion: The NSA has a bias towards proactive supervision, which could be considered good practice.*						3	3
I	Rail	F	"As far as the audits are concerned it's systematic. And as far as incidents in the database are concerned, we don't like to wait until something really has gone wrong; we look for tendencies, then we decide that a particular problem really needs to be the subject of an inspection and then we plan it and we go. I would say the vast majority are proactive… Round about 75%."						2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: The French NSA prioritises proactive supervision, which can be considered good practice.							

Table B.22: Delivering supervision

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Rail	GB	Balancing targeting low-freq, high risk activities vs high-freq, low risk activities: "The low frequency high consequence is where we devote a lot of effort and a lot of inspector effort, but very much on the principle of safety management system, you know, does the system work, because we don't know when that catastrophic incident may arise, whereas the problem with the high frequency, low consequence incident is it's happening everywhere… Take slips and trips at stations. A large amount of that is how far do you go in regulating what the passenger does? So we actually give that to what we call our RICOs, our Railway Incident Contact Officers. So they're not inspectors, but they will go visiting train operators, infrastructure managers, looking specifically at stations, and how passenger flows work. Slips and trips, those sorts of… I wouldn't quite call them basic health and safety criteria, but they will go and specifically look at those, in the hope that the duty holders will then act on that advice." *Our opinion: NSA inspectors focus on preventing catastrophic risk. Low risk activities are often inspected by RICOs that do not have the same powers (e.g. they are not warranted inspectors) but can report back to inspectors and escalate an issue if they feel it is not being managed appropriately by RUs/IMs. The NSA can ring fence a budget for this activity and doing so may enable the safety authority to focus on its targets for proactive inspections given that many reactive inspections are likely to be related to low risk activities that can be dealt with using this system.* *If an NSA historically has to deal with high-frequency, low risk incidents, it is good practice to consider efficient working practices to deal with them. This may include a team of staff with a different standard of qualifications who can serve as a more efficient workforce for dealing with such incidents.*	2	2	3			3	3
D	OSH	GB	Investigations: The authority expects discretion to be used for deciding when to investigate. This discretion should be based on assessing: • the severity and scale of potential or actual harm; • the seriousness of any potential breach of the law; • knowledge of the dutyholder's past health and safety performance; • the enforcement priorities; • the practicality of achieving results; and • the wider relevance of the event, including serious public concern. *Our opinion: Discretion should indeed be used, providing that there is a basis for an NSA investigation to begin with. The NSA will need to cooperate with the NIB and any other authorities to establish*	2	2				2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			whether it is appropriate for it to investigate and incident. It is acknowledged that in some Member States, the NSA may be required to investigate in addition to the NIB for the purposes of making safety recommendations and enforcement decisions (the NIB will typically explore the technical cause rather than any underlying SMS failures). If it is appropriate for the NSA to investigate an incident, the decision should then be subject to discretion. The principles listed in this example are sensible given the frequent need to prioritise use of resources and work efficiently; however, the remit of an NSA is narrower and so the criteria used to decide may need to be more focused.							
D	OSH	CZ	Website mini-poll – Question and multiple choice answers regarding key methods/procedures followed by dutyholders. After submitting response, can view distribution of results. *Our opinion: Simple but potentially effective way to encourage dutyholders to think about key issues – and to collect some data on the range of responses as well. Not tracked so responses are likely to be more honest, although range of respondents may be outside of the marketplace.*			2			2	
D	OSH	IRL	Online applications service By law, workplace accidents must be reported to the Health and Safety Authority, as soon as possible. Construction Reports (AF2) must be submitted before construction work starts. Using the online system to submit a report: • is faster than filling in a paper IR1 or AF2 form and posting it • allows users to view all accidents reported online over the last year • allows users to view all construction reports submitted online over the last year • provides a confirmation reference for each accident reported or construction report submitted • enables the Health and Safety Manager of the dutyholder's organisation to view all the accidents reported or construction reports submitted for their organisation online over the previous year *Our opinion: NSA should consider whether it is appropriate to establish a system for the market to self-report specific events. Where there is relevant legislation governing the reporting of incidents and occurrences, an online system is efficient. Such a system could be interrogated by the NSA as one approach to supervising the market.*		2	2				2
D	OSH	DK	Special surveillance method: dialogue and guidance. The WEA identified core problems for certain industries based on staff attrition rates (early retirement for health reasons, chronic illnesses, etc). Companies within these selected industries were then visited twice – the first to primarily offer guidance and the next to see how it was being implemented. Visits are slightly longer, require two			3			3	3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			experienced staff from the WEA, includes dialogue with management and staff, and visits are separated by 4-6 months. *Our opinion: Rather than relying on standard supervision and enforcement activities to cover all risks, the WEA has opted to focus on high-priority areas (based on risk profiles) and use its experienced staff to first offer guidance and then see if the guidance is being followed and applied correctly. This approach is an example of good practice when there are specific concerns about safety.*							
I	Rail	GB	"Inspectors can ring up and go 'I've got this problem'. This is… an on-going advice service, for want of a better description, just based on our knowledge and experience of doing these things and where people should be going or where people should desperately not be going." *Our opinion: Internal advice service enabling field inspectors to engage directly with senior inspectors to seek help and guidance whenever necessary to ensure that supervision and enforcement action is carried out correctly and according to the principles. More appropriate for larger NSA that have staff distributed across the country. The principle of being able to consult senior staff is good practice and it is recommended that NSA implement this in some way.*	2	2				2	
I	Rail	GB	Rail Management Maturity Model (RM3): each year the account holder will use the model to plot how good or bad the RU/IM is on 40 criteria. *Our opinion: It is good practice to have a comprehensive and consistent approach to ranking relative performance of RUs and IMs.*		3				3	
D	Aviation	IRL	Carried out a safety culture and SMS survey of dutyholder staff. The IAA was already carrying out regulatory audits to focus on the formal aspects of the SMS, such as the compliance with regulations. This survey sought to explore the beliefs, attitudes and values attached to SMS implementation – the 'culture'. Survey sent to all aviation organisations and completed by staff at all levels. Survey results shared with whole industry. IAA will use to prioritise its activities in the next 2 years. Overall aim is to promote dialogue within industry and with the regulators. *Our opinion: Good practice for understanding industry issues and also for feeding into strategy.*			2		2		2
D	Rail	EST	Q&A forum available – appears to be mostly used by passengers but could potentially be used for SMS issues etc. *Our opinion: Good practice for understanding industry issues and also for feeding into strategy.*			2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	GB	Whistle blowing policy in place. The CAA will endeavour to respect the confidentiality of a whistle blower unless agreed otherwise with them. The whistle blower should be assured that CAA will endeavour to maintain confidentiality and that they will receive a response to their complaint/allegation. Whistle blowers will be kept informed of progress with their complaints if requested. Whether the investigation is ongoing or has been concluded can be confirmed but information regarding specific details of the investigation may not necessarily be provided. Whilst it may be possible to progress a whistle blowing complaint without speaking with the whistle blower, experience has indicated that this can result in wasted or duplicate effort in order to fully uncover the detailed facts. As such, it is recommended that a telephone discussion or meeting take place. Wherever possible, interviews with whistle blowers should take place on CAA premises with another CAA member of staff present as a witness. It can be very difficult to verify allegations without adequate detailed information. The whistle blower should provide as much detailed evidence as possible, either hard copy or by email, not just verbal allegations. The preferred method of reporting to the CAA is by email using the Whistle blowing report form[1] or if this is not possible, reports may be given by calling the CAA Whistle blowing Focal Point. *Our opinion: it is important for the NSA to engage with staff at all levels across the market. Whistle blowing policies permit staff to escalate safety concerns that they are unable or unwilling to escalate within their own organisation – and to do so without fear of reprisals or identification. To ensure that such information is collected and processed correctly, it is good practice to establish a policy and reporting system.* *Such a policy may also be more effective if the NSA has taken care to disseminate widely information about the safety regulatory framework and its role as a regulator.*				3			
I	Rail	DK	Discrepancies, or minor non-conformities, with the SMS may be discovered during supervision. "What we do is we make a remark instead of a non-conformity. You could also describe it as a minor or a major non-conformity but we call it remark if it's a minor. What is a minor? That could be if in the safety management system there's a procedure that tells the company that they shall make sure there are two signatures on a maintenance form or something and if we see that there's evidence that there's never any signatures on these forms, then it would be a non-conformance. If we can see that, okay, some guy forgot this one time, it's a minor. Then you can say, okay, you have a system which is working, you forgot this, and we just make a remark. We would say it on site and we will make a note in our report and we will probably make an interim note about it, so next time we go to	2		3			2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			this company we'll just check again, just to be sure." *Our opinion: Somewhat similar to the Danish OSH authority, the NSA seeks to use dialogue to address some issues before implementing formal enforcement. Developing dialogue with RUs/IMs may enable more effective supervision if the market feels that the NSA is working collaboratively to improve safety rather than simply delivering enforcement.*							
I	Rail	CZ	The Czech NSA can issue enforcement notices. Using an example of level crossing visibility, the NSA would inspect the crossing and, if visibility was affected by vegetation, it would request that the RU/IM correct this within a certain time limit. However, failures of maintenance were not readily recognised as indicating a problem with the SMS of the RU/IM: "If you go for inspection, always find something that it is not exactly right, but I can't say that the safety management system in this case of infrastructure manager work or doesn't work properly. I think it works. I think that it depends on the financial quality, or financial possibilities of infrastructure manager. I feel that the supervision is to introduce some pressure on the infrastructure manager. I think that they should maintain mainly the local things, the reasonable condition to avoid possible dangerous risk." *Our opinion: It could be considered poor practice that a failure to maintain a level crossing is not explored as a possible SMS fault. The assumption is that the oversight is due to insufficient finances; however, this is not necessarily an acceptable reason for overlooking safety matters. The NSA acknowledges that supervision exists partly to encourage RUs/IMs to improve and yet some of this improvement could be realised by changing the SMS.* *There would appear to be some inconsistency in the logic of supervision. On the one hand, the NSA suggests that some of the problems it identifies would be a financial burden to control via an SMS, and are not sufficiently hazardous to require strict controls within the SMS; and on the other hand, the NSA is deploying its limited resources to identify these problems and then requests that RUs/IMs rectify them.*						-1	-1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	CZ	The NSA has limited staff (3) who supervise using the SMS-based approach. Of the 100 or so other supervision staff, "quite rarely" will they consider if a safety management system failure is a contributory factor in a breach of regulation. The NSA indicated that the underlying cause in '90%' of most breaches was 'human factor[s]'; however, there was no apparent effort to encourage RUs/IMs to improve their SMS to mitigate against the human errors that were occurring. *Our opinion: It is desirable for NSA to prioritise the transition of responsibility for safety to RUs/IMs; maintaining supervision practices that place the burden of responsibility for safety on the NSA does not encourage RUs/IMs to develop their SMS so that it is fit for purpose.*						-1	-1
I	Rail	E	The Spanish NSA has not yet established its approach to supervision. In developing a framework for supervision, the NSA has considered how it can introduce proportionality and consistency: • Enforcement measures have to be relative to the risk presented. Part of the assessment of risk will depend on the 'volume' of the operator. • Measures also depend on supervision findings: "We know the sector. We know we have global information of the railway sector. So with the person/people responsible safety from each RU and IM, we talk. Then we ask them for documents, documents of safety, operating, their plans, their projects, and then with the European regulatory team we make a first assessment. Then we have a second meeting with them to seek clarification on some questions, and then we apply a proportionate and consistent, depending on their own activity." • Internally, the NSA is developing consistency in its procedures: "We try to establish a general criteria… related to audits and supervision, and then we try to exchange our information, our procedures, and try to see if operators can do all we are asking for. So if they are in a degree of development of the activity lower than we are asking for, we try to encourage them to improve..." *Our opinion: The NSA is considering, to some extent, the operational status of the RU/IM when determining how to supervise/enforce, as well as the global risks that exist within the sector. To ensure consistency, the NSA appears to have established a baseline set of requirements that everyone within the NSA agrees upon. Action is focused on RUs/IMs that fall below this minimum requirement.*	1	1				2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	E	The Spanish NSA is focussed primarily on 'influencing behaviour' rather than forcing it. "We try to meet with every RU and IM staff. We are continually talking with them. We have a lot of meetings because we try to make them understand that this area, this supervision and enforcement involves all of us, not only the NSA. We are very successful because all enterprises of the sector are trying to improve continuously. It's difficult because they are operating day by day with a lot of specific procedures that are current[ly] right out of [existing national legislation] and now they are coming into a new regulatory framework, and it's difficult for them. But they actually are making all the changes that we're asking them and it's very good feedback for us. Right now we are not forcing at all. We are only making, influence behaviour because the RU and IMs behaviour related to legal means is quite good. But they can't do all that the regulatory framework is asking to them, so we have to be patient and we are trying to make influence and not force. We are making meetings, we are exchanging a lot of documents… plus, we have a global meetings with our RU/IM enterprises and they are understanding. They are making changes. They are developing task force teamwork. So we prefer to influence than force behaviour..." *Our opinion: This NSA has reported a positive safety culture within the sector that is conducive to enforcement via 'non legal', influential methods. The NSA is observing change within the sector and is satisfied with the pace so sees no reason to use legal enforcement methods. This positive safety culture may well have been promoted by what would appear to be open and regular dialogue between the NSA and RUs/IMs.*						2	1
I	Rail	BG	"We have rules of the control activity, and these regional structures, of the regional inspectorates, in which it's written how they shall make the inspections, and how they shall report back to the NSA. And these rules are on the website of the agency, so they are published." *Our opinion: The NSA has a regional structure so it demonstrates good practice by having a centralised set of procedures for how to conduct supervision activity. Publication of these procedures provides transparency for RUs/IMs.*		1	1	1			
I	Rail	D	"Traditionally, we're focused on technically oriented supervision… there is always a discussion whether to focus on process or on the product, if you may distinguish it like that. We do many product oriented or technically oriented inspections. That's what we did in history and we think it's also necessary to decide process oriented supervision because it's… important to do a certain number of inspections, really technically checking the stage that it's on – product, whatever you may find.						1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			There are other countries which focus more on the process level, which don't really go out and check the state of wagons or technical state of this or that product. We focused on that in the past. We have shifted a bit towards company oriented — process oriented on a system level — supervision activities. So the shift or the share between these two has also shifted inside EBA but I think, compared to others, we still do many of these product related actions. I don't know how far that will go. As I said, there was a shift. We have seen it align in process oriented at system levels, supervision, auditing the SMSs or the undertakings, but I don't know how far that will go and I think not all the technical inspections can be, as you said, devolved to RUs/IMs or taken out of what the NSA does. It's for us checking the outcome of the SMS and how effectively does it work. And it is for us to make maybe even random checks on the ground to see if it's really delivering what it should. If they [the RU or IM] have a very effective internal monitoring, which you have checked once and you have considered to be very good, then maybe you can do a bit less in that area as you would do in another undertaking where this is not yet perfect or in a good state." *Our opinion: With regard to the level of technical inspection, the NSA did acknowledge that RUs/IMs are expected to be responsible for checking that their own SMS delivers the required outcomes (which would include technical inspections to ensure equipment is safe). However, the NSA was reluctant to devolve its previous responsibilities for this suddenly. It currently combines SMS-based supervision with technical inspections, which may be a greater draw on resources and may not incentivise RUs/IMs to take on full responsibility for safety. The NSA does plan its technical inspections in accordance with the knowledge it has of the RU/IM's own internal monitoring processes so if these are considered to be good then the frequency of technical inspections may be scaled back. The forthcoming CSM on monitoring was expected to assist with the transition of responsibility as it places greater emphasis on RUs and IMs being responsible for monitoring safety outcomes.*							
I	Rail	F	"We will employ the systematic audits for… a railway undertaking or an infrastructure manager, or even someone that wants to put a new system into place, a promoter as we call them. We do systematic audits six months after they've begun effective operations, and that applies to all operators, notably railway undertakings. So we treat them all the same and there are some very large railway undertakings and some very small ones as well. But six months after they've started, so that's where we think we are consistent and also proportionate because when a new entity starts	2	2					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			up, the fact that it's new can mean that there may be a higher risk than a large entity, which has perhaps got more of an organisation behind it. There are two types of inspection… An inspection which comes about because we've identified what may be a problem from our database. And other times we will do inspections where an audit has not had very good results for the entity audited. And there we may decide to do a follow-up inspection from the audit, but that really is based on the results of the audit. Audits tend to be systematic and inspections are chosen according to the risks that we've identified, which would include perhaps a result of an audit which weren't what they should have been or could have been." *Our opinion: The NSA consistently audits new RUs/IMs six months after they start operations. This approach is also stated to be proportionate as it reflects that the (lack of) experience of an RU/IM is a factor in its safety. The use of inspections to follow up an audit suggests that the audit process itself is defined as a document-checking exercise with inspections being the stage at which an RU/IM's frontline operations are checked.*							

Table B.23: Supervision practices: audit methods

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	NL	"I'll come to an audit, it can be to translated as an assessment, it is trying to understand the way the company has organised its processes to check whether those processes are organised, and that can be done by interviews, but also… with staff, but also by sending documents so that's also a way of supervision. What I meant by investigation we also do accident investigation next to the safety investigation board, we do the little incidents. If we discover in an investigation that there is something wrong with for instance… well, the maintenance, it always goes back to maintenance. But it can also lead to the conclusion that there's something wrong, and with the SMS. And inspection is also a term we use for all kind of things. We use this term for all kinds of supervision. So the audits are the ones we do when we give the Certificate, but we can also do it in between, and the same applies for the investigations and the inspections. We will do them whenever we think it necessary." When interviews are used, they include all levels in a company: "From the directors, the ones on top of the… and also the ones on the floor, on the workshop, and not only the safety managers, because they often know a lot about safety and about the safety directive and the Safety Certificate, but we want to know whether it's all through the whole organisation, the safety awareness and the safety knowledge. So it's not… we always ask an organisation chart on the basis of that chart we plan our interviews. Yes, sometimes we talk with the safety people and sometimes with others." *Our opinion: This is a demonstration of core good practice. The audit methods include interviews, document checks and frontline inspections. Interviews are planned to ensure that staff at different levels of the RU/IM are interviewed.*						2	
I	Rail	DK	"Now that we supervise the companies we are very aware of doing audits that could result in added value for the company. They will almost have the feeling that they've learnt something after supervision or during supervision. We of course identify areas where a lot of companies or many companies are not performing well so we do a special effort on having that as an item on their supervisions and have a dialogue on how they are performing on that particular issue. And then every time we visit the company we will make sure that half a day is spent on this very topic. We try to make it some kind of cooperation between us and the companies and not two opposite fronts. We call it dialogue based audits." *Our opinion: A good practice approach to audits is to use them as an opportunity to help RUs/IMs*			3			2	2

<table>
<tr><th>I/D</th><th>Sector</th><th>MS</th><th>Examples</th><th>Proportionality</th><th>Consistency</th><th>Transparency</th><th>Accountability</th><th>Cooperation</th><th>Targeting</th><th>Prioritisation</th></tr>
<tr><td></td><td></td><td></td><td>improve. Strengthening RUs/IMs is the stated short-term target of this NSA and its approach ensures that areas of weakness for the industry and/or specific RUs/IMs are subject to scrutiny and specific guidance.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>I</td><td>Rail</td><td>DK</td><td>To summarise the distinction between audits and inspections, the NSA publishes the following table in its strategy:
<table>
<tr><th></th><th>Audits</th><th>Inspections</th></tr>
<tr><td>Focus</td><td>Process-oriented
‘Top-down’</td><td>Object-oriented
‘Bottom-up’</td></tr>
<tr><td>Purpose</td><td>Certification of the undertakings’ management systems, so that the ability of the undertakings to manage their own risks is maintained or enhanced.</td><td>Intended to create transparency concerning a particular theme and initiate improvements relating to this theme.</td></tr>
<tr><td>Process</td><td>Review of the undertakings’ safety management systems, which covers the entire system over a predetermined period of time.</td><td>Sporadic checking of a specific theme within one or more undertakings.</td></tr>
<tr><td>Contribution towards outcome target</td><td>Directly derived from the short-term outcome target. Expected to contribute to the outcome targets to a greater extent than inspections.</td><td>Expected to contribute to the outcome targets to a lesser extent than audits.</td></tr>
<tr><td>Method (one or more of…)</td><td>Document review
Functional inspection
Desk-based inspection</td><td>Functional inspection
Desk-based inspection</td></tr>
<tr><td>Resources used for each individual inspection</td><td>60-90 hours</td><td>16-24 hours</td></tr>
</table></td><td></td><td></td><td>3</td><td></td><td></td><td>3</td><td>3</td></tr>
</table>

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			<table><tr><td>Ratio between the total resources used in TS Supervision.</td><td>80 %</td><td>20 %</td></tr></table> This table is based on the last strategy and the proportion of proactive supervision (audits) and reactive supervision (inspections) has altered so that now 90% of time is spent on audits. This is based on reacting to all incidents where necessary. *Our opinion: It is good practice to explain to RUs/IMs what is involved in each process and to summarise the key differences. It is also made clear that audits are a priority activity and occupy up to 90% of the NSA's available time for supervision and require substantially greater resources.*							
I	Rail	DK	"As a principle, might not always, but in 99% of the time, we have two auditors at the same supervision and they are shifting. We do not have fixed couples. So we have a rotation, making sure that we have adjusted on a continuous basis the way of doing the audit. We do not have a written evaluation procedure but we have these shifting partnerships, you might call it, doing the audits to make sure that we perform the audits in the same way." *Our opinion: Regular circulation of staff is good practice as it will help to create uniformity in the approach to supervision.*		3		3			
I	Rail	DK	"To check a part of a safety management system will not provide an objective testimony about, if the rest of the RU is incompliant. So, if I check one element in the safety management system only, it will not give me evidence that the whole management system is incompliant or is effective. That is why we actually go through the whole safety management system for the duration time. Critical issues, we do every year. We have picked items that we think are critical and we go through those every year. And the rest are on a five year basis. A lot of other countries will say, 'well, we have checked this and that looked good so we don't check it again'. And I think that's a risk." *Our opinion: Through its system of distributed auditing, this NSA will not only check the entire SMS at the point of assessment/reassessment, it will also ensure a full check is completed during the validity of the certificate/authorisation. In addition, safety critical issues, as identified by the strategy and/or supervision experience, will be targeted for annual checks. This would appear to be good practice and strikes a balance between auditing the entire SMS every year and auditing only parts of the SMS for the lifecycle of the certificate/authorisation.*		2				2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	A	The Austrian NSA uses an accredited body to certify the SMS of an RU/IM: "For part A for the safety management, the certification of the safety management, we have an accredited body that does this. So for this of course within the accreditation procedure he sees the first certification for the safety management system and then this accredited body will also examine [the SMS] yearly." The NSA was asked about the level of interaction it has with the accreditation body: "There are with these accredited bodies informal meetings. We're also exchanging information. For instance, now with the new regime of the regulation on safety conformity assessment that they also have to… consider the Annex two which is available for part A certificates, and so this is something new they have to consider in their accreditation process. There are some meetings to bring this to their notice." The NSA is therefore not involved directly in the initial assessment of the SMS for the Part A certificate. If there are flaws in the SMS, the accredited body will discuss these issues with the applicant and will not issue a certificate until they are resolved. "Only if the accredited body says he can't issue a safety certificate it will come to the [NSA]." The NSA did not recall any examples where the accredited body brought issues to the attention of the NSA after certifying an applicant's SMS. The NSA stated that it gains a more detailed understanding of an RU's SMS when it considers the application for a Part B certificate: "There is always part B. Part A is done for undertakings which are situated in Austria, so we have a step before. We have to have an application for the general authorisation to take up operation and so we know them already, and then this is done by a third party, this certification. But they come to us with part B and they have of course the general processes they have to describe and transform them to part B, so it's not given that something is done by [the accredited] body and we don't have any connection with it. So, because if we have some doubts about part A, or because we see when they try to put it into force on a certain infrastructure for part B that there might be some problems within the processes, we could, for instance, require them [the accredited body] to send us the audit protocols." *Our opinion: In this example, the NSA may become detached from weaknesses in the SMS at the*				-1		1	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			application stage that, whilst not sufficient to prevent certification, could direct planned supervision activity. The use of an accredited body appears to distance the NSA from having a detailed understanding of each applicant's SMS. Whilst the Part B certification process will provide some insight, it is not designed to encompass a detailed assessment of the SMS as with Part A.							
I	Rail	BG	"By checking the elements of this safety management system… we audit the system itself. And then we check how the Railway Undertaking itself complies with, or applies its safety management system. For example, implementation of plans or execution of plans, different programmes for training of staff, or development of the system, the legislative needs of the enterprise itself. Also during these checks by the inspectors, if there are identified deviations, then we check this part of the safety management system of the Railway Undertaking, which is where the deviation has been found." *Our opinion: The NSA reports a process that shows a fundamental understanding of the SMS-based approach to supervision.*						1	2
I	Rail	S	Supervision/audit 'checklist': the NSA uses this checklist to guide its inspectors when carrying out and reporting on supervision activities. "It's headlines and thoughts from the Safety Management System; what evidence we see when we are out making audits on the policies, on the risk assessment, on the competence management system, on taking care of accidents, and so on. And then we have some points related to Swedish regulations about Safety certificate Part B where we are asking about the evidence in this check-list about assessing competence, health, about vehicles maintenance, about rescue plans and so on. So this kind of check-list we are using when we are making audits, but it's also an input for the staff assessing applications for certifications." The RU department is consistent in its application of this checklist: "We say they have to have everything [in the checklist]... A small company has to have some kind of answer on every point in the regulation… but it could be a very short answer… [like] the staff are taking the phone or going to the office and inform the manager. In other bigger companies they have to have a special [reporting] system for that. We can evaluate [at] different levels, but they [RUs] all have to have all levels." The IM department uses the same checklist but exercises flexibility in how it is applied:		1	1			1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			"They have the same check-list, because the check-list is an internal rule for the Agency, but… [differ in] how they evaluate the different Infrastructure Managers size and traffic and how many staff they have. So they said, 'all right this you should have, but you don't need to have that and that and that, because you are so small'." *Our opinion: It is good practice to have a system for inspectors to use that will guide them in their supervision and the structure of their reports on such activities. The RU department of the Swedish NSA is also demonstrating good practice by applying the checklist consistently; whilst it accepts that the extent to which each item is covered by an RU may differ based on the size and type of operations, the RU department is firm in expecting all items to be considered. The NSA as a whole demonstrates poor practice by not ensuring that the checklist is applied with the same consistency and intensity by the IM department. Again this sends mixed messages to the market and is not conducive to safety or market access.*							
I	Rail	S	"We can choose to make audit over the whole safety management system or we can choose to only check one part of the safety management system. Then we of course have interviews at the audit with the management, with staff and checking evidence about maintenance or evidence about education and so on. We can go to another step where we interview staff. We can go to see if the system is working all the way out. At the audit, we interview train drivers, we can interview people working on the train, we can interview people working with the maintenance to see how they knew the system and how they can share if they feel something is going wrong or something difficult with documents or how they report accidents or how they report if they see other things. Where they get information and they have to show that they are the right documents. If they have on the intranet they show us how they get the information, how they share information and we can see if the system is working. Subcontractors is the one way to check if the safety management system is working but are used because the RU is responsible for the subcontractor and also the Infrastructure Manager and we can check does the subcontractor know about that. Has he the right information. Has he documentation from the RU or IM or has he something else because it's difficult to be a subcontractor because one week you are at one company and another week or another day you are at another company, but you have to follow each company's different rules. So do they know that and have they competent management system and do the RU at the beginning		1				3	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			have the information and how they share information with different subcontractors." *Our opinion: The NSA describes a comprehensive audit process that addresses a range of levels within the organisation, including subcontractors. The description suggests that the NSA has a clear focus on collecting evidence that the SMS is functioning and understood by staff. The NSA has recognised the particular challenges faced by RUs/IMs in ensuring that subcontractors follow their SMS.*							
I	Rail	CZ	In carrying out an audit, the NSA will usually interview only management at an RU/IM. It will visit both main headquarters and regional offices of an RU/IM. An audit will take approximately 1–2 days. *Our opinion: It is not good practice to interview staff at only management levels in an organisation.*						-1	1
I	Rail	PL	The NSA has conducted a total of 7 inspections that have included assessing some aspects of the SMS but only one has been a full (pilot) audit of an RU/IM's SMS. The audit was abandoned part-way through because the RU protested that there were insufficient legal grounds for conducting an audit. In conducting these audits, the NSA did learn more about the safety culture of RUs/IMs: "In our experience, there's extreme weight attached to the commercial aspect at the cost of any other aspect and if there's any imperfection in the laws or if the laws allow different interpretations, of course, it is used in such a way as to make life easier for the commercial entity, which means limiting the actions in the field of safety as much as possible. One of the conclusions from the seven inspections conducted last year was that the new approach also requires a change of mentality in the general approach to the activities, to the operations because the introduction of SMS forced the railway undertakings to adopt a process-based approach. For many of them, it was a considerable change. Doing it properly simply requires a lot of goodwill on the part of the management because it can be empty documents. We found two of the enterprises which had model implementation of the SMSs and one of them did have some experience with other management systems, like quality management system or health and safety systems. They said it helped. Whereas the other did not have any experience at all but in that case, everybody in the company was aware of the significance, from top management to simple employees. Everyone knew what this was about. I think that would be how important the change in mentality was, in that case."						2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: The comments reveal that the safety culture of rail markets can vary considerably and it is desirable for NSA to promote a safety culture so that it is not seen as a second priority to commercial factors. The NSA itself has recognised that SMS documentation alone is not a clear indicator of the safety culture in an organisation – much of this is embedded in the way staff operate.							
I	Rail	E	As part of its audit process, the NSA does not appear to conduct interviews with a wide range of staff at RUs/IMs; instead it focuses on, "…people with management competences related to safety, related to safety engineering and safety operations, and they have people that we know and that people we have with a long background and they are authorised people of these RUs and IMs staff. We know them from a lot of years and they are of our… they are very, very reliable for us." *Our opinion: To establish the extent to which a SMS is effective, it is good practice to interview staff at all levels in an IM/RU to explore how well the SMS is understood and followed. By selecting staff for interviews that the NSA are familiar with, and who may have an unusually detailed knowledge of the SMS, it may not collect sufficient evidence of the SMS for audit purposes.*						-1	
I	Rail	DK	The NSA emphasised that its approach is focussed entirely on supervision of the SMS used by each RU/IM: "Just underlining that our way of looking into this is to be able to supervise a safety management system and by incident this is in the railway industry but it's the safety management system as the first and most important and then it happens to be the railway industry. We are looking into what is the main object and we are not in doubt the main object is the management system. I would say in other words we don't check the nuts and bolts but we do check that the companies are checking the nuts and bolts." *Our opinion: This NSA has clearly adjusted its entire culture so that it is aligned with the European safety regulatory framework. It is good practice to adopt fully the SMS-based approach to supervision, rather than running a mixed supervision regime.*		1				3	
D	OSH	DK	Descriptions of the supervision process online – the stages before, during and after an inspection are described according to company size. This includes the duration of the visit, which increase with company size. *Our opinion: It is good practice to provide clear instructions to dutyholders about what they should do, how they can prepare, what demands an inspection will place on their workplace and what will happen*	2	2	2	2		3	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			afterwards. *It is also good practice to consider how resources may differ according to the size of the company that is being assessed. In this example, a longer process exists for larger companies and the safety authority specifies the typical number of days spent on each audit depending on the size of company. NSA may benefit from reviewing the duration of previous audits in line with dutyholder size and establishing whether there is a consistent trend in how long an audit takes for dutyholders of different sizes. Not only will such information help the dutyholder to be consistent in future (and better plan its resources), the same information could also help dutyholders know more about the timescales for assessment and the impact on their business.*							
I	Rail	GB	"We get line managers to make sure that [investigation plans and processes are being followed]…on a regular basis. They're on a maximum of a monthly basis… will monitor progress with those investigations on a monthly basis: are they going, are they progressing, are they being done in a timely way?" *Our opinion: A monitoring process by senior inspectors on a minimum of a monthly basis is good practice. This ensures that progress with current investigations is consistent and allows issues to be identified during the investigation, rather than once it has ended. Together with team surgeries to discuss enforcement decisions, the two approaches achieve consistency on two levels: one level monitors the ongoing progress and process, and the other level reviews the initial decision and overall case report.*		1		1		1	
I	Rail	A	A typical audit will take 7–14 hours. If staff are interviewed, they will be selected from all levels in the organisation. *Our opinion: It is good practice to interview staff at all levels.*						2	
I	Rail	S	"When we see it [an RU] misses something, or we want the companies to take care of something, we send out letters with a clear view of what they have to do to reach the level of regulations, and they have to answer in a specific time. Usually it's one month – three or four or five weeks – and I will check the answer is very often some evidence, perhaps a new documentation, risk analysis, or something else like we want to evidence. Then we try to evaluate the information and see if we think they have reached some of the steps to the goal and then it's probably most times it's all right, but sometimes we pay another visit or audit, so we can see that they have made the steps like we set out. Letters will often raise with the RU points of non-compliance from audits – if not, the correspondence		1	2			2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			will be regarding incidents: "If we have been on audit then… we have every non-compliance matter in the letter we are sending, every point that's corresponding to the Safety Management System or the regulations that we see. Otherwise we can also… take input from accidents. We take input from the National Investigation Body. We take input from people outside seeing, giving us information about some difficulty with different companies and we try to evaluate and see the risk. And some of them it could be all on a level with that we… why we say we knew that your passenger train had an open door in traffic; what have you taken for kind of measures to secure that it's not going to happen again, and how are your investigation about this? And then they have to respond in some weeks and let us know what have they done? Have they worked with special information for staff or is there a technical problem with the part and so on: what is it? That kind of an example." The letters are equivalent to enforcement notices: "When we are out on an audit, or when we are sending letters to RUs or IMs… there we have no common light version, there we only have the legal means in our decision. This is non-compliance; you have to change that and that. And in the letters we are not telling them you are a good company, and you have a good audit on this, and so we don't have that kind of letters. We only have a very clear letter where we are saying this is non-compliance." *Our opinion: The audit process considers a range of inputs and delivers requirements for SMS adjustments that have to be complied with within a specific timeframe. The approach is consistent and transparent.*							
I	Rail	S	A full audit of an RU is typically conducted by two people who will collectively dedicate approximately 200 hours to the task. This includes approximately 32 hours (2-3 days each) spent at the premises of the RU. *Our opinion: Comparatively the time allowed for a full audit seems to be greater than that allocated by several other NSA.*							2
I	Rail	E	Each audit lasts approximately one month: "We receive the documentation from RUs/IMs. We make a first assessment about one or two weeks. Then we propose an interview and from this interview we will, we make a new assessment and we							2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			analyse our document, and then we propose then a second interview and finally we share our information. It used to be about one month." Approximately eight people from the NSA would be involved in each audit. *Our opinion: The audit duration and size of the team seems substantially greater than for other NSA.*							
I	Rail	D	"There are regular coordination meetings where all the lead auditors or the ones dealing with the supervision activities meet to share their experience and develop a kind of harmonised approach. So they meet two days somewhere in Germany because they are spread all over Germany and they come together and discuss and exchange. As I said, a kind of harmonised approach shall be developed or is developed. [The frequency of these meetings] differs from subsystem to subsystem but I think it's at least twice a year. There is a kind of written notice that is spread to all the participants and stored for future consideration, future activities." *Our opinion: It is good practice for those carrying out supervision to discuss their approaches and reach a common consensus on the methods and decision-making practices that should be followed. The frequency of these meetings varies because the NSA organises its supervision and enforcement by different subsystems. It is also good practice that the meeting outcomes are documented and can influence NSA procedures.*		2		1		2	
I	Rail	D	"For an audit we normally would announce to the undertaking that we intend to do an audit, where, when and on what issues. We would ask the undertaking to provide the necessary stuff, documentation and whatever. We would set up a team of auditors and then... go out and visit the undertaking and there you can interview staff, review documents, ask for more documents, go out and check what the staff is really doing, enter the premises. I won't say whatever he likes to do but he has a broad variety of things that he can do or he can ask the undertaking to do." The NSA stated that interviews can be with staff at any level in the organisation. *Our opinion: The audit procedure combines document checks with inspections and would appear to follow good practice. The NSA informs the RU/IM in advance which provides transparency.*		1				2	

Table B.24: Decision-making approaches

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	GB	The HSE's principle tool for achieving consistent and proportionate supervision and enforcement is the Enforcement Management Model (http://www.hse.gov.GB/enforce/emm.pdf). The model is defined graphically as a flow diagram and then each element is explained in detail. The steps involved are as follows: • Set priorities for action (based on regulatory contact, the strategy and the type of risk). • Assess the actual risk. If it is serious, there are legal options for immediate action, such as a Prohibition Notice. If not, the Model procedure should be followed. If the risk is serious, the Model procedure may still need to be followed after immediate action has dealt with the serious risk. • Risk gap analysis: compare the actual risk to the benchmark risk (based on being compliant). The difference is the risk gap. The risk gap must be used to determine what level of enforcement is necessary to bridge the gap and also whether prosecution should be considered. The differences can be hard to quantify so descriptor categories are often used based on likelihood, consequence and extent (i.e. the number likely to be affected). • Initial enforcement expectation. "This is the enforcement action solely reflecting, and proportionate to, the risk to health or safety or the seriousness of any breach of the law." A colour-coded table of enforcement action is provided to assist inspectors with selecting appropriate initial enforcement action based upon the size of the risk gap and the status of the laws/standards that have been breached. • Dutyholder factors are "specific to the dutyholder and their activities, and usually confirm the initial enforcement expectation or alter the action up or down the hierarchy by one level". Factors include incident history, previous supervision/enforcement action, deliberate economic gain, actual harm, general standards, and confidence in the dutyholder. Decision charts are provided for several factors to help inspectors select appropriate enforcement action that is proportionate and consistent. • Strategic factors are also an important consideration. Such factors include public interest, impacting on vulnerable groups, expectations of sustained compliance, the message to other dutyholders, likelihood of achieving the benchmark, the functional impact (e.g. unemployment), and compliance with strategic policy. Again a decision chart is provided to help inspectors navigate these factors. *Our opinion: Collectively, the Model demonstrates good practice in providing a systematic approach to enforcement that, if followed, should deliver proportionate and consistent enforcement action. Decision*	3	3	3	3			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			trees and colour-coded tables and risk matrices are accessible tools that can be used to deliver consistent and proportionate decisions. The process itself is constructed of a series of steps that help to address the somewhat qualitative, subjective nature of supervision and enforcement by encouraging inspectors to make decisions based on categorical hierarchies. *The use of a comprehensive model for decision-making helps to remove variations from the process. Every enforcement decision is structured using the same framework and consequently some restrictions are placed on individual decision-making. However, there is still freedom and flexibility in the decision-making process: users of the model can consider variables that may affect the enforcement decision at which they ultimately arrive. The EMM describes these variables to some extent and encourages users to record how and why they have deviated from the model where appropriate.*							
D	OSH	GB	Enforcement Management Model (http://www.hse.gov.GB/enforce/emm.pdf) is: "a logical system that helps inspectors to make enforcement decisions in line with the… Enforcement Policy Statement (EPS)". The EMM: • provides inspectors with a framework for making consistent enforcement decisions; • helps managers monitor the fairness and consistency of inspectors' enforcement decisions in line with HSE's policy; and • assists less experienced inspectors in making enforcement decisions. It can also assist others (e.g. those directly affected) in their understanding of the principles inspectors follow when deciding on a particular course of action. The EMM (with additions) is used by the GB NSA. "The processes only set out what we expect people to do, only in terms of what they should be doing in terms of processing a case. It won't give them any indication of what the answer is in terms of enforcement action, and I think as an organisation we've taken the view that we should never write that sort of thing down." *Our opinion: The GB NSA has modified a procedure used by the GB OSH authority to fit the rail domain. It is good practice to share fundamental procedures and policies across domestic authorities and tailor them to specific circumstances.*	3	3	3	3			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	GB	Enforcement guide (for inspectors): the HSE publishes on its website the enforcement guide that its staff are trained to follow. This documents in detail the processes that inspectors must follow in order to enforce within the law. This includes how to investigate and present a case in order to secure a prosecution. Publication of the guide demonstrates good practice by sharing the policies and procedures that must be followed to bring about a prosecution, helping to satisfy the principle of accountability. *Our opinion: It is good practice to publish the guidance and policies by which the NSA operates.*			2	2			
D	Rail	GB	"It's that balance of how extensive is that risk that you're looking at, against how much confidence do you have in the duty holder's safety management regime and their application of that regime because you could have quite a significant breach that the duty holder really hasn't picked up on, but if they're capable and confident as a duty holder to… recognise this is a major mistake… mitigate all that risk and… have a mechanism in place in a short, very short period of time that controls that risk. We'll probably walk away going that's really pretty good. Equally, on the other hand you may find exactly the same risk in another duty holder and they go, do you know what, I'm not going to touch that with a bargepole, at which point the inspector will be balancing that risk with the response and approach of the duty holder and say… that's just completely unacceptable. We've got to resolve the problem. You're clearly not willing to act. We will make you act through whatever mechanism we deem fit. The difficulty is if you start to write down all the risks, you'll end up with a huge great book of risks that if you've got an x, do y. Well, that doesn't work. What you need to be able to do is train your inspectors to understand and communicate that… the extent of risk and the confidence they have in the duty holder to be able to make a judgement of what we want. We want that risk mitigated. How do we achieve that through the best means, and if that means the duty holder does it just like that, that's fantastic. If it means we have to utilise one of our enforcement tools, that's fine, either way the risk is mitigated and that's what we want them to be able to do for whatever risk they see." *Our opinion: Focus of enforcement action is mitigating the risk through the fastest and most efficient means. The decision to use enforcement action is based not simply on the breach that has been observed but also the RU/IM's response.* *It avoids a process whereby all risks are listed alongside the 'appropriate' enforcement action: this can*	1	1					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			remove the need for judgement on behalf of the NSA staff and thus reduce both staff morale and the quality of staff who perform supervision activities.							
D	Rail	GB	Enforcement decisions are made by one person. The decision may be checked and approved by other staff—and the NSA has an independent review process to ensure that decisions are checked by someone who was not close to the investigation—but the decision itself is always made by a single person and never by committee. *Our opinion: Empowering a single person to make an enforcement decision can be considered good practice in that it is a transparent process and achieves accountability because decisions can be traced back to the source. Often a case will be investigated by one person so it is desirable if the individual who is closest to the facts is also responsible for making the enforcement decision. A process of review is important (particularly by a legal professional if the outcome is set to be prosecution or similar legal action); however, in this example, the review process is a check of the reasoning that has been applied. There is a risk that decisions by committee may be swayed by the most senior staff present, or may not be based on all the evidence available. It should be noted that some Member States have legal regimes that may hold individuals legally liable for the decisions they make: this may affect the decision to adopt the practice of empowering an individual.*			2	2			
D	Aviation	IRL	The formal process for how compliance failures and appeals are processed is fully-documented in a decision tree. *Our opinion: Graphical representation of decision-making structures can be a helpful quick-reference for staff and this is a good practice approach to formalising a decision-making procedure.*		2	2				
D	Rail	GB	"There's a couple of other things as well… one of our colleagues runs some surgeries for team managers where they'll go round and discuss issues that they've got about cases and you might feedback… to the team managers so that they understand where things are going. When notices are served, [the senior inspector] will always do some feedback to the person who's served the notice and by doing that he gets a view of what sort of issues are coming up and how they're being dealt with across the organisation." *Our opinion: Measures to improve consistency and proportionality are welcome. Team surgeries are an essential element of the EMM approach: the decision-making process is devolved from senior management so regular surgeries ensure that the link with management and peers is restored. The discussion is always focused on the decision-making process; this is assisted by each case following a*	2	2		2			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			defined structure and being reported according to that structure. It is desirable for outcomes of these meetings to be recorded if they have learning points for future supervision and enforcement activities.							
D	Rail	GB	Line between legal and non-legal enforcement: Enforcement decisions through the EMM are based on an initial enforcement decision that can be modified by RU/IM factors and strategic factors. However, the model only permits these factors to enable the enforcement decision to be increased or decreased in severity by one level. There would not be a situation where the model would recommend reducing a prosecution to verbal advice, for example. The EMM encourages inspectors to consider these factors through a number of decision tree diagrams. However, they are not to be followed rigidly. *Our opinion: It is good practice to permit escalation or reduction of the initial enforcement decision to account for other factors. This is a process that helps maintain proportionality between enforcement and risk. However, the process is limited to adjustments of just one level in the enforcement decision. This limit introduces consistency: for example, an RU/IM cannot have an initial decision to prosecute reduced to verbal advice by other mitigating factors. The application of this process involves a decision tree and broadly defined criteria to guide staff when considering factors relating to the RU/IM or the NSA strategy. This approach helps the NSA to deliver a spectrum of enforcement action, from 'influencing' behaviour to 'forcing' behaviour without sacrificing a structured approach to ensure consistency and proportionality.*	3	3					
D	Rail	GB	No adjustments for large RUs/IMs: specific guidance on the interpretation of the EMM has been issued for large IMs. Although spread geographically, the EMM guidance encourages inspectors to still think about the IM as a single entity, not a collection of regional or distributed bodies. *Our opinion: The purpose of supervising the SMS is to ensure that organisations have the processes in place to operate safely and responsibly irrespective of their size. In a large entity, a substantial part of the SMS will be devoted to ensuring that devolved partners and regional centres operate under the same SMS. It is not good practice for enforcement decisions to be directed at parts of a single entity: a good SMS will be at the centre of the entity and its executive management should be able to respond to any enforcement decision, even if the breach has occurred in a devolved part of the organisation.*	1	1					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	NL	One NSA summarised its approach to enforcement on its website as "Where it can be, soft; hard where necessary". This was explained by the NSA: "The soft measures are, if they work, they are more pleasant for everyone, not only for the company, but also for us and the inspectorate, because it doesn't get any legal mess, and if you can enforce some behaviour because of a visit to the company and having a cup of coffee over there and talking about how things should be, and the company says, "yes, you're right about that, it sounds reasonable." And the company does what you expect of them, by drinking the cup of coffee with them, that's okay. Then you have reached your goal without using a lot of people or finance, and the legal stuff, so it's always better to use soft measures. And then I give you the example of drinking a cup of coffee because that's the one we always use, because I come from an unfortunate role. My former job was really enforcement, so I had to get used to the drinking of cups of coffee. I've said that's not enforcement. That's not real, but that's soft. That's too soft, but now I'm convinced of the working of soft measurements and that they can really work, that they really can be effective." When defining the point at which the enforcement measures would become stricter, the NSA explained that: "As an inspectorate [we] have a certain relationship with the companies, and with that relationship goes a softer way of… So sometimes it is thought to be not fair to use the harder way for enforcement. So it's difficult to point the exact point of turning to harder [enforcement]. I suppose that we will use the harder enforcement ways when the softer ways don't work anymore. We always, even before we give the hard way, we always give a warning. We never give a legal measure without warning the persons, so it's never a surprise for the company that they're punished with administrative sanctions, so there's always a warning, or when there's a need to highlight danger, of course. Not very often we've had… to give a sanction without warning, because we thought, if we're going to wait, there will be a derailment, and we don't want to have that. But there is a point of turning in the warning, of course. The higher the risk, the more direct measurements and harder measurements are needed if we want to put out of service a railway company… That has never happened, but a railway vehicle—that has happened—then we would do what we think is necessary to take it out of service now, and also with the infrastructure manager, if we think the infrastructure is not okay, if it has a great risk for derailment, or other accidents, we forbid them to use that infrastructure. We have done that."	2					2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: A risk-based approach to enforcement is described here, with serious safety hazards being subject to the level of enforcement necessary to ensure safety. However, the general approach taken is to use the softest measures available to achieve compliance, and only switch to stronger methods of enforcement if the softer approaches are not effective or if there is an immediate risk to safety. If safety is not compromised, this approach could be considered good practice with the caveat that it must be administered consistently (which requires the other measures that this NSA has such as peer reviews of decisions, as well as a documented approach to ensure that all staff work to the same principles).							
I	Rail	NL	Decision-making is by two people and is checked by senior staff for legality. "I don't think they sit together behind the computer. I think one of them will be a judge, but not really being a boss but being the actual writer, and the other who reads it and commands it. And then for the boss who wants to say something, and usually I come in there, and I add something; whether it's legally allowed." *Our opinion: If decision-making is shared, it may be good practice if one individual has a lead role in the process. There appear to be benefits to empowering individuals with decision-making.*	2	2					
I	Rail	DK	"We have two roles: we are a certifying body issuing certificates – safety certificates and approvals – and then we are the safety authority. The first role is only based on management, safety management system, and... if we find non-conformances, we will ask the company to correct it, the safety management system. If we see something that is a hazard, a critical safety hazard, then we will immediately turn into the safety authority. Then we will give provisions and bans and that's the way we make the proportion. Our response will depend on how critical it is, how big is the hazard, and that will be our judgement. We don't have many steps in our... We don't have a long response staircase or whatever you call it. We give a prohibition or a ban and say, stop this activity right now, get it fixed, that's it. We don't have... If it's a safety hazard, then we go in full. We don't have an [escalator for decision-making]." *Our opinion: the NSA reports minimal options for escalating its response.*		2					
I	Rail	DK	To achieve consistency in decision-making, this NSA has weekly meetings: "What we do is the inspectors or auditors once a week have a meeting where we discuss these kinds of things and we will... If we have non-conformities, bans or have made some kind of enforcement, we will discuss at this meeting what were the circumstances and why did we react as we did and that should	2	2					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			give us some kind of... to bring us up on the same level, I think." *Our opinion: This NSA has five staff so weekly meetings are a feasible forum for exchanging perspectives on recent activities.*							
I	Rail	DK	There is flexibility in who is responsible for making an enforcement decision depending on several factors: • If the non-conformity or hazard is identified during an audit, the two-person audit team is likely to decide jointly on the action they will recommend. • If the audit team is at the NSA offices, then "We have the legal department, we have a lot of people and we will make a joint decision." • If the non-conformity or hazard is identified off-site at the premises of the RU/IM, a decision may be made there and then by the lead auditor. Auditors are authorised to issue bans/prohibitions immediately and on location if the real or potential safety hazard is sufficiently serious. *Our opinion: Decision-making processes may vary depending on the severity of the safety hazard. Decision-making appears to be carried out jointly or with reference to other colleagues if staff are at the NSA's premises; however, if on location at an RU/IM, decisions may be made without reference to collective knowledge. However, such decisions will only be made if there is a risk to safety, either potential or realised.*		2		1			
I	Rail	DK	The NSA Director is available for all staff to call upon to check their decision-making if they are in any doubt. *Our opinion: It is good practice for decision-making to be open to review and comment.*	3	3					
I	Rail	DK	This NSA supplements weekly meetings of inspectors with regular sessions to discuss enforcement decisions – e.g. why a ban, observation or non-conformity was issued. *Our opinion: It is good practice for decision-making to be open to review and comment.*	2	2					
I	Rail	DK	Between the three enforcement measures used by this NSA (observations/remarks; non-conformities; orders/bans), there are 'grey areas' at the borders of each measure. "They will always be should it be a ban or should it be a non-conformity and should it be a non-conformity or should it be an observation? Every company will from time to time have non-conformities, also the good. If they are not done as they actually should, we state it in our audit and they will have a	2	2					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			non-conformity. If they are almost there but not quite, at a well-functioning [company] it will be an observation, at a not well-functioning [company] it will be a non-conformity." These grey areas, particularly the border between a ban and a non-conformity, are often the subject of discussion at the weekly meetings of the NSA. These discussions do not change the definition of each measure but are used to understand the circumstances in which a particular measure might be appropriate. *Our opinion: It is good practice to recognise where there can be difficulties with decision-making. This NSA is regularly reviewing how decisions are being made to provide insight and consistency for future decisions.*							
I	Rail	DK	"The lead auditor will issue the safety certificate or safety approval to the company but before that we have to put the case, the whole case, before a Certification Committee. The Committee will consist of our boss and another auditor who hasn't been involved with this audit and they will make sure that... everything is current and has been done correct[ly]." *Our opinion: To ensure consistency and proportionality at the award stage, the NSA has a Certification Committee to review application decisions.*	3	3					
I	Rail	A	To be proportionate, this NSA stated that, "we consider which risk arises or which failure, for instance, has developed in the undertaking and to compare it; what would be the result or how we should react to this." The NSA is currently developing a procedure for enforcement decisions but the primary factors it considered appear to be: • Inspector experience • Examples from previous supervision activities • Proposals made by the NIB (if an incident has occurred) • The potential or actual risk to safety This will change in the future: "We don't really have a table, for instance, or a checklist where I can look through at the moment. That's just in development also. But it's simply, at the moment it's mostly based on the experience of the experts." *Our opinion: These are positive steps towards a consistent and proportionate decision-making*	2	2					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			approach. The NSA is aiming to introduce a procedure for decision-making that captures the range of factors that should be considered and the way in which these factors may affect the decision.							
I	Rail	A	To deliver consistency in decision-making, the NSA stated how that is done, "with comparison… taking into consideration when something similar to that happens to another railway undertaking that of course we act in a similar way. Because the list we have of our whole actions, I can always compare and look up what has been done and try to… of course it has to be adapted to the specific cases, but in a general way we always of course compare it, that the criteria is of course the same." *Our opinion: Consistency can be achieved by reviewing action taken in previous cases with similarities; however, this does assume that the action taken in previous cases was proportionate and correct. The NSA acknowledged that a range of other factors are considered and may affect the decision taken, which does indicate that a more robust, structured framework for decision-making may be needed.*		1					
I	Rail	A	Enforcement action is a "team decision". Teams initially comprise a legal expert and an operational expert. Then depending on the nature of the incident or breach, technical experts are also involved. *Our opinion: Decision-making in teams does not empower any single individual with responsibility for a case. Whilst it is good practice to have expert assistance, a team decision may not consider all data consistently.*		-1		1			
I	Rail	BG	The Bulgarian NSA does not have a formal decision-making process *per se* (and certainly nothing that is documented); instead, the national Railway Transport Act states that inspectors of the NSA can "make prescriptions which is made on their judgements". Therefore, to ensure such judgements are proportionate, inspectors must be suitably qualified for the role. Enforcement decisions are then based on the level of risk presented by the RU/IM, "the bigger the risk is, the risk that we have spotted, the bigger and the more persistent is the supervision activity and the control that we perform". In addition to the real or potential risk, the NSA also considers the speed with which the RU/IM responds ("if there is not a timely elimination of this inconsistency… a higher level of control shall be performed"), and the frequency of the inconsistency ("it can be low risk, but higher repetitiveness of these inconsistencies… imply increase of control, or increase of the supervision"). The person or persons responsible for making an enforcement decision depends on the scope of the enforcement: "[Inspectors'] judgement is based on their… experience and competencies. And when	1	-1					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			necessary, the decisions are taken by higher level… by the management of our agency, which can send prescriptions to the… managers of the Railway Undertakings". The NSA explained that, generally, if a decision affects management of an RU then the decision will be made by management at the NSA. If it concerns a technical issue, it will probably be made directly by the inspector. The NSA believes it has the necessary experience to formalise the decision-making process it follows if this is required. "There is no problem to describe this process in a procedure, as we have already gathered enough experience. So of course we will discuss this." *Our opinion: There is an indication here that the type of intervention taken by the NSA may not be focused on the SMS and how the RU/IM itself can be responsible for safety. It is good practice for all enforcement decisions to be escalated to management so that changes to the SMS can be initiated where appropriate—it is not necessarily for the NSA to decide at what level it is appropriate to report the enforcement decision (even if an RU/IM's own systems will escalate the issue through the company).* *The absence of a formal decision-making procedure places considerable faith in the equivalency of staff competencies and it is not entirely clear the mechanism by which proportionality is achieved. However, the NSA does have common factors that it considers when deciding on the level of enforcement required – although the influence of these factors is not openly prescribed or limited.*							
I	Rail	S	The Swedish NSA follows a risk-based decision-making process during supervision. Enforcement action is therefore based on evaluating various operational factors, such as: "…are you transporting people, transporting goods, or you are having dangerous good, or you're on the high speed network, or are you just shunting on a side-track, or are you just shunting on a different area in a factory?" The amount of rail traffic and the size of the company are also considered. *Our opinion: The NSA is considering which additional factors may affect its decision. This is considered good practice.*	2	2		1			
I	Rail	PL	If two RUs/IMs were to commit the same offence, the NSA's enforcement response would be identical, irrespective of any other factors (such as whether it was a first offence or a repeat offence). "Our reaction would be the same… the first step… would be the recommendations. So both in the case	1	1					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			of a company that commits a certain violation for the first time or… another company that violates the same provision but it's a systemic problem, there would be the same recommendation; start complying with the law. And then it depends on how they respond to the recommendations because if it's a single case and the company either starts complying or presents a plan of how to avoid it in the future, it's fine. If it's systemic and the company refuses to cooperate, at that point the reactions will be different." *Our opinion: The approach described here appears not to consider any factors other than the type of breach when determining initial enforcement action; only when the initial enforcement recommendations fail does the NSA consider the context.*							
I	Rail	PL	"Recommendations are issued by regional branch managers because they are… in charge of the inspections, controls. Once we have to impose a penalty, a decision is taken at the head office level with management involved. It's very rare that things go as far as the penalties because it's difficult to enforce the penalties. It's better to work with the recommendations and see them being implemented." *Our opinion: the decision-making structure is divided so that decisions to escalate enforcement actions are only taken by NSA management. It is not considered good practice that staff are not empowered to make decisions and also that penalties are not often issued due to administrative difficulties.*	-1	-1		-1			
I	Rail	PL	The Civil Service Act in Poland makes employees individually accountable for their actions. A recent amendment has increased the maximum penalty to an amount that is equivalent to the annual salary of the person. The change "actually promoted inactivity, because it was better not to act and thus not be accountable than to take action and be accountable". *Our opinion: In some Member States, national legislation makes staff liable for their actions (or inaction) which can affect the supervision activities of an NSA.*				-1			
I	Rail	NL	To be proportionate, the NSA has the following procedures in place for making decisions: • Dutch law already requires sanctions to be proportionate and subject to normal jurisprudence. • All supervision reports are read by another colleague. • Peer group discussions are organised to consider decisions that are about to be issued. *Our opinion: It is good practice to implement administrative rules that govern general government practices.*	2	2					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	D	Since 1994, the NSA has followed German national administrative law, which prescribes that action must be proportionate and consistent. The NSA has a series of published documents for each of the structural subsystems that are subject to supervision: these documents indicate, "how we do supervision, what we will supervise, how we will act, whom we would supervise and so on." The NSA has not made any specific changes in response to the regulation by the EC of the principles of supervision. It also does not have any procedures to evaluate specifically whether it is following the principles. "We have made our principles, how we act, what we will supervise and so on, and we will stick to them no matter what we supervise or who is the addressee or what the case is. We will apply them in a consistent way." *Our opinion: as with the Dutch NSA, the German NSA follows national administrative rules regarding the conduct of authorities. These rules require that proportionality and consistency are applied; however, there is no procedure to check that these principles are indeed being applied.*	2	2					
I	Rail	D	Given an example of two RUs that have committed the same safety violation, the German NSA stated that, "There might be factors coming from the history of the safety records of these undertakings triggering a different approach." Specifically: "For undertaking one they might have an SMS which has been assessed by us, which from our point of view works perfectly, which hasn't had any incidents in the last five years and where this is the first one we find for the last five years. So there might be undertaking two, where the SMS has been assessed by us. There were some improvements which had to be done and they have had, I don't know, eight safety relevant incidents in the last time. So we have a little bit of a different picture of that company. So that might trigger another way of dealing with that. That's a decision based on experience, knowledge and expert judgement. I would say that's a consideration or an assessment that the NSA is allowed to do it in such cases, to take into consideration all the aspects of… the case." *Our opinion: As with other NSA, the German NSA will adjust its enforcement decision in light of factors related to what it knows of the RU's operations. Specific mention was made of the quality of the SMS when making a decision.*	2	2					

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	D	"Each undertaking has a leading auditor or somebody being the main contact person for that undertaking. So all information concerning that relevant undertaking is stored and can be reviewed or reflected or analysed if there's a current case which has to be decided. They should then always contact this leading person or this main contact person in order to ensure harmonised approach or harmonised action. They have… an enhanced decision [-making] role… they should be consulted before a decision is taken." *Our opinion: The decision-making process is apparently influenced by the member of staff who has been assigned as a point of contact for the RU or IM in question. The German NSA views the assigned point of contact as the person who will have the most knowledge of a RU/IM and can share this knowledge to harmonise the response.*	2	3					
I	Rail	F	"When we do an audit or an inspection, before we notify… what you may call nonconformities, we first decide in a collegial manner. We have a thing called a harmonisation committee, and the harmonisation committee meets after every audit or inspection to determine first of all that if the things that we found during the audit or inspection which are identified by the inspection team as nonconformities, first of all, they are not confirmed to be nonconformities until the harmonisation commission or committee has actually confirmed them to be nonconformities. That's one thing. If it is a nonconformity based on the grading that we give them, we have to decide how serious the nonconformity is. Is it just an observation we wish to make? Is it a reserve that we will put on or is it a major nonconformity which will require relatively quick remedial action? Or is it actually something which is seen as being producing a potentially dangerous situation, in which case, we would just take immediate action with the entity. So, "You must stop doing this or this is a restriction we're going to put on you now". And this harmonisation, we try to make the same sort of decision no matter how large or small the entities are, based on what we've seen before. So the consistency comes from this systematic use of the harmonisation process. The person in charge of the inspection or audit will be there. Then his peers, as heads of different divisions, will be present or represented… because sometimes the audits or inspections don't spot things which are a bit detailed from a technical point of view, so we make sure that normally you would have an expert in your team anyway but we would also have, say, the head of the specific division also present. He's not part of the audit team, he will be there anyway because of the heads of the divisions or somebody senior from the divisions that will take part in the harmonisation committee, and then the	3	3		3			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			committee itself is presided by somebody senior. Could be the head of department or the deputy." The NSA described how the harmonisation committee is put together and planned as part of each supervision activity unless it is a response to a dangerous incident, in which case senior members of the team (who would probably be part of the committee anyway) would be consulted. The process can happen quickly enough to avoid 'red tape' preventing an urgent response. *Our opinion: As with certification committees and other independent bodies employed by other NSA, the French NSA has a harmonisation committee which is responsible for assessing the validity of any decisions regarding non-conformities (which is essentially the main enforcement action that can be issued by the NSA). The committee is compiled from a mix of people who are and are not familiar with the content of the RU/IM's audit. This is good practice for ensuring proportionality and accountability.*							
I	Rail	F	"We have a procedure which identifies the criteria for allocating a particular severity. And that procedure is available on the internet for anybody to look at, including the people who are audited and inspected. So upfront they know the criteria we apply and we apply it when it comes to allocating severity, if you like. So use of that procedure perhaps could be standalone, that you just say is there an immediate risk or is the risk more or less in the near to medium future? So making the difference between two different grading. But what we also do is sometimes you have to look at the number of nonconformities in the same subject, so this is where we use our experience and we look at what we've done before in similar circumstances. An example would be, for example, a training centre. Training centres in France have to have an authorisation from the NSA, from EPSF. And we make sure the training centres all operate in the same way because training we see as very important. So for the training centres, we have a database of nonconformities, which we can look at when we do the harmonisation process." *Our opinion: It is good practice to document and share the decision-making criteria that are used for enforcement. The NSA also refers to previous cases and trends in non-conformities to establish whether the enforcement action should be varied from the expected course.*	3	3		2			
D	OSH	B	Enforcement of administrative fines: website provides a brief explanation of the process. It is: report on breach; report viewed by auditor to determine if offence is administrative or criminal; if criminal, referred to Court, if not, sent to a Directorate that manages administrative fines; Directorate considers any defence and then decides on the fine, if at all.			1	1			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: The process described lacks clarity and provides no detail on the decision-making criteria used, or the detailed process. It would be better to provide fully-documented approaches like the EMM used by the GB OSH and NSA. However, some description of the process is desirable. The process here does not demonstrate a good level of dialogue between the safety authority and the dutyholder to discuss the problem.							
I	Rail	GB	The NSA is involving its staff in reviewing its decision-making procedures: "[For] the enforcement management model… we've had recently a set of seminars with some of our inspectors… where we've gone through to refresh them with the help of HSE [the OSH authority] because they wrote it and they understand it clearly better than we do, how it should be used, and I think that's thrown up some issues about how maybe our inspectors are using the model to determine what is the right course of action. So we'll be doing some more work on how we brief out the EMM as it were and what are our expectations of our inspectors when they use it." *Our opinion: It is good practice to involve staff in reviewing decision-making practices as they will be most familiar with the strengths and weaknesses of the current approach. The NSA is also demonstrating efficiency by sharing its basic decision-making policy with its OSH authority and involving this body in the review procedure, too. Updating procedures for decision-making can deliver greater consistency and proportionality.*	3	3					
I	Rail	DK	The application of observations/remarks, non-conformities or orders/bans can vary according to the NSA's perception of the RU/IM: "If we are looking into a company with a well-functioning safety management system, an observation could do pretty much… the same as a non-conformity because they are willing and they want to be better. A non-conformity is an agreement with the company to fix something and they sign it. So, if we feel that this company needs more support, we will issue a non-conformity but [if] a company will react with an, "ah, okay, we see that, we have to adjust that", we will just say, "okay, this is a remark or an observation and we'll write it in our report"." *Our opinion: It is good practice to moderate enforcement action based on RU/IM factors such as the capability of the RU/IM.*	2	2					

Table B.25: Examples of NSA service standards/pledges

NSA	Content of what is expected of RUs/IMs	Content of service pledge
Great Britain	All relevant information about how we regulate RU/IMs and what we expect from them.	-
Sweden	Information about framework, regulations, guidance.	The Swedish Transport Agency is working to achieve good accessibility, high quality, secure and environmentally aware rail, air, sea and road transport. We have overall responsibility for drawing up regulations and ensuring that authorities, companies, organisations and citizens abide by them.
Estonia	Legal framework and any changes.	Mainly contacts (tel. nr-s and e-mail addresses).
Lithuania	These legal acts contain requirements for RU to comply with.	It describes services that NSA provides and duties of NSA too.
Romania	Legal requirements.	-
Germany	-	General aspects on how EBA acts in processes of authorisation and supervision.
Denmark	-	Our supervision strategy.
Spain	-	-
Latvia	Procedures, contact persons, available information about fulfilment, guidance.	Question - answer forum.
Poland	Information on the website is limited to the list of requirements set in the Polish law and sometimes in additional documents (guides etc.). Additionally, NSA employees make further explanations on telephone or during meetings.	-
Bulgaria	Up-to-date information about changes in the safety regulatory framework	Railway Administration Executive Agency i.e. the NSA of Bulgaria is

NSA	Content of what is expected of RUs/IMs	Content of service pledge
	at EU and national level, new requirements relevant to their work and their cooperation by means of establishment of working groups for the performance of specific tasks.	certified under ISO 9001:2008
Austria	Guidance for SC/SA already available, strategy paper for supervision under development.	-
Portugal	-	-
Czech Republic	-	Requirements for certification.
Netherlands	Procedure + needed information from applicant.	-
Channel Tunnel	-	-
Hungary	The website contains all necessary information.	-
Norway	-	-
Ireland	Guidance on the RSCs supervision and enforcement activity.	Guidance document for supervision, which sets out rights / obligations of all parties concerned.
France	On the website of the EPSF, a guide describing the procedure used during controls that makes the EPSF is available. The EPSF publishes its annual activity reports and safety (supervision strategy...). The meetings allow REX (return of experience) including discussions between stakeholders and with the EPSF. The EPSF publishes a monthly newsletter that lists the incidents characteristics to which attention is particularly drawn to the RU.	
Finland	-	-
Italy	-	-

Table B.26: Website communication

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	GB	"We run a number of processes about how we go about doing our work to be consistent so we have a process for inspection, we have a process for investigation, we have a process for, you know, if matters need to go to prosecution; we have a prosecution process for how we approve such cases – they're on the website, free for everyone to see. So we train and expect our staff to follow those processes." *Our opinion: publication of full decision-making process is good practice.*		1	1	1			
D	OSH	H	A suite of resources is available for dutyholders including 'What you should know' FAQs, Factsheets and Topic pages published on the website. *Our opinion: These are helpful resources for ensuring that dutyholders appreciate their responsibilities.*			2				
D	Aviation	LV	Website links to multiple examples of SMS guidance from other safety authorities			1		1		
D	OSH	A	Website features on key issues that dutyholders have to tackle (e.g. noise). *Our opinion: A focus on key issues for industry can be useful, providing a focal point for dutyholders to turn to when they are looking for references, support and advice for common problems. It also shows that the regulator is in tune with the market and is aware of current difficulties.*			2			1	1
D	OSH	GB	Website: contains a wide range of information as well as publications/ guidance documents available for download which highlight the value of undertaking enforcement activities. The regulatory frameworks and supervision/enforcement tools are promoted on the website under a 'resources' category. The strategy and business plan are provided under the 'about HSE' category. *Our opinion: Websites are an essential part of a good practice approach. Looking at approaches by other safety authorities helps to identify what information should be presented.*			2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	GB	News feed: Fines, prosecutions and relevant news are displayed on a web page. *Our opinion: This is considered good practice as it keeps the industry aware of the regulator's activities and demonstrates to the public that it is performing its functions.*			2				
D	OSH	DK	Website structure: Catalogue of work issues, notices, rules. Can be organised alphabetically, by industry sector and by category. Compilation of information by multiple means. For example, the main rules are listed and then the user can select one of 36 industries to find specific rules that apply. Within each sector, the rules are described followed by a simple-to-follow practical example of how others are working to solve problems. *Our opinion: This simple-to-use and customisable approach to searching for information is an excellent model of how to help dutyholders find what they need to comply. The option to search by industry, category or alphabetically could be worth carrying over to NSA websites for the railway sector. Information should be made easy to find and, wherever possible, it is beneficial to group information in a way that collects together relevant documents for an RU or IM according to the service they wish to provide.*			3				
D	OSH	DK	Information in foreign languages on the website covering selected working environments that are most likely to include foreign workers. *Our opinion: Good practice to cater for foreign-language dutyholders. Clearly, providing all information in all languages of the European Union would be a disproportionate burden. However, NSA may wish to consider the composition of the market they supervise: if it is home to several RUs/IMs from other Member States, there may be safety benefits to providing some essential information in the native languages of the RUs/IMs. This applies to non-regulatory as well as regulatory information: whilst a foreign RU/IM may have a good working knowledge of the safety regulatory framework, it may not have the same knowledge of the information provided by an NSA (e.g. about its strategy, processes, how it supervises and enforces). Language difficulties may also be addressed by cooperation agreements between NSA; for example NSA could direct foreign RUs/IMs to relevant information provided by another NSA in the native language of the RU/IM, rather than providing their own direct translations.*			3		1		

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Rail	GB	All improvement and enforcement notices are published on the NSA website.		1	2	2			
D	OSH	GB	Register of Prosecution and Notices: contains enforcement information on notices and prosecutions. A search function allows users to call up details of prosecutions which resulted in a successful conviction within or beyond the last five years. *Our opinion: The search facility and database are comprehensive but without actively searching, the examples are not visible. Examples of prosecutions can be a deterrent and a source of information at the same time but these values diminish when the examples are not readily available.*			2	2			
D	OSH	GB	"Information on improvement and prohibition notices should be made publicly available." This includes annual publication of convictions, including company names and the regulatory action taken. Media exposure for cases is advised if it draws attention to the need for compliance. *Our opinion: Publication of enforcement action can be considered good practice for a number of reasons, such as:* • *Visible deterrent: there is an element of public shame associated with enforcement action against a company being published. This activity may be an incentive to other organisations to work harder towards implementing an effective SMS.* • *Commercial loss: publication of enforcement action may affect the commercial competitiveness of an organisation by deterring customers. This outcome does depend on the type of organisation: a RU/IM without commercial competition may not be affected but a freight RU that is competing with others for trade may incur commercial losses. The outcome may depend on how the enforcement action is presented. An example that describes how the company has responded positively and effectively may present it as responsive and aware of its role in improving safety.* • *Demonstrate the role of the NSA: the function of the NSA as an enforcer can be demonstrated by publishing its enforcement actions. This message can reach the industry, the public, other NSA and stakeholders, providing a degree of transparency and cooperation in the process. For some cases it may be in the public interest to publish enforcement actions, particularly for high profile incidents, as this may reassure the*	1	1	3	1			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			public that the incident has been taken seriously and has led to corrective action. • *Guide the industry by example: as well as being a visible deterrent, published enforcement action may also serve as guidance to the industry regarding how it should operate – and in particular, the practices it would do well to avoid.* *However, a note of caution is required. Publication of enforcement action may be prohibited by law in some Member States. If the law permits publication, the safety authority would be advised to consider if the overall level of enforcement action will still be proportionate when the effects of publication are included. This may depend on the type of organisation, the type of action taken (e.g. has a fine already been issued), and the style of reporting (e.g. how the publication present the facts of the case and the company's response). The safety authority should also consider which levels of enforcement should be published (e.g. only prosecutions) and the format for publishing. Some safety authorities may choose to publish high profile enforcement decisions and/or the more severe cases in a prominent position on their website but place details of more minor offences in a less visible section of the website (e.g. in a searchable database). Finally, if publishing enforcement actions, NSA must avoid generating social norms that suggest to the industry that 'everyone is breaking the law'. Violations should be shown as infrequent and unacceptable.*							
I	Rail	NL	"Our yearly plan is published [so] we are transparent in what we are going to do next year but we are not open in what we've done last year. We make a year report on how many administrative and criminal sanctions we've done in this year, but that's without naming the companies. So it's partly transparent, it's partly open. We're publishing without naming the companies that are concerned because the naming is an extra sanction and there is no legal basis in that extra sanction. So it's jurisprudence that it's not allowed to… in some domains it is allowed but not in the rail domain. It would be an extra punishment." *Our opinion: in contrast to some Member States, the Netherlands does not have a legal basis for disclosing which RUs/IMs have been subject to enforcement activity.*			1				
I	Rail	F	"We're certainly transparent because the procedure we use to audit and inspect entities is not a secret; it's in the public domain… Not only that, if you look on our internet site there's a lot of information for the different entities, including guides on how to produce the different documents they have to produce." *Our opinion: The French NSA, in common with the majority of NSA, believes that publishing documents on its website satisfies the principle of transparency. However, the NSA*			1				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			demonstrates good practice by supplementing the website with monthly incident reports and three-monthly meetings with the market.							

Table B.27: External communication: conferences, workshops and seminars

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	B	Range of workshops available to demonstrate safe working practices. *Our opinion: Enabling dutyholders to access the collective experience of the safety authority and other dutyholders by booking workshops on specific subjects is a good way of disseminating such information. Such workshops are particularly useful for encouraging dutyholders to engage with each other to discuss and share practices, with the NSA present to provide a regulator's perspective on the discussion.*			2			1	
D	Aviation	GB	SMS conference held in 2011. 'This was an opportunity for large and small fixed-wing Commercial Air Transport operators to share their experiences of implementing SMS and for the CAA to provide the delegates with an overview of its oversight of SMS.' Conference materials available on website. Includes reports on practical experiences of implementing SMS from representatives of four different airlines, achieving management commitment, and building a good safety culture. *Our opinion: Conferences demonstrate good practice by bringing together stakeholders to discuss subjects of common interest and to share experiences. Of note is the range of stakeholders taking part (both large and small) and the role of the safety authority in sharing its own knowledge of SMS. Good practice can be demonstrated further by publishing conference materials for wider reference.*			2				
D	Aviation	LV	The authority held an SMS implementation course in 2008 for 30 participants from Latvia and 2 from Estonia. The course emphasised improving knowledge and skills to certify and oversee SMS implementation. *Our opinion: Training courses that offer guidance on implementation may be considered good practice. Allowing cross-border participation is helpful for developing a harmonised approach.*			2		1	1	
D	Aviation	CH	Annual Swiss Air Safety Conference which provides a platform to the industry to present and exchange examples of best practice. Proceedings of recent conferences hosted online to provide a resource library giving access to the latest industry perspectives on SMS. *Our opinion: Conferences demonstrate good practice by bringing together stakeholders to discuss subjects of common interest and to share experiences. Good practice can be demonstrated further by making events regular and publishing conference materials online.*			2				

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	B	States that the BCAA will organise safety seminars in conjunction with the Belgian aviation sector and the Accidents and Incidents Investigation Unit. *Our opinion: Seminars such as this are an example of good practice because they show how the authority can bring together key stakeholders to discuss safety issues. In this example, the authority is involving the accident investigator to facilitate exchange of information with the market. Seminars are an opportunity for more targeted participation and discussion within smaller groups.*			2		1	1	
D	Aviation	F	Hold occasional seminars (one in 2007, two in 2008, one in 2010) on relevant topics, e.g. proposed extension of EASA powers to 'summarise these developments and ongoing work…so that everyone can prepare for the change'. The website contains the agenda for each seminar with links to presentations. *Our opinion: It is good practice to use seminars to harmonise the understanding and approach of the market.*			2			1	
D	Aviation	F	CASD symposium in November 2011 was focused on subject of moving 'from dealing with incidents to risk management'. Agenda available on the website and a DVD of the symposium is available. *Our opinion: Events that bring stakeholders together to discuss key industry issues are usually considered good practice.*			2			1	
D	Aviation	PL	Conference materials from previous annual conferences available to download. Safety-related newsletters also available. Conferences and proceedings are focused on the EASA (central agency) top safety themes. *Our opinion: It is helpful for authorities to retain proceedings from previous conferences and similar events in an accessible form. It is also good practice for such events to focus on Europe-wide themes to promote harmonisation.*			2				
D	Aviation	N	Aerospace Conference scheduled in 2012 – presentations/workshops include 'flight safety measurements', 'safety, security and environment'. *Our opinion: Events that bring stakeholders together to discuss key industry issues are usually considered good practice.*			2			1	

ID	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	A	Local dissemination and promotion of EU-OSHA campaigns (centralised agency). *Our opinion: If a central European agency for the sector has a campaign, it is good practice for safety authorities within each member state to promote the campaign.*			2				

Table B.28: Other communications

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	DK	External communication strategy – 3-5 year programme. "We will communicate directly with our audiences. Communication must be recipient-driven, meaning the recipient's knowledge, attitude and actions will form the basis for the way we communicate. Our primary target market is companies." Aim to be "open and simple… approachable, honest and straightforward. The values in our communication, respect and cooperation." *Our opinion: this approach appears to be driven by the market, indicating that it may be underpinned by market research. It is good practice to have a long-term plan for engagement.*			3	1		2	
D	OSH	GB	Three key provisions made by the GB HSE to ensure transparency during inspections are: • when inspectors offer dutyholders information, or advice, face to face or in writing, including any warning, inspectors will tell the dutyholder what to do to comply with the law, and explain why. Inspectors will, if asked, write to confirm any advice, and to distinguish legal requirements from best practice advice; • in the case of improvement notices the inspector will discuss the notice and, if possible, resolve points of difference before serving it. The notice will say what needs to be done, why, and by when, and that in the inspector's opinion a breach of the law has been committed; • in the case of a prohibition notice the notice will explain why the prohibition is necessary. *Our opinion: These provisions emphasise the importance of dialogue between dutyholders and safety authorities to ensure that whatever action is taken, it is understood clearly. The focus of these provisions is to be entirely transparent with the dutyholder and ensure that they understand fully any enforcement action that is to be taken.*		1	2	1			
D	OSH	GB	Leaflet: "Dutyholders… need to know what to expect when an inspector calls and what rights of complaint are open to them. All enforcing authority inspectors are required to issue the HSE leaflet *What to expect when a health and safety inspector calls* to those they visit. This explains what employers and employees and their representatives can expect when a health and safety inspector calls at a workplace."		1	3				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: NSA primarily liaise with RUs/IMs via inspections and audits. Even if information is provided elsewhere and at other times, during an inspection it seems pertinent to have this information in an accessible format to remind or inform those who are affected by the supervision activity of their rights. It should be considered that those RU/IM representatives affected by an inspection may not be the people within the organisation who are familiar with the NSA's procedures.							
D	OSH	GB	A progress report ('One year on'; http://www.hse.gov.GB/strategy/one-year-on.pdf) to update the industry with how the strategy had been received and implemented. Key features to engage the industry with the activities of the regulator include: • Quotes from company representatives discussing how they have tackled their obligations. • Case study examples taken from supervision/enforcement activities and efforts to achieve compliance amongst the industry. • Key facts from research that has taken place (e.g. highlighting the positive effects of involving workers in health and safety compliance). *Our opinion: This document is an example of how it is good practice to promote good practice. If organisations have impressed with their efforts to be compliant and have developed clever initiatives, it makes sense for the safety authority to help promote these examples to other organisations. It also shows how the strategy is recognising that improvements are being delivered.*			3				
D	OSH	GB	Poster/advertisement campaign: a four-year programme focussing on regulatory 'myths', with a new myth featured and debunked every month. *Our opinion: This is an example of good practice in two ways: firstly, media are used to promote the activities of the authority; and secondly the authority is seeking to dispel damaging misconceptions that can affect the success with which it acts as a regulator. Poor perceptions of a safety authority and its work can be damaging when trying to develop a compliant industry. The regulation of safety in the rail industry may not be subject to such myths but there are likely to be country-specific issues about which it is worth raising awareness. For example, some safety authorities may wish to promote the SMS-based approach amongst all levels of the workforce to challenge traditional 'blame cultures' and*			3				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			promote 'just cultures' where staff at all levels of an organisation are engaged with creating an effective SMS.							
D	Aviation	CH	Safety awareness campaigns - stay safe! Campaign raises awareness of important safety issues in the aviation industry. FOCA does this with posters, flyers and brochures – some downloadable from website. http://www.bazl.admin.ch/fachleute/safety_risk/01357/index.html?lang=en *Our opinion: As above.*			3				
D	OSH	I	"INAIL prepares and circulates publication, audio-visuals and software aimed at improving the implementation of the rules and regulation regarding Health and Safety at work, e.g. the Virtual Enterprise. This is a 3D animated application which presents some typical risk situations in the workplace and shows potential actions for their elimination or reduction. INAIL also provides a 'Catalogue of Best Practice'." *Our opinion: It is good practice for safety authorities to be open to using a wide range of media for disseminating information to stakeholders. The examples here discuss more innovative techniques when compared to simply publishing or linking to regulations and guidance in their original format. Use of alternative media should be supported by market research to better understand what the industry wants and needs, and how it would like such information to be presented. Innovative media may be best suited to explaining key messages, or complex practices. Safety authorities may be able to decide on the content based on supervision activities (e.g. issues where there are common misunderstandings may benefit from further explanation using such media).*			2				
D	OSH	B	SWIC (Safe Work Information Centre) – a specialised documentation centre that can be accessed on appointment. Contains monographs (books and reference books), pamphlets, periodicals, unpublished (conference proceedings, working papers ...), documentaries and folders, standards, videos and DVDs. *Our opinion: Hosting a library of resources is one way of making relevant information available. It is perhaps not the most accessible option; ideally, such information would be made available online.*			1				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	FIN	Safety posters free to download. *Our opinion: It is good practice to have a range of materials to disseminate information.*			1				
D	Rail	GB	Monthly meetings between RUs/IMs and local inspectors: teams of inspectors are assigned to certain RUs/IMs or groups of RUs/IMs (inspectors become 'account holders'). Regular engagement occurs between the two and monthly meetings are a way of keeping each other aware of what is happening. Having an account holder means there is a single point of contact between the RU/IM and the NSA but in acting as an account holder, that person may speak to many other inspectors (for the main IM up to 30) to get a complete picture of current activities. Only the major RUs/IMs will have an account holder assigned (about 60 overall to include the IMs and RUs). The account holders are rotated regularly to reduce 'regulatory capture', whereby an RU/IM becomes close enough to the account holder to influence (and even control) the regulatory authority. *Our opinion: this is a good practice example of how to maintain regular dialogue with RUs/IMs. Meetings of this type add another layer to the supervision regime and provide an opportunity for the NSA and the RU/IM to discuss issues that may have emerged, from operational observations or during recent inspections. Frequently changing the point of contact that an RU/IM has with an NSA helps to avoid the difficulties that may arise from such an arrangement.*		2	3				1
D	Aviation	GB	Publish an annual review of aviation safety.			1				
D	OSH	LT	Since 2000, the electronic weekly newsletter of the State Labour Inspectorate "News of the Inspectorate", dedicated for employees of the Inspectorate, is issued. It has become the acknowledged form of the systematic exchange of internal information of the Inspectorate – in this publication regional divisions are informed about decisions of the top management, activities, events held by the Inspectorate and jointly with other institutions, foreign partners, topical tasks carried out by the divisions of administration, thoughts, experiences		1	1				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			from events, business trips, study visits are shared, news from regional divisions, advice and recommendations (methodologies) on the improvement of inspection activities are shared, local acts, data and indicators of the system of assessment of public servants of the State Labour Inspectorate are published. *Our opinion: A regular, internal system of communication is good practice. However, for a system of communication to become "the acknowledged form of the systematic exchange of internal information" there must be a mechanism that ensures it is accessed by all staff. A weekly newsletter may not be the most appropriate method of informing staff of management decisions and recommendation for improving inspection practices.*							
I	Rail	D	Lead auditors are assigned up to 10 RUs or IMS for which they are the first point of contact and will coordinate activities that involve the NSA and specific RUs/IMs. This process was initiated in 2009 (although not in response to any particular problem) and at the moment the lead auditors have remained assigned to the same RUs/IMs. This is likely to remain in place for five years (the duration of a safety certificate and be reviewed after that point. There are no current plans to rotate the assignments. "This has proven to be a good thing to have such a coordination point inside EBA to aggregate the information and the activities towards one undertaking in such a contact point." *Our opinion: Assigning an 'account holder' or similar to specific RUs/IMs is a potentially good practice approach to delivering effective communication and engagement with the market. However, it may be desirable to re-assign NSA staff to different RUs/IMs on a regular basis; it could be argued that the benefits of this approach may be diluted by the risks of having specific RUs/IMs communicating with specific NSA staff for the duration of the safety certificate/authorisation.*		2	3				1
I	Rail	F	"We have three-monthly reviews of performance with the railway undertakings and also with the infrastructure manager for the French national network. We feel that the REX [return of experience/lesson learning]… is a very important part because it's a very good method of communicating in a less regulated manner, the people that are subject to our inspections and audits. It's a joint meeting where we share results and typically the railway undertakings will be		1	3	1		1	1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			asked, not necessarily each in turn, but those who feel they've got a subject which they'd like to share with other railway undertakings and with EPSF, by definition. There will quite often be a presentation. So that's where, I suppose, we get some feedback also, as to how we feel we are performing. Also, certain incidents that gave us cause for concern during the early years, we see a reduction in certain types of incidents, notably on some of the infrastructure side." *Our opinion: The NSA demonstrates good practice by organising regular meetings that enable open discussions and presentations amongst RUs/IMs for the purpose of communicating outside of regular supervision activities. This platform for open dialogue is intentionally designed to be 'less regulated' so that behaviour can be influenced. The meetings also provide the NSA with informal feedback on its performance and it has noted that some of the incidents discussed at the meetings decrease in prevalence afterwards so there is some evidence that this approach is an effective form of influential enforcement.*							
I	Rail	F	"There is a monthly incident report which is sent out to everybody. We review incidents internally and then we decide which of those incidents we would like to notify to everybody, because I'm sure you appreciate that with railway undertakings, not everybody knows what incidents have happened with their neighbours or their competitors, in fact. The incidents are issued in a formal letter to everybody. I think it's quite useful for them, notably the railway undertakings… to send a formal letter saying these are the incidents which we've picked out this particular month." *Our opinion: A further example of good communication is to update the market on the latest incidents monthly. It is good practice to share the lessons that can be learned across the market; in this respect, the NSA is helping to harmonise market knowledge and is encouraging all RUs/IMs to consider the relevance of recent incidents in their own operations, irrespective of whether an RU/IM was involved directly.*			3			1	
I	Rail	N	The Norwegian NSA hosts regular 'breakfast meetings' at its offices and invites RUs and IMs to come and discuss any issues they have (as reported by the Swedish NSA following a meeting with the Norwegian and Danish NSA). *Our opinion: Informal communication and engagement practices are good practice: they can build trust between RUs/IMs and the NSA, provide a forum to exchange views and*			3				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			guidance and can help identify emerging issues before they become a safety hazard. It is also a good example of NSA cooperation that such practices are being discussed between NSA.							
I	Rail	S	The NSA has an annual meeting with the management of the largest RUs and IMs (approximately 10 altogether). It may also arrange special meetings with managers following an audit, for example, to discuss management responsibilities. *Our opinion: The Swedish NSA supervises a large market of approximately 100 RUs and 400 IMs; it is therefore good practice to have regular communication with the largest RUs/IMs in addition to the communication that occurs during audits.*			2				
I	Rail	A	Regular meetings are arranged between the NSA and RUs/IMs. For the main undertaking, "we have on different levels meetings with them and you could say that's going from… because still we have an approval process for internal regulation of the undertakings concerning safety-related activities and these are, for instance, monthly." For other RUs/IMs, "At least half a year we make meetings with the safety managers, and then of course if something special happens there are meetings in between". *Our opinion: Regular dialogue with RUs/IMs is good practice; however, in this instance it would appear that the process for some of this contact is based on national rules and may not therefore contribute towards SMS-based supervision. This can occur during a transition to the European supervision regime; however, if good communication practices exist in the current regime of operation, it is desirable to carry over the concept to the new supervision regime.*			2				

Table B.29: NSA descriptions of communication

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	NL	"In general you can say we should communicate more about our actions. And sometimes we never actively show something to the press, but the press sometimes asks what we are doing and then we have to come up with an opinion. There should be a better communication strategy about how we communicate about our actions. I think there we do too much in silence. But that's very close to the publishing of sanctions, so there is a line between what you can do and what you can't do. I don't know. I think we can do more than what we do now, [we do not] with the excuse of that it's not allowed, but the excuse is made bigger than it should be." *Our opinion: An NSA should have good communication with its stakeholders. This can be facilitated by press coverage and formal communication about activities. It is not good practice if laws against disclosing the identity of companies that are subject to enforcement prevent wider communications from an NSA.*			1				
I	Rail	DK	"We have our website, we have a seminar every year where we have key issues that will inform the companies about how we interpret regulations... we have guidelines on the order of what a SMS should include for both railway undertakings and infrastructure managers. Then we have different forums actually inviting the companies to… regular meetings in our authority. We have just implemented new rules on the authorisation and we invite companies to sit in almost like a school class, going through what this means, what the company has to do to be in line with the regulation. We have something called CSM School… for the risk assessment… Knowing they [RUs/IMs] didn't have a clue what it was. It's also very important… to have one opinion of the regulation. We needed to get the sector together and facilitate this. If we don't there's a chance that every company will develop their own, interpret the regulation their own way and we will have a lot to do afterwards, trying to get it all in place. *Our opinion: The measures taken by this NSA to engage with stakeholders demonstrate good practice. The NSA has gone beyond simply having a website and has set up events that bring the stakeholders together with the NSA to discuss relevant matters and latest guidance. Of particular note is the CSM school which was established to ensure a unified approach to risk assessments.*		2	3			1	1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	A	Measures taken to be transparent include web-based guidance, meetings and direct contact: "Beginning with the issuing process [of safety certificates/authorisations] we have on our official website guidance for this concerning what documents have to be delivered and also the process the authority takes doing this. The general strategy of the ministry itself, publish[es] its general aims concerning the issuing… the next step will be that the supervision strategy and the decision principles will also be made public… a date [for which] will be the coming into force of the regulation [CSM Supervision]. That would be the last possible date we would be publishing and so we see when we have finished the work. I don't think it will be in the first half of the year, but we are trying to be in accordance with the regulation so there should be no problem when it comes into force, that we don't have to alter really very much the development we are taking now. We try to give the undertakings the opportunity to learn in advance before an application. It's also the same with rolling stock. They have published the decision principles that they know what they have to expect when they come to the authority. And also of course if we take enforcement actions, these are combined with meetings and personal contacts and explaining of course why this comes in this way." *Our opinion: The NSA will expand its communication with RUs/IMs to increase its transparency when it publishes its supervision strategy. In the meantime, it is using the website and contact with RUs/IMs (primarily at the application stage) to share guidance.*			2				
I	Rail	A	The NSA is active in trying to guide the industry when new regulations are released: "With the new regulation supervision and monitoring there is… a possibility that we… put it into writing… as an information paper to all undertakings which operated at that time on the Austrian network that we brought the new regulation into force, in which act of their applications or the processes they have to consider them. So this is part of our information, when something on this above national level is coming into force we put this also in writing as an information to the undertakings." *Our opinion: It is good practice to issue guidance related to new regulations to make RUs/IMs aware of the salient points and develop a uniform understanding.*			2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	BG	Measures taken to be transparent with the market include: • Advance warning of proactive supervision/auditing, with questions issued beforehand so the RU/IM can prepare. • Consultation with the whole market when there is a need for legislative change. • Seminars and twinning project for when Bulgaria joined the EU to educate the entire sector. • The NSA website which is regularly updated with legislation. *Our opinion: The use of seminars is a good practice example of how to engage with the market beyond simply having a website of information and guidance.*			2				
I	Rail	PL	Although "the principle of transparency is not part of our legal system", the Polish NSA has several measures to improve transparency: • "We… publish those legal instruments that apply to the railway sector on our website." • "When they apply for certification, they are made aware of the expectations…" • "Before an inspection takes place, the entity to undergo it has to receive some notice [one week] describing the scope of the planned inspection." • "We publish on our website the non-legislative documents prepared in the EU, which explain a lot of the issues that may not be completely clear from reading the legislative text." The documents are usually translated into Polish, although they do not stand as official translations. Through meetings and other contact with RUs/IMs, the NSA has learnt that the website is commonly used and the market is positive about the assistance provided by the NSA. The NSA also participates in seminars and workshops as a way of communicating with and guiding the market; however, poor transposition of Article 16.2(f) of the Safety Directive means that it has no powers or funding available explicitly for these activities. *Our opinion: The NSA is attempting to communicate essential information to the market and is assisting them, where possible with understanding the documents. It is likely that the NSA would do more in this field if it had both the remit and the funding.*			2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	E	The NSA is considering how it will communicate guidance to the sector and explain its role: "We will inform… the sector of our procedures so they could expect what we will ask them to develop. So we're going to give all our procedures to the RUs. We consider that we have to develop one consistent structure of NSA activity and it could be appropriate that the sector knows what our guidance, our principles, and perhaps via internet or via meetings... We are making supervision and enforcement, but not make them to feel like we are police. And we will try to make them to see that we are a part of this business and perhaps with a service pledge. We will have something to discuss." *Our opinion: This is further evidence that the NSA wishes to take a relatively collaborative approach to supervision, working with the industry. It is keen to avoid any negative associations that might be related to its role as a regulator.*	1		1				
I	Rail	D	"…concerning this principle of transparencies… we think the general aspects of our supervision are defined in the regulations [administrative procedures] which are published [online]. Everyone can read that and can see what, in principle, we do or what we expect, the ones we supervise… should do or what they should provide towards us, including on a general level the methods we used. So we think everything that's necessary is there. For all the rest it's the general principle of administrative law once again. We have to be as transparent as possible. We have to hear the ones we supervise before we reach any decision. If there is danger we have to act immediately but, in general, we have to make a hearing to collect their view, to discuss it with them and then, if we issue any kind of decision, then this is subject to review. So that's also an aspect of transparency, in my point of view. So that's how we think we fulfil the requirement of transparency. The other way is the yearly discussions with the single undertakings but that's only on a bilateral basis between the NSA and the respective undertakings. If there's something new, some law has been changed, something from Europe or whatever, then we do… workshops or information sessions or we issue information in writing, or a letter to all who need it. That's not something… we use regularly but only in exceptional cases where we think it's necessary. So, for example, when the whole certification thing came up, we informed everyone by our letter and made three workshops/information sessions, however you may call it, around Germany, to offer the information and the possibility to inform to everyone.			2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			I think there's always room for improvement. We could maybe think about offering workshops more frequently or on a regular basis, which we didn't do up to now. We saw, last year when we had the European Railway Agency here, in Bonne, for a workshop on SMS and CSM on conformity assessment and ECM aspects there was a high interest from the sector and many people said why not do this more frequently or on a regular basis to have such discussions. That's maybe something that could be intensified in the future." *Our opinion: In common with other NSA, the German NSA relies on the documents it publishes via its website as its main method of communication with the market. Although it asserts that all RUs/IMs can access these documents, it does not necessarily mean that they do – or that the information is understood and adopted where appropriate. The substantial interest that the German rail market has shown in the workshops that have been offered could indicate that there is a desire for greater communication and engagement with the NSA. That desire has been recognised and the NSA would like to provide more, although there are no firm plans to deliver more workshops or similar activities in the future. Other methods of communication include direct mailings to inform RUs/IMs of new legislation or issues but this is only done where the NSA perceives it to be necessary.*							

Table B.30: Examples of guidance issued by authorities

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	GB	"Recover more of our costs, by recognising the value of the experience and material HSE has, and charging for it where there is legitimate scope to do so; and seek to level the playing field by ensuring that those businesses which create risks by operating outside of the law, or where a continuing high level of engagement is required, meet more of the regulator's costs that are generated as a result. HSE will be consulting on proposals to introduce such arrangements." *Our opinion: The approach outlined here suggests that competent authorities can package and sell their knowledge and support services where appropriate to generate additional income for supervision and enforcement—provided that the level of maturity is there in the first instance. If applied in the rail environment, care would need to be taken to ensure that any such services were provided ethically and did not influence the decisions made by NSA. The sale of support and advice should also not interfere with an NSA's function to promote and develop the safety regulatory framework within its Member State. In addition, the GB HSE is exploring how to offset its regulatory costs when extensive involvement is required to rectify breaches. This approach does not demonstrate good practice. The sale of guidance that is then used for the purpose of supervision and enforcement is a conflict of interest. The process generates soft legislation from guidance. The safety authority must also be completely confident that its guidance is beyond reproach.*			-1	-1			1
D	Oil and gas	B	The Metatechnical Evaluation System (MES) is intended for the systematic auditing of the organisational and managerial competence of the companies that are concerned with managing of the risks of major chemical accidents. The MES is organised as a questionnaire, with each question having a set of measures (or sub-questions) which the dutyholder is expected to answer coherently and concisely. Each question has a set of criteria against which the dutyholder is measured. The MES requires that audits are regular. Components of the MES can be used separately. Dutyholders must be warned of the audit in advance and should prepare written responses to each question. Each response should take 5-7 minutes and no longer than 10. Pre-audit procedures require all relevant documents to be sent in advance. Inspectors have the authority to demand ALL documents necessary for the audit. The main audit is an interview, during which time documents can be consulted and other staff interviewed. Failures in the SMS must be reported within 2 weeks. Reporting is recommended in a tabular form ordered by priority of shortcomings. A corrective action plan will usually be agreed and delivered within 2-3 months. Evaluation may be looking at individual points or re-applying the MES for affected sections.		2	2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: Demonstrates consistency and transparency in health and safety auditing. Dutyholders can access the criteria by which they will be assessed. The tool is flexible enough to be used in whole or part. The design of the questions means that the audit process can be repeated to monitor changes in compliance for a dutyholder's SMS. It is good practice for an NSA to establish its expectations of the market and disseminate these expectations in a way that is structured to mirror the audit requirements.							
D	OSH	DK	Starter kits for new enterprises – new initiative to develop a starter kit on the working environment for newly established enterprises with employees. This starter kit will provide enterprises with an introduction to the requirements stipulated in the Working Environment Act for enterprises with employees. For instance, the starter kit informs enterprises of the requirement to prepare a workplace assessment and where they can find the help they need for this. Enterprises will receive the starter kit when the Danish Working Environment Authority becomes aware of the fact that the enterprise in question has employees. *Our opinion: Good practice to help new dutyholders achieve compliance from the outset. Sending to enterprises based on knowledge of employees being registered means that the authority is proactively contacting dutyholders rather than informing them of their duties reactively or through inspections.*			2			1	1
D	Aviation	F	Provides case studies describing actions taken on safety recommendations. These studies describe the incident, recommendations made, response and stage of completion for each recommendation. There are five case studies. *Our opinion: It is good practice for guidance to be based on real-world examples.*			2				
D	Rail	LV	Checklists and guides are organised into the four principles and 13 components of successful SMS to ensure a clear structure. Checklists include useful printable forms for tasks such as gap analysis, and series of questions to test implementation and understanding of the organisation's SMS at all levels (accountable managers, functional department heads and employees). *Our opinion: Resources that help RUs/IMs fulfil their obligations through self-assessment are considered good practice. Not only does this help RUs/IMs reach the necessary levels of compliance (thus making it less burdensome when supervision activity occurs), it also helps safety authorities target their resources more usefully by potentially reducing the number of revisions that must be advised during a supervision activity. Better prepared RUs/IMs are more likely to meet requirements.*		1	2			1	1

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	IRL	BeSMART tool – Business electronic Safety Management and Risk assessment Tool for small businesses This is a free tool designed for small businesses with the aim of helping dutyholders to identify hazards, prepare risk assessments and safety statements. It is accessible from the HSA. Users are required to set up an account, select their business type and then they can begin using the tool. The tool guides dutyholders through lists of hazards associated with their particular business type and describes controls that could be used to mitigate the risk. The tool then uses this information to generate a risk assessment and a safety statement (including an 'action list' for things that need improving. The tool has video demonstrations and online help facilities as well as a telephone support system. Also available for download are risk assessment templates and fire safety checklists. *Our opinion: There are several key benefits to this type of system: it is free to small businesses, so it is an accessible tool, it stores information electronically for ease of access, it offers a variety of different help facilities and it offers resources for managing risks that fall outside of the BeSMART tool (e.g. risk assessment templates).* *Not all of these approaches can be recommended as good practice. The notion of an NSA assisting a dutyholder with identification of hazards and subsequent controls is a conflict of interest given that the NSA would then be supervising the subsequent implementation of its own action plan within the dutyholder's SMS.* *However, it is good practice to offer a tool that helps guide dutyholders to the information they need, with templates and checklists to assist them with fulfilling their obligations for managing safety.*			1	-1			
D	Rail	LV	Full presentation of SMS fundamentals and an 'implementation evaluation guide' with checklists for achieving good practice *Our opinion: Resources that help RUs/IMs fulfil their obligations through self-assessment are considered good practice.*			2				
D	OSH	DK	Risk assessment support – the website has a section devoted to assisting companies with carrying out their own risk assessments. This includes a series of downloadable checklists organised by industry sector and type of work (e.g. construction > scaffolding) *Our opinion: Resources that help dutyholders fulfil their obligations through self-assessment are considered good practice.*			2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	IRL	HSA Online Courses - e-learning courses have been developed by the HSA with the aim of improving knowledge of workplace health and safety for those working within the education sector and for post primary students within the education system *Our opinion: Innovative use of newer technology (e-learning) to assist dutyholders with their knowledge and understanding of the regulations is good practice.*			2				
D	Aviation	GB	Providing information to assist organisations in preparing an SMS (guidance material, evaluation framework/gap analysis, training material, hazard log example). Includes guidance with an accessible explanation of an SMS (leaflet to download), a full guide to SMS (report to download), plus links to other respected SMS guidance. Includes downloadable tools for carrying out SMS activities (e.g. hazard log). Includes SMS Evaluation Framework/GAP Analysis - should be completed by organisations to demonstrate how they have implemented and established a working SMS. It may be used for gap analysis to assist an organisation in implementing and assessing its SMS. The completed framework should be provided to the CAA Inspector/Surveyor who will arrange a visit to assess the SMS as part of the first phase of SMS assessment. Completing the framework and arranging an assessment helps organisations to understand whether they have a working SMS to the satisfaction of the CAA. *Our opinion: Resources that help dutyholders fulfil their obligations through self-assessment are considered good practice.*			2				
I	Rail	S	"In Railway Undertaking department, in January when they [the new regulations] were in force, we started to put regulation text in what the meaning of a Safety Management System is in our old guidelines. So we renewed our guidelines and put the regulation text in it and out on the website, so companies applying for certification could see the change and here are the things we are going to evaluate for assessing your certification. And then later on we have tried to explain more in the guidelines because they were written in dry lawyer text, so we tried to explain a little bit more of what we accept from the applicants, and tried to guide them to understand what do we need for evidence; what they should have in their system." *Our opinion: It is good practice for NSA to issue guidance that can help the market understand how new regulations apply to it. Whilst the vast majority of NSA reproduce or link to regulations on their website,*			2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			it is potentially more helpful if NSA guide market players to the pertinent points.							

Table B.31: Examples of authorities engaging with research

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	DK	Working Environment Research Fund – aims to strengthen health research in Denmark through a research strategy and the distribution of funds. *Our opinion: Providing funding for research is good practice if it can support developments that have safety benefits for all dutyholders. Caution is required to ensure that funding does not provide a competitive advantage to any particular dutyholder.*						3	3
D	OSH	GB	Research: funded by the authority and published on its website, the research includes surveys of industry attitudes towards regulations and statistical analysis of incidents affecting the industry. *Our opinion: Funding research to help the safety authority develop is good practice. Greater knowledge of how the market responds to the regulatory framework can assist the authority with targeting its supervision and communication activities. Incident analysis may assist with identifying precursors to accidents providing further data to assist with targeting supervision.*			2			3	3
D	OSH	B	Grants available to support initiatives that assist workers over 45 years of age. Criteria and grant application process explained online. *Our opinion: Provides funding to support dutyholders that wish to develop practices that are not necessarily regulated but that are seen to benefit industry. This cannot be recommended as good practice in rail due to the inequalities that it may create between market entrants. It may also not be appropriate use of NSA resources. The OSH sector is somewhat different from the rail sector in this respect given that research to support different age groups of the workforce is a justifiable concern for OSH authorities.*						-1	-1
D	OSH	I	Funding for Safety at Work "INAIL promotes prevention support measures in compliance with section 23 of the Accidents at Work and Occupational Diseases (Amendment) Regulations 2000 by funding: • Programmes to adjust labour structures and organisation to the rules regarding health, hygiene and safety at work in small and medium sized businesses, in the agriculture and craft sectors, in compliance with the Health and Safety at Work (EU Directive NO 89/391/EEC Application) Regulations 1994. • Training and information projects on dangers and risks at work in the company and the related prevention measures, as well as projects for the production of information, including multimedia products and databanks made available to anyone either for free or at a production price. *Our opinion: Funding training and information to address risks within the businesses of dutyholders may encroach on the responsibilities of dutyholders to manage their own risks.*						-1	-1

Table B.32: Examples of authorities issuing rewards

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	Aviation	N	Presents an annual safety trophy. Criteria for nominees are: good safety performance; awareness of their own efforts in security work and promote a good safety culture; have developed, implemented, maintained or revised administrative or operational systems that have given positive results; the effort should have been carried out over at least five years. (Also open to aviation clubs). *Our opinion: This may not represent good practice as it could polarise the rail market.*		-1				-1	-1
D	OSH	D	The German Work Award – "the award recognised companies that commit to a particular degree of health and safety at work. Companies need to demonstrate concrete examples from practice that make it clear that they've increased innovation and long term health and safety measures that create value for both the employees and the company." *Our opinion: This may not represent good practice as it could polarise the rail market.*		-1				-1	-1
D	OSH	A	State Prize Safety Award – annual award ceremony for companies who excel in health and safety. Website provides details on winners' projects and all that have been nominated (video presentations). *Our opinion: This may not represent good practice as it could polarise the rail market.*		-1				-1	-1
D	OSH	A	Office Manager Award – provided to a dutyholder with a long history, during which many enforcement and supervision actions had been taken. Award was for consolidating internal practices to satisfy all previous actions and provide one systematic approach. *Our opinion: This may not represent good practice as it could polarise the rail market.*		-1				-1	-1
D	OSH	D	The German Work Award – "the award recognised companies that commit to a particular degree of health and safety at work. Companies need to demonstrate concrete examples from practice that make it clear that they've increased innovation and long term health and safety measures that create value for both the employees and the company." Publishes photographs and names the winning dutyholders and their organisations on the website, as well as describing how many other organisations entered the competition. The judging panel is made up of field experts and the candidates are all measured against the same criteria: Efficiency and cost-effectiveness; Innovation; Implementation; Transferability. *Our opinion: This may not represent good practice as it could polarise the rail market.*		-1				-1	-1

Table B.33: Penalties notified to the EC under Article 32 of the Safety Directive

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
Great Britain	Powers: Enforcement notices and prosecution, withdrawal, restriction, make safe, prohibit and destroy. The GB NSA does not have powers to issue fines. It can only prosecute in court. There were 8 prosecutions in 2010/11 (for offences occurring in earlier years). Prosecutions can result in a fine and a maximum of two years imprisonment. (In addition, 12 prohibition notices and 36 improvement notices were served to RUs/IMs although these do not amount to penalties).					
Sweden	Submit to RU (23 times) or IM (25 times)	Submit for the penalty (0 times)	Prohibit RU 2 IM (2 times)	Revoke RU 3 IM (1 time)	To prosecutors for RU (1 time), for IM (0 times)	-
Estonia	Violation of Railway Technical Rules: fine for IM/RU up to 3200 EUR (2 times)	The railway-construction without permission: fine for IM up to 3200 EUR (2 times)	-	-	-	-
Lithuania	Powers: Option to suspend safety certificate or authorisation. Penalties notified to the Commission include: 100–2000 LTL for illegal passenger activity (e.g. littering). 50-1000 LTL for violations of rail traffic safety. 100-1000 LTL for concealing or failing to investigate an incident. 500-1000 LTL for unauthorised use of subsystems/rolling stock.					

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
	100-500 LTL for violations of the register. 50-500 LTL for failing to comply with or obstructing the duties of railway transport control officers. The above are listed amendments to the original act. The original act is thought to contain larger fines for more serious infringements.					
Romania	No information on penalties given in questionnaire. Notified to the Commission are fines from 5,000-20,000 ROL.					
Germany	No statistics available and no penalties reported in questionnaire. Fines of up to €10,000 and €50,000 specified but without details on reasons for application.					
Denmark	Comments: Small discrepancies (in general). Given on all audits	Findings (N.C): Small discrepancies (in SMS, not safety related). Given on almost all audits	Injunction: Safety related issues. (Once or twice a year)	Prohibition: Safety related issues. (Once or twice a year)	Report to police: almost never	Revoke the license / approval: have not yet been done
	No notifications to the Commission.					
Spain	Currently it does not apply. When a supervision/enforcement method is established (currently under development) we will consider the penalties set out in Title VII from 91/2003 Law of the Railway Sector. These penalties will be: €30,001–300,000 for very serious offences: endangering safety; operating without safety certification/authorisation; obtaining certification/authorisation by deception; disruption to the railways caused by failure to follow rules; obstructing rail market; failures to correctly transport hazardous goods that are very serious; working on the railway without authorisation, with very serious consequences. Two or more					

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
	infringements in a year may lead to further administrative decisions. €6,001—30,000 for serious offences: unreasonable service interruption; congestion due to unused capacity; withholding information; refusing/obstructing inspections; the use of unsafe/uncertified equipment that is not a very serious offence; failure to guarantee consumer/user rights; failures to correctly transport hazardous goods that are not considered very serious; working on the railway without authorisation, but not with very serious consequences. €6,000 for minor offences: typically relate to offences by passengers (e.g. using the emergency brake on the train unnecessarily). Fines may be multiplied by three times the profit made, if they have led to profit. Very serious infringements may lead to revocation or suspension of certification/authorisation for up to one year. Affected rolling stock could be sealed and stopped. The amount of the sanction imposed will graduate according to the following factors: a) social impact of the offence and the danger for life and health of people, the safety of things and the environment. b) The importance of damage or deterioration caused. c) The intent. d) The benefit obtained. e) Prior offences. f) Remedial action taken prior to any regulatory action, if any.					
Latvia	Financial penalty (3 times)	Powers: Able to stop the movement of trains, to reduce the speed of trains and to prohibit the utilisation of technical equipment if the safety of humans and environment is at danger. Until non-compliances are corrected to stop the utilisation of rolling stock and/or railway infrastructure. To issue a financial penalty. No penalties/fines in notified documents to the Commission.				

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
Poland	Powers: Decisions with immediate effect forcing RU / IM to act in line with requirements, then penalties if the decisions are not implemented by RU / IM, decisions on closing lines or excluding vehicles from operation in case serious risks are identified. The penalties can be applied both to the whole undertaking and to the members of board. Penalties, their amount, kinds etc. are set by the state. NSA is not capable of doing this. Railway Transport Act of 28th March 2003 with amendments sets several penalties, including: - possibility to issue a fine for up to 5000 euro per day of non-compliance of its decisions; - suspending or restricting railway traffic on a certain line or forcing withdrawal of a railway vehicle from service or restricting its usage, if it's required in terms of safety of railway traffic and transportation of goods and passengers; - forbidding the use of a subsystem or an interoperability constituent, which does not fulfil the essential requirements for up to 2 months with possibility to lengthen this period; - revoking an issued document (safety certificate / authorization, train driver's license etc.). During last year none of these penalties was used.					
Bulgaria	Any revocation of an IM safety certificate will include a proprietary penalty of 100,000 BGN. - Not applied in the last 12 months.	Any IM that infringes an RU's right of access to the railway infrastructure shall be punished by a proprietary penalty of 10,000 to 100,000 BGN. - Not applied in the last 12 months.	Any RU using rolling stock on the railway infrastructure without the relevant authorisation shall be punished by a proprietary sanction from 1,000 to 10,000 BGN. - Not applied in the last 12 months.	Proprietary sanction from 5000 to 50000 BGN shall be imposed to a railway carrier or a chief executive of the infrastructure who has failed to fulfil any obligation of his/hers or who has in any other way treated unfaithfully,	There are provisions regulating the financial penalties imposed on RUs and IM that do not comply with the requirements of Regulation 1371/2007.	Additional: Sliding scale of smaller fines applicable to infringements that are not punishable by heavier penalties. These fines range from 50-1000BGN for specific violations that

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
				discriminated or affected another carrier. - Not applied in the last 12 months (not in notified penalties/not translated).		(e.g. SPADs). Penalties of 50,000-100,000 BGN for any RU operating without a certificate, or with an expired certificate.
	Additional Bulgarian penalties exist and are wide-ranging. Penalties for other offences can reach 50,000BGN. Penalties can increase for repeat offences.					
Austria	No information on penalties given in questionnaire. Notified to the Commission: Fine of up to €20,000 under Federal Law (or imprisonment for up to 6 weeks if unpaid).					
Portugal	No information on penalties given in questionnaire. Notified to the Commission: Fine of €1000 to €3,740 for offences by an individual. Fine of €2,500 to €15,000 for offences by a legal person. Fines of €10,000 to €44,800 for unauthorised/unlicensed operations, failures to comply with licensing conditions, violations by the IM/RU of various regulations.					
Czech Republic	Operate without safe	Operate unauthorised	Operate driver without	Does not follow	Does not notify	Does not deliver

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
	certification (up to 20m CZK) - exceptionally.	vehicle (up to 20m CZK) - exceptionally.	licence (up to 1m CZK) - exceptionally.	operational rules of IM - exceptionally	changes of SMS system - exceptionally.	annual report of safety - exceptionally.
	Multiple acts appear relevant and exceed the scope specified in the questionnaire, e.g.: Penalties of up to 10,000 CZK for failing to provide data as a rail vehicle owner. Penalties of up to 100,000 CZK for an RU/IM that disobeys a supervision order. Penalties of up to 1m CZK for rail damage or disruption; an RU that fails to report an incident or identify its cause; an RU that fails to implement measures in the specified time frame to prevent potential incidents. Penalties of up to 10m CZK for the owner of an IM who fails to maintain or repair the railway to the required standard for operability, or fails to facilitate interoperability. Penalties of up to 20m CZK for use of unauthorised vehicles, or deceptive use of certification marks; for failure to comply with protective measures; and for failure to rectify the aforementioned violations. Sliding scale of fines for violating regulations regarding use of emergency oil stocks.					
Netherlands	Admin fine imposed when an order is not observed. Issued 3 times.	Admin penalty that can cover any action, e.g. stopping the rail traffic. Imposed 2 times.	Admin fine applied directly (not after an order). Imposed 3 times.			
Channel Tunnel	For the GB half of the Tunnel, the IGC has recourse (through enforcement by ORR) to the full range of enforcement measures available under GB law where an RU or IM fails to comply with the safety regulatory framework. This includes, among other measures, powers to serve improvement					

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
	and prohibition notices and to prosecute offences (which can lead to fines or imprisonment). The IGC has not needed to take any enforcement action in the last 12 months. For the FR half of the tunnel, the only possible penalties under French law are the withdrawal or the restriction of the given authorisations. The IGC has not needed to take any enforcement action in the last 12 months.					
Hungary	None in questionnaire. From documents, penalties can include: • Pay costs associated with the breach. • A fine. • Impose conditions for operation. • Prohibit the activity. • Suspend or revoke safety certificate/authorisation.					
Norway	None in questionnaire and none notified in translated documents.					
Ireland	NSA use enforcement powers laid down by legislation: • Improvement plan. 7 times • Improvement notice. 0 times • Prohibition notice. 0 times • Prosecution. 0 times					

NSA	Penalty 1 and frequency	Penalty 2 and frequency	Penalty 3 and frequency	Penalty 4 and frequency	Penalty 5 and frequency	Penalty 6 and frequency
France	The EPSF may establish records which may provide a basis for criminal prosecution (after transmission to the public prosecutor). This includes: - If an RU/IM operates a motor vehicle in violation of provisions relating to registration or authorization of commercial operation. - The act of driving a train without being the holder of the license and the documents required by safety regulations or affect the conduct of a trainer who does not hold these documents.					
Finland	-					
Italy	A Legislative Decree about Penalties is currently in progress and it is expected to be adopted within a few months. Consequently, no penalties have been set or applied.					

Table B.34: Range of enforcement powers - desktop and interview findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	DK	The organisation lists the legal enforcement powers and penalties that it can apply to infringements of the safety regulatory framework: Prohibition - The company may receive a ban to continue working if there is an imminent and substantial danger to employees or others' safety and health. A ban means that work must stop immediately and that it should not be resumed until it can be performed safely. Immediate Injunction - The company can get an immediate injunction if there is a serious safety problem. An immediate injunction means that the error must be corrected immediately. Companies that have an immediate injunction, may be allowed to solve the problem temporarily, until it is possible to solve the problem permanently. Injunction with deadline - An injunction deadline means that the company can continue production, but that it must find a permanent solution to the problem before the deadline. Working Environment Authority will set a time limit is long enough to ensure that the company is allowed sufficient time to find a good and viable solution to the problem. Investigation Injunction The company can obtain a survey injunction if WEA has a concrete suspicion that working conditions are not safe and healthy sound, or as part of a more general investigation or ongoing monitoring of conditions in such an industry. The order requires the company to carry out investigations, take samples or carry ou inspections to determine if working conditions are reasonable. If the company gets an order to investigate the psychological well-being of staff, the study should be conducted by a qualified safety consultant. Act without orders - If a company brings a violation in order after the WEA has been visiting, but before the order is sent to the company, the Labour Inspectorate does not make an order. In this situation the company will instead receive a ruling that found a violation when the Labour Inspectorate was on supervisory visits. The company will also learn when not to take any further action since the relationship has been restored. Administrative fines - The Company may receive an administrative fine in the case of coarse material violations by clear and generally well-known areas of OSH Act. Working Environment Authority shall not issue administrative fines if the violation is clear and straightforward and not discretionary. An administrative fine is an offer for the company that it may close the case if it pays the fine within the deadline. The company therefore has a right not to pay the fine, but the Labour Inspectorate will then set the company to court prosecution after the payment deadline. Police report - The company may be reported to the police if there is a serious breach of safety law or if it does not comply with WEA orders. Police may subsequently indict the company. It is the prosecutor who	3						

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			decides whether to take criminal proceedings against the company and it is the prosecution which must prove it. Violation of OSH Act is punishable by a fine normally, but in particularly serious cases a custodial sentence. *Our opinion: Clear listings of enforcement powers. The use of different injunctions helps tailor the enforcement to the type of breach.*							
D	OSH	GB	"Enforcing authorities have a range of tools at their disposal in seeking to secure compliance… Giving information and advice, issuing improvement or prohibition notices, and withdrawal or variation of licences or other authorisations are the main means. A prohibition notice stops work in order to prevent serious personal injury." The main tools are: • Giving information and advice face to face and/or in writing, which may include warning them that they are failing to comply with the law. • Improvement or prohibition notices (a prohibition notice stops work in order to prevent serious personal injury). Information on improvement and prohibition notices should be made publicly available. • Withdrawal or variation of licences or other authorisations. • Prosecution (and if appropriate, cautions) to bring dutyholders to account for alleged breaches of the law. Where it is appropriate to do so, prosecution or cautions should be used in conjunction with improvement or prohibition notices. *Our opinion: It is good practice to have a range of enforcement tools.*	2						
I	Rail	NL	Dutch NSA has developed a pyramid of enforcement methods. From top to bottom, the range of enforcement methods are: • Withdraw/revoke safety certificate/authorisation • Criminal sanctions • Administrative sanctions • Publication/disclosure • Warnings • Recommendations • Agreements with the sector	3		2				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			• Rewards • Guidance *Our opinion: The pyramid illustrates the NSA's policy towards enforcement: the majority of RUs/IMs will be subject to 'enforcement' activity that exists at the lower reaches of the pyramid, encompassing activities such as guidance, agreements and recommendations. Scaling the pyramid, the severity of enforcement methods increases but the frequency of application decreases.*							
I	Rail	DK	By way of enforcement, the NSA issues: • Observations/remarks: In some cases, the NSA will come across many circumstances during an audit which require a response from the RU/IM but which are not deemed an actual nonconformity. Such remarks are recorded in the subsequent supervision memo or supervision report. The remarks should be taken into consideration in the further work of the RU/IM relating to the safety management system. It is likely that the areas mentioned will be followed up by the NSA in future supervisory measures. The NSA expects the RU/IM to respond to the remarks and to justify the choices that it makes based on its safety management system. • Non-conformities: If, in connection with an audit, the NSA establishes that the undertaking is not complying with its own safety procedures, or that the undertaking is not adequately ensuring compliance with applicable requirements concerning safety management systems, a nonconformity is deemed to exist. A nonconformity is objective confirmation that a given requirement is not being met in its entirety. Confirmation of a nonconformity will not normally result in railway safety being in direct danger. If railway safety is at risk, the nonconformity will be accompanied by an order or ban. A nonconformity will usually mean that the undertaking must implement measures to fulfil the requirements that are not being complied with. This will usually be a change in behaviour or procedure or the production of missing documentation. A nonconformity is not an Authority decision but a step towards ensuring that the undertaking's management system fulfils applicable requirements. The RU/IM must acknowledge receipt and acceptance of the nonconformity and deadline. (If a similar issue is identified during assessment, it is classified as a 'deficiency' as the SMS has not yet been certified).	2		1				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			• Orders/bans: if the NSA identifies circumstances in which safety is at risk, it can order an RU/IM to rectify the situation either immediately or by a deadline. The NSA may ban an activity if the risk to safety is substantial. Verbal bans last for 3 days and written bans for 14 days. Both can be extended. Failure to comply with deadlines can lead to: further bans; suspension of operations; NSA action (at the expense of the RU/IM); revocation of authorisations; police action, which may result in a fine. *Our opinion: It is good practice to have a range of enforcement tools.*							
I	Rail	PL	The NSA described the range of enforcement methods it has available: • "The traditional control is… a report is produced after the control [supervision activity/inspection]. The contents are agreed with the railway undertaking and… recommendations are issued. This is a way to influence the railway undertaking in a given matter, be it very specific or be it something general. Once the railway undertaking gets the recommendations, they have deadlines to comply with various recommendations and those deadlines depend on a given case. If it's a relatively small violation, there can be quite a long deadline for improvement." • "If we see a threat to safety, we can even suspend a given device or vehicle from operation." • "It is quite rare that inspectors make motions for penalties – by penalties, we mean financial penalties. We have two types of penalties available. Both are administrative penalties. The first kind is regulated by article 66 of the Railway Transport Act, the main instrument regulating the railways. It can be a penalty of up to 2% of the entity's revenue. However, it's a lengthy procedure, it requires a lot of effort and for these reasons it is very rarely applied. The first step is to request that the undertaking removes the violation, cures the situation, depending on what it is. We don't often apply this sort of procedure because we would need lawyers and more staff to enforce the penalty. This is generally lengthy and quite a lot of effort is needed." • "The other penalty is regulated in the same Act, in article 65. It's a fine according to the Petty Offences Act, provisions. The word used is 'idiotic', because it means judicial actions. You take the entity to court."	1						

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			"What we don't have and what we would find much more useful would be the right to impose penal tickets [administrative fines for summary offences], because they would be a simple and efficient way to change the behaviours, to discipline the railway undertakings. It is a measure that is applied in other sectors of transport so it is only our office which cannot impose tickets. However, talking of efficiency, another specific example; this office is, at the same time, the National Safety Authority, the market regulator and the passenger rights watchdog. So in terms of passenger rights, last year, exactly a year ago, in March, three penalties were imposed for breaching passenger rights; quite notable amounts. Two entities were ordered to pay 0.5 million zloty and one smaller penalty. Until today, no money has been paid because you can appeal against the decision and then it's a judicial procedure which can take years." *Our opinion: A limited range of enforcement powers is available to the NSA, and stricter controls are both difficult to administer and not entirely successful due to the associated legal process. The NSA has identified that 'penal tickets' would enable it to conduct its activities more efficiently and forcefully but it is not able to introduce this change. This also highlights inconsistency in enforcement powers afforded to the NSA and to other transport sectors in Poland.*							
I	Rail	GB	"The enforcement policies that we've got very much reflect HSE's enforcement policies in general health and safety issues, so we try and adopt the same approach so that we are consistent" *Our opinion: This NSA has general enforcement policies that mirror the policies of other competent authorities in the Member State (e.g. for OHS). The overall framework of enforcement was described as broadly similar: for example, the inspection and enforcement process is relatively independent of the industry sector and staff carrying out this function can benefit from following the same legal procedures and training programmes. Often, similar enforcement measures can be taken (e.g. enforcement notices, prohibitions, prosecutions) so the same legal reasoning is required. However, this NSA had tailored the general approach to enforcement so that it met the specific requirements of the rail industry. It is important to permit flexibility in following a single model of enforcement so that it can be adapted accordingly. In summary, it is efficient and consistent to adapt a single enforcement regime to different industries such as rail, so long as some adaptation is permitted.*		2					

Table B.35: Application of enforcement powers - desktop and interview findings

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	DK	Differentiated administrative fines – the WEA will operate sliding scale of fines that increases according to the size of the dutyholder. • Small enterprises with one to nine employees that violate the Danish Working Environment Act will receive a standard fine. • Medium-sized enterprises with 10-34 employees will receive a standard fine plus 50% (however, not for procedural violations). • Large enterprises with 35-99 employees will receive a standard fine plus 75% (however, not for procedural violations). • Larger enterprises with more than 100 employees will receive a standard fine plus 100% (however, not for procedural violations). *Our opinion: Fairer distribution of penalties according to a defined metric (in this example, it is dutyholder size as measured by the number of employees). Other metrics may be appropriate for administrative fines. Defining the approach to administrative fines is one method of achieving proportionality – and the process of defining and publishing the system of fines achieves consistency and transparency.*	3	2	2				
D	OSH	GB	Combining penalties: "Prosecution and, if appropriate, simple cautions are important ways to bring dutyholders to account for alleged breaches of the law. Where it is appropriate to do so in accordance with this policy, enforcing authorities should use one of these measures in addition to issuing an improvement or prohibition notice." *Our opinion: Enforcement tools can be combined to adjust the severity. A smaller range of tools can be available if this approach is used, because the scope for combining methods of enforcement can expand the range of tools available. This safety authority has emphasised that policy goals may encourage additional action that goes beyond addressing the breach with a notice to improve or ban the activity; such goals may, for example, be linked to supervision targets or issues that are in the public interest.*	2						
D	OSH	GB	Prosecutions: The authority expects discretion to be used for deciding when to prosecute. Prosecutions are also advised "as a way to draw general attention to the need for compliance with the law and the maintenance of standards required by law, and conviction may deter others from similar failures to comply with the law", or if investigation or regulatory contact has taken place	2					2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			but "a breach which gives rise to significant risk has continued despite relevant warnings from employees, or their representatives, or from others affected by a work activity". *Our opinion: the remit under OHS may have different criteria to rail. However, the need for discretion is valid, as is the potential for deterring other dutyholders from similar actions. Prosecution is considered as the highest level of enforcement and is a potentially useful tool when it is necessary to escalate a response.*							
I	Rail	GB	Financial penalties: not used by this NSA. Did consider applying penalties but RUs/IMs were not keen: "They understand the principle that up until prosecution, they might not like enforcement notices, but most of them see that they've made a significant error for whatever reason and they agree that they've got to put it right. They might not like the principle that they've had an enforcement which is telling them to do that, but underneath they know they've got to rectify it and it's not until you get to prosecution that real financial penalty or a straight financial penalty kicks in." NSA argues that applying financial penalties places additional burden to be accountable for being consistent and proportionate which can be difficult when calculating the size of a fine. Prefer this process to be done through prosecutions. Also legal framework means that NSA does not receive income from fines so it does not help to cover the direct cost of regulation. Also RUs/IMs pay a financial safety levy to fund the NSA so further fixed fines were considered disproportionate. *Our opinion: A range of enforcement tools should be available. NSA are free to decide on the appropriateness of each tool. The discussion here explains why administrative penalties are not considered useful by some NSA.*	2	2				2	
I	Rail	NL	This NSA has established a working group with the Ministry to deliver improvements to the range of penalties it can use. The NSA is aware that its national legislation was drafted at a time when railways were a state operation; consequently, the legislation is not designed for enforcement and it is difficult to find a legal basis for issuing administrative fees as a sanction. The working group has a priority to ensure that all railway violations can be punished with an administrative fee. This will be delivered within the next year. *Our opinion: It is desirable to update or abolish national safety rules that are incompatible with the current approach to running a European rail network. In this example, the Member State is required to have rules on applicable penalties so it is recommended as good practice for the NSA*	3	3	2	2			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			and ruling Ministry to have established a working group with the purpose of updating parts of the legislation so that they are fit for purpose. It is also good practice to have a timescale attached to such tasks, as shown here.							
I	Rail	DK	The NSA is not certain if it is satisfied with its current legal powers. "We have not gone to the borders of the legal powers we have today. We are of the opinion that it could be beneficial to have a more widespread catalogue of possibilities, for instance fines for not answering a deadline. That's not possible for the time being. We have discussed it with the ministries of justice and they said well, until you exploit the powers you have, you will not get any more. If you come back and say we have tried everything and it's not working, probably we would like to have more powers, then we can discuss that you can have more powers." The NSA has raised this issue because it is concerned that the current range of enforcement measures does not cover a broad enough spectrum of action: "We have two steps for the time being; we have a ban and we have almost nothing. A ban is in line with revoking an authorisation but it's quite out of proportion and the ban is also a very huge step and we get in trouble with the proportionality." *Our opinion: A good practice approach to enforcement requires a range of responses that permit a proportionate response. This NSA is concerned that it does not have sufficient power to enforce its will without resorting to extreme measures such as a ban (or a prosecution). Administrative fines were raised as one option but this would only be considered once the existing powers had proven to be insufficient. It may not be considered good practice to wait for deficiencies to appear in the enforcement powers before taking action, especially if the NSA is aware that it may be difficult to act proportionately.*	-1	-1					
I	Rail	A	"We have a general administrative regulation which says every action of [the] authority must be legally based, so non-legal is something out of our influence. If we take written reaction, it's mostly resulting in some enforcement action. The non-written advice is mostly done in meetings of course with protocols done about them, but it's something that we reach a common result at the end of the meeting…" *Our opinion: This NSA, as with others, is required to take action that has a legal basis.*				2			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	BG	"Sometimes we have some certain difficulties when applying the penalties, from the point of view of the fact that they have to be specifically described in the Railway Transport Act. The Railway Transport Act cannot cover absolutely all sorts of penalties, and sometimes there are occurrences of such deficiencies… for which the law does not prescribe a specific penalty. And for which we write letters to the respective managers of the Railway Undertakings to take measures. In our Railway Transport Act, the sanctions or the penalties are divided for physical persons, which means staff of employees of the Railway Undertakings and Infrastructure Manager, and for legal entities, which means the Railway Undertakings and Infrastructure Manager themselves. These lacks or shortages are for physical persons, they concern physical persons." *Our opinion: An NSA's enforcement function can be hindered by national legislation that has not kept pace with the European approach to rail regulation. Outdated national laws can restrict the enforcement actions of an NSA – a good practice approach would be to work collaboratively with the government to address any deficiencies in the national regulatory framework (as the Dutch NSA has described).*	-1	-1					
I	Rail	CZ	The NSA has to follow an Administrative Code which appears to complicate the process of taking immediate action if there is a threat to safety: "Disadvantage is that this administrative procedure is… very difficult… in this Act we have to find the legal way how to stop operation from day to day, and exclude possibility to appeal. Not possibility to appeal, but postpone to the decision in case of appeal. They always have right to appeal. And if we don't… follow this act properly… in case of appeal, the Ministry cancel our decision and send the file back to start the process again. And it's very, very simple to make mistake in this process. We have to inform everybody who can be by our decision influence, ask them for evidence, ask them for their opinion, make a decision, send the decision to everybody, and they, for a time, for when they can appeal. And in case that nobody appeals, the decision is valid. In case that somebody appeals, we have to inform everybody. They can express its opinion for the appeal of some of the actors, and then we pack it together and send to the Ministry of Transport. And Ministry of Transport check completely the process from the beginning to the decision, and decide. So I think this act guarantee the transparency."	-1	-1	1	-1			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Our opinion: The legal process described is clearly transparent although in delivering transparency, the NSA may find that it is unable to act immediately in the interests of safety.							
I	Rail	CZ	The NSA reported that it has difficulty finding a legal basis for issuing penalties: "Penalties are mainly, and almost only with something extreme, if somebody breaks this Act, and not other rules. We can say, we can use, in this case, some general paragraphs, general section that doesn't operate in same way, and it is much more difficult, and unclear and not transparent to say if they do it or not do it. Everything is in standards, which are not binding. Many things are in internal rules, and we can't issue penalty [for] that… For example, what is problem that completely is missing in Czech legislation [is] definitions. Each directive starts [with] definitions... These definitions are usually missing…" By way of example, the NSA explained that train drivers must know the Czech language but the Act that prescribes this does not define how this will be assessed, only that it is necessary for Czech to be the driver's mother tongue. The NSA finds it has limited legal basis to dispute the evidence offered by foreign drivers that Czech is their mother tongue as the requirement is poorly defined. The Ministry has begun drafting a new Railway Act but it is expected to take 3–4 years. The NSA reports that it has very little influence over this process and, moreover, there are few within the Ministry itself who are familiar with the European safety regulatory framework. *Our opinion: There are clear difficulties with the regulatory framework that the NSA has to follow and it does not seem as if these difficulties will be resolved satisfactorily.*			-1	-1			
I	Rail	E	The Spanish NSA reported that its enforcement powers and penalties are considered appropriate although it has not had recourse to make use of them as yet. "We consider that legal powers and penalties as a first stage is not appropriate right now because RUs/IMs are doing all that they can to make their work as the European regulatory framework is establishing, so we consider that we have to help them to adapt to the process and procedures, specific procedures to the legality of the regulatory framework. We consider that legal powers right now are not appropriate and we don't have penalties or guidelines of penalties because we are asking, we are trying that they do all that they have to develop related to the European	1						

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			regulatory framework, but it's not appropriate right now to make this, to take these penalties or legal powers in a strict, in a right way." *Our opinion: It is a potential risk that the NSA apparently has not considered the guidelines or processes that would apply if legal enforcement was required. Whilst the NSA reports that it is achieving success with its current approach of influencing behaviour, it is not clear how it would escalate its response if an RU/IM failed to make adjustments.*							
D	Aviation	IRL	Unintentional contraventions of the regulatory framework will be addressed via dialogue to agree corrective measures and an action plan to implement them. Intention is to avoid a safety culture based on fear of punitive action – employees are more likely to report safety deficiencies if such fears are removed. (This contrasts with taking punitive action against unintentional violations). *Our opinion: The underlying message in this approach to enforcement is sound: the safety authority is trying to avoid a 'blame culture' and is instead promoting a 'just culture' wherein the focus of a regulatory breach should be on how the system has failed (i.e. the SMS) rather than how individual employees have failed. The value of a systems-based approach is that individual employees may feel more able to report safety hazards if they know that the deficiency will not necessarily be linked to them as an individual. Unfortunately, the interpretation of 'unintentional' in this respect is open to discussion. If an individual employee fails to follow procedures and subsequently breaches the regulatory framework then this can be considered 'unintentional'; however, if the organisation fails to account for the regulatory framework in its rules and procedures then this can hardly be considered 'unintentional'. The statement is ambiguous in that it may lead organisations to think that they will be free from punitive action if they claim ignorance—this should not be the case if the SMS has failed to account for the regulatory framework in the first instance.*	2						
D	OSH	GB	"When inspectors issue improvement or prohibition notices; withdraw approvals; vary licence conditions or exemptions; issue formal cautions; or prosecute …ensure that a senior officer of the dutyholder concerned, at [executive] board level, is also notified." *Our opinion: This is an important point for targeting the enforcement action itself: any enforcement action of this severity should reach the highest level of management at the RU/IM. This will help to ensure that the action stimulates change at management levels above those that may be responsible for the breach directly. This process of escalation to executive board level should already exist within an organisation's SMS.*			1				

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	DK	Red, yellow, green and crown smiley – awarded on the basis of company performance. Allows the public to follow progress of a company with creating a safe and healthy working environment. Green smiley shows that the company has no dispute with the Labour Inspectorate. Yellow smiley shows that the company has received an immediate injunction, an order with a deadline, a decision on mental health, or an act without orders. Red smiley shows that the company has received a ban or a counselling order. A crown smiley shows that the company has a recognized health and safety certificate. The company has therefore made an extraordinary effort to ensure high safety standards. Green smileys can be displayed for up to 5 years, after which they expire. This coincides with the maximum period between risk-based supervision. Red and Yellow smileys are displayed for at least 6 months (even if the issue is resolved sooner) or until the triggering breach has been resolved. *Our opinion: Draws public attention to the health and safety record of a company. Motivates companies to rectify breaches – albeit, the fixed timeframe may not encourage them to do so as quickly as might be desirable. Rewards high levels of compliance. Uses a simple, RAG graphical system to rate organisations. Expiration of green smiley can be used as a prompt to the company to book a new supervision inspection with the Inspectorate, thereby sharing some responsibility for repeat inspections with the dutyholder.* *The principles on which the example is founded could be considered good practice. It makes public the relationship between the regulator and the market, and indicates clearly the recent level of enforcement activity taken by the regulator against specific dutyholders. The approach used here may risk trivialising the process; however, as a method of indicating safety management to the wider public, it is an accessible approach.*			3			2	2
D	Rail	GB	Investigation report form: a comprehensive document that captures all of the information used in an investigation in a step-by-step format. This enables the NSA to retain a documented understanding of the enforcement process and why a certain decision was recommended. Partly prompted by feedback from legal team which was unhappy with the lack of information to support a prosecution request. These report forms are used for the internal review process. Each decision is also reviewed by a		1		1			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			line manager and an approvals officer. The form was updated recently following concerns from the legal review team that it did not contain sufficient reasoning to justify the decision-making process. This has now been addressed and it mirrors the stages that are required by the EMM (the NSA's decision-making tool). *Our opinion: a standard pro-forma for recording enforcement decisions is recommended good practice. In this example, the report form follows the decision-making model used by this NSA for reaching enforcement decisions. This is a further check to ensure that staff are applying the model consistently. With all information documented in this way, review processes can be initiated on a regular basis. It also provides a foundation for accountability.*							
D	OSH	GB	Enforcement Policy Statement (http://www.hse.gov.GB/pubns/hse41.pdf): the document is available to view and download from the HSE website. It outlines the authority's proactive approach to enforcement. It reflects the principles of the Enforcement Concordat (a voluntary, non-statutory code of practice) and the Code for Crown Prosecutors (a public document, issued by the Director of Public Prosecutions that sets out the general principles Crown Prosecutors should follow when they make decisions on cases). *Our opinion: It is good practice to explain to dutyholders the purpose of enforcement action in general, and the principles that will be applied when carrying out enforcement. Although these principles exist in the regulations, there is value in each NSA describing to the market how they will enforce in accordance with these principles.*			1	1			
I	Rail	DK	This NSA explained that when there are doubts about the SMS of an organisation, it may force a full reassessment of the safety certificate/authorisation to "have a full view on how your safety management system is working". This approach may be used in situations where it is not practicable to revoke a certificate or authorisation (due to the scale of disruption it would cause to traffic) but where there is a need to send a strong message to the RU/IM about the lack of confidence the NSA has in its SMS. *Our opinion: It is good practice for NSA to be proportionate in their response and consider the wider impact on the network. Revocation of a certificate or authorisation may be impracticable in which case an approach must be taken that seeks to resolve the issues that have been identified. A full reassessment is one option available to force the RU/IM to address fundamental faults within its SMS.*	2						

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	A	The Austrian NSA describes its enforcement process: "There's also different possibilities. For instance, we may start, if we have a meeting already planned, we discuss it in a meeting, or else we put into writing, for instance, questions. Mostly we do it in this way. I wouldn't say it's advice because the first step we take, we ask questions and give the railway undertaking the opportunity to find the solution within itself. Because of course the undertaking knows best its own organisation and structures and in many cases different possibilities help solve… a question. So the first step we take… if we stay with incidents… [is if] there has to be taken immediate action because of danger there is no possibility to begin asking the railway undertaking [questions]. But if it's a normal procedure, we start in writing and do it through questions and then give the railway undertaking the opportunity to answer them and then we take the next step." *Our opinion: The NSA demonstrates good practice by using a process of questioning that encourages the RU/IM to change and develop its SMS independently. The exception is when there is a real or potential risk to safety.*			2			1	
I	Rail	BG	The national rules of Bulgaria do not permit a spectrum of enforcement (i.e. influencing or forcing behaviour): "In our case this enforcement is mandatory, in general. Concerning this soft approach, we apply both approaches, we… make consultations with them, in a way we give them guidance when there is a necessity to take some decision. So we also apply the soft approach, but the legislation is mandatory and our function does not apply to interpretive meanings. When there is a breach of law we have to enforce the respective penalties." However, the NSA may 'soften' an enforcement measure by, "giving longer periods for elimination of this breach, when the breach is small." *Our opinion: The NSA is consistent in its application of penalties when there is a breach of the law. However, it moderates its response in accordance with the severity of the breach by varying the deadline for delivering improvements. In this respect it demonstrates that it is attempting to be proportionate and is also targeting the most serious risks by making RU/IM improvements a priority.*	1	2				2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	CZ	"We don't issue penalty regularly. I think we need to have a special reason to issue a penalty. I can show you… [an] example [of a] crash at the level crossing. The level crossing was in the maintenance. So signalling system was out of order, but the employees who did the maintenance, they didn't apply for permission from the dispatcher, so the dispatcher didn't know that the signalling system is out of order. And then there went train, and crashed car. Consequences, not important. Always, fortunately, nobody was killed or injured, there was some damage in the car, and some damage in the railway car. And IM said, that it's not important problem, because it was a human failure, and he can't exclude this human failure, and he has no responsibility for this accident. But we receive some information from the police investigation, because police investigated this case as an accident, road accident. As indicate, [overtalking] here on this paper. And the result of the police was quite different. It appeared that the people who did maintenance spoke to the signaller who work in that place, appeared that they do it regularly, that they admitted that there were no reason to inform the dispatcher because they knew that at that time, no train goes. So they, I think, it appeared that they normally don't follow internal rule… normally they don't apply for permission of dispatcher because it wasn't necessary, because normal at that time no train goes. But that day… went an extraordinary unexpected train, and the result was the accident. And now we are in legal process with the infrastructure manager, we issue penalty and infrastructure manager appealed to the Ministry of Transport that the penalty wasn't in the right way, and now we don't know how the Ministry of Transport will decide, make decision about that penalty. They have three possibilities. Firstly to confirm our decision, secondly change our decision, third to cancel our decision and send the file back and we start the legal process again." The Ministry of Transport is described as the 'board of appeals' so has the final decision on whether a penalty can apply if the RU/IM objects. The appeal is because the RU/IM believes they were operating a safe and smoothly running network. In addition, "They are a state organisation, so in case of penalty they have to do everything to avoid this penalty. From the reasons to, I think, to save state money." The NSA was clear that its decision to issue a penalty would not depend on the status of the RU/IM;	-1	-1	-1			-1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			however, it could not state with confidence that the Ministry of Transport would operate with the same independence when dealing with penalties for state or private organisations. *Our opinion: This example shows that the NSA is attempting to enforce in appropriate situations. There is clear evidence that the IM has a poorly functioning SMS and further details on the case show that it took no remedial action after the event and appealed on the basis that it could not have prevented the human failure. There are several items that point towards poor practice:* • *The NSA does not appear to have issued an action plan/enforcement notice to the IM following the incident. A penalty may be a financial disincentive to continue this unsafe practice but a risk to safety is still likely given that the IM has taken no remedial action. It is unclear why the NSA did not insist on changes to the SMS.* • *It is interesting to consider why staff at the IM were not following the SMS and showing responsibility for safety. It would suggest that the SMS culture is not prevalent throughout the organisation and that staff are not fully aware of how to manage their responsibilities for safety. Other NSA have reported substantial improvements in safety culture through supervision at all levels in an organisation. It is possible that the NSA could engage better with RUs/IMs and their staff to promote the SMS-based approach.* • *Equally, it is interesting to consider why a clear failure of the SMS is not being accepted by the dutyholder. Again it would indicate a fundamental lack of understanding of the SMS-based approach, it would suggest that there is more work to be done by the NSA in guiding and promoting the safety regulatory framework, and it brings into question the value of the appeal system. As a state-run organisation, the IM is now awaiting a decision on a financial penalty from the state. The potential for bias an inconsistency in this system raises doubts about the value of issuing financial penalties (rather than using other enforcement methods) as well as the negative messages that might emerge for other market players.* *In summary, the response is:* • *Not proportionate because the NSA has not used enforcement measures that will force the IM to improve its safety management procedures to avoid such incidents in the future.* • *Not consistent because the Ministry may uphold the appeal for reasons not necessarily*							

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			related to the case (suggestion was that fining a state-run IM was not beneficial). • *Not transparent because the IM has failed to explain to the IM what it expects of the organisation (i.e. improved SMS) – the IM does not acknowledge it is at fault and demonstrates poor understanding of the SMS-based approach.* • *Not targeted – the NSA would not appear to be focusing its supervision on the most serious risks otherwise it would have identified this procedural flaw in the level crossing maintenance programme, especially given that it was a frequent occurrence.*							
I	Rail	CZ	The size of financial penalty is typically within a given range according to the legislation that applies to a specific violation. In this range, the amount is often 1% of the highest maximum penalty that can be applied. There are no documented criteria for determining the size of a penalty within a range but whether it is a first or repeated offence is often considered. *Our opinion: The NSA uses its judgement to determine the size of penalty, which demonstrates a degree of proportionality. The ranges for the penalties are published so there is a measure of accountability and transparency although it would be more consistent, transparent and accountable if it defined the criteria that are considered when setting the size of penalty. Some targeting of risk is demonstrated by considering the frequency of previous offences.*	1	1	1	1		1	
I	Rail	CZ	The NSA does have power to issue bans without the right to appeal when there is a substantial risk to safety, as in the example of a rail vehicle with inadequate braking systems being prohibited from using a line with a steep decline. This was because of drivers flouting the rules: "There are written rules with regard to behaviour of the driver, and they say if the driver follows these rules, the accident wouldn't happen. But I think that it's too risky. At first we had no evidence that the technology guarantees safety. And the case that the braking system is out of order, in fact, and in effect it is too risky to rely on the behaviour of the driver." *Our opinion: The NSA demonstrates essential enforcement practice by ensuring that activities that are a real safety hazard are not permitted to continue.*	1					1	
I	Rail	DK	"We have these two roles, being safety management auditor or doing authority inspections. Actually, some years ago we had a very thorough discussion with our legal department on this. When we explained how we are using our competencies in the auditing scheme and using non-compliance, the legal department said, you cannot use that, that's not part of the law, you have to use a ban or prohibition.	2	2	2			2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			We said, no, definitely not, this is actually a way of guided communication using non-conformities. We make an agreement with the company when to solve this non-compliance, so we are actually in a dialogue with the company. If we use the other legal frame, there's no dialogue, we just say what to do. In 95% or 98% or more of the cases we are using the dialogue option and using non-compliance and only using the legal framework for enforcement if safety is endangered. When safety is endangered—that's a very clear line. If we feel that safety is endangered, we will take the other role, of the safety authority." *Our opinion: It is good practice to engage with RUs/IMs and guide them to improve. This NSA has chosen to follow this approach (rather than issuing legal penalties for every non-compliance) even though its legal basis has been disputed within the Member State. This contrasts with other NSA (e.g. Netherlands, Bulgaria) that have been encouraged to follow a stricter, enforcement-based approach.*							
I	Rail	F	The French NSA described how it balances influencing the behaviour of RUs/IMs and enforcing it: "First of all, we're not allowed to give advice… at the end of an audit we have a meeting where we… meet with the entities and say, "look, this is what we've found" and then we formally issue the nonconformity forms if there are any to be issued. And it is at that meeting where discussion takes place, because we make sure that they've understood [in] what way they've got a nonconformity. In our procedure it is for them to identify the cause of how it came about and to propose corrective action. But quite often people from an operational point of view, they won't actually understand straight away where they should be going. So we don't give advice but when we see that people need it we orientate them the right way, and that is provided for in our procedure. That's from the influence point of view. [For enforcement]… we give these nonconformity forms to them. We define the cause [N.B. that is to say the reason why EPSF has identified the nonconformity. The actual cause of the nonconformity has to be identified by the RU/IM] and we give the reference to the text which has been transgressed… and this may be a national rule, it could be a law or some regulation they had or it could be the entity's own safety management system document, which says they are going to do something and we find on the ground that it's not done or it's not efficient. So having notified and graded ourselves at the harmonisation committee the severity of the nonconformity, we then ask them to... if we want immediate measures taken straight away for certain things to correct the problems …we tell them we would like their proposals for remedial methods, which we then	2	2	2			2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			give an opinion on. And it is agreed between us and them as to when these measures are put in place. Further down the line, in the treatment of the nonconformity, we make sure that they're taking on-board the specific problem we've found… But we will expect it [corrective action] by a date and they will have to agree the date so that we're not seen as pushing a date at them which they just can't possibly manage. The immediate remedial action, there's never a problem with the date. But it's down the line when they have to look through the whole organisation that sometimes they're a bit optimistic and we always insist that they identify dates which they can meet. Having said that, in order of severity as far as taking action, or enforcement as you call it, first of all, the French NSA doesn't have legal powers to instigate legal proceedings. It doesn't work like that in France. What we have is the power, ultimately, to suspend their operations. So in order, we give them the nonconformity forms. If they fail to meet the date we contact them and say, "you're late on this, what's happening?" And if they give us a reasonable explanation and something's being done we may accept an extension to the date. If on the other hand, they're just not meeting the date and nothing seems to be happening, we will send them a letter, a warning letter, saying that if they don't get the corrective action represented to us and in place within 90 days. If we saw something more urgent we could do that. And the warning letter, in fact, reminds them that we can suspend or restrict their operations. In other words, the authorisation which is granted by EPSF could have its terms modified or suspended. And if they still don't do what is asked of them, despite this letter… we will actually take action and suspend or restrict their operations. It concentrates their mind possibly more than having to pay a fine in court." The NSA reported that it was satisfied that this enforcement approach offered sufficient escalation in severity and was both 'easy to understand' and effective. *Our opinion: The French NSA demonstrates good practice by engaging in guided dialogue with any RU or IM that breaches the safety regulatory framework. This dialogue is structured in a way that will guide the RU/IM towards understanding the nature of the breach and where it should explore taking remedial action. If the NSA's action has to escalate to enforcement this is essentially issuing a formal nonconformity, which references the breach and requires the RU/IM to make a proposal to rectify the fault by a certain date. This would appear similar to the 'improvement*							

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			notices' issued by other NSA. The NSA then can exercise its right to inspect the remedial action and, if it is not delivered on time or to the necessary standard, the NSA can threaten to escalate the nonconformity to a suspension or revocation of the RU/IM's certificate/authorisation. There is a potential concern that an important RU/IM (perhaps one with national coverage) could fail to comply and revocation of its certificate/authorisation would generate substantial disruption to the network. However, the NSA reported that RUs/IMs of this size were quick to deal with nonconformities and would do so quickly. This would suggest that the good dialogue that appears to exist between the NSA and most of the market is an effective behavioural influence.							

Table B.36: Enforcement responses to case studies 1 and 7

NSA	Example 1	Comments	Example 7	Comments
Great Britain	Issue written guidance	-	Issue written guidance	-
Sweden	Take another type of formal enforcement action	Issue a formal submit and ask for action plan for information of staff	Our NSA do not deal with this kind of problems – it's another authority responsible (workers' safety).	
Estonia	Issue written guidance	NSA will make its conclusions known to operator	Issue written guidance	-
Lithuania	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-	Issue written guidance	-
Romania	Issue a fixed fine	-	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-
Germany	Issue written guidance	-	Issue written guidance	-
Denmark	Issue written guidance	We will ask the company to explain how they ensure that this does not happen again and if possible, how the safety management system should be corrected.	Problems concerning working environments are not an issue for the Danish NSA. This type of problem is handled by the Danish working Environmental authority. (If a NSA inspector discovers such an event, he will naturally turn to the proper authority).	
Spain	Issue written guidance	-	It does not apply. This is not competence of the NSA.	
Latvia	According to Cabinet rules NSA doesn't investigate such incident. It should be investigated by RU's internal investigation committee.		Issue a formal enforcement notice (e.g. a formal legal requirement	Prescribe to amend the procedures how to do

NSA	Example 1	Comments	Example 7	Comments
			to address a non-compliance)	constructional work to ensure safe working
Poland	Issue verbal guidance	It could be possible that no action would be taken provided that all procedures worked well. Sometimes it can also be a written guidance.	It's more the responsibility of the Building Control Authority or Labour Inspection, not the NSA. The NSA will probably only verify, if an IM has all relevant rules and procedures on supervision over subcontractors in place. NSA would also inform of the situation the relevant institutions.	
Bulgaria	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	After investigating the case the NSA of Bulgaria would issue a written obligatory prescription, in which we would inform the RU about the non-compliance and would impose fixed deadlines and ways of correction of the problem. In this case, the NSA of Bulgaria is entitled to impose the following penalty: Railway Transport Act Art. 128. (3) Any person infringing or not observing a provision of the ordinances or the other normative acts based on this Law shall be imposed a fine or a proprietary sanction in amount from 100 to 1000 BGN.	The NSA of Bulgaria would inform the competent authorities responsible under the Health and Safety at Work Act.	

NSA	Example 1	Comments	Example 7	Comments
		In case that the formal obligatory prescription of the NSA is not complied with in the prescribed way within the prescribed deadlines we would impose the following financial penalties. Railway Transport Act: A fine from 1000 to 10000 levs or a proprietary sanction from 5000 to 30000 levs shall be imposed to a person failing to fulfil an obligatory prescription issued by the employees referred to in Art. 117, par. 2 or a direction issued by the Executive director of the 'Railway Administration' Executive Agency within his/her powers.		
Austria	Issue written guidance	NSA initially reluctant to select just one response	Take another type of formal enforcement action	Inform State Labour Inspectorate about the incident
Portugal	Issue written guidance	-	Issue written guidance	-
Czech Republic	1. NSA probably would not get this information. 2. NSA would not take any measures.		1. NSA probably would not get this information. 2. NSA has no responsibility in this way.	
Netherlands	Take another type of formal enforcement action	We will ask for a written action plan of what they will do to give us	Other	Ask to improve the SMS of the IM with this subject.

NSA	Example 1	Comments	Example 7	Comments
		the proof that everything is done to avoid an accident next time.		
Channel Tunnel	Issue written guidance		Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	
Hungary	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)		Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	
Norway	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity.
Ireland	Take another type of formal enforcement action	Railway Safety Act 2005 section 76. Request an improvement plan and monitor implementation.	Other	Safety at work is Health and Safety Authority matter. Notify HSA in accordance with MOU
France	-	-	N/A	This topic is outside the remit of the NSA, according to Directive 2004/49/EC.
Finland	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)		Other	This is an occupational health and safety issue, which belongs to another government agency.
Italy	Issue written guidance		Other	The "safety at work" is not included in the safety tasks

NSA	Example 1	Comments	Example 7	Comments
				assigned to the Italian NSA, consequently, in such a case, a warning should be sent to the competent authority.

Table B.37: Enforcement responses to case studies 3 and 6

NSA	Example 3	Comments	Example 6	Comments
Great Britain	Issue verbal guidance	-	Issue verbal guidance	-
Sweden	Our NSA does not deal with this kind of problem – it's another authority responsible (workers' safety)		Our NSA does not deal with this kind of problem – it's another authority responsible	
Estonia	Issue verbal guidance	-	Issue written guidance	NSA (or IM) will also inform the Local Government and/or Municipality Police that kind of a problem
Lithuania	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-	Issue a fixed fine	-
Romania	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-
Germany	Other	In this case it is a labour-protection law case. Station buildings are not the responsibility of the NSA, the relevant local authority is responsible. In this case, the NSA would inform the competent national authority in writing.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	The IM would be expected to fix the fault and update its maintenance plan accordingly.

NSA	Example 3	Comments	Example 6	Comments
Denmark	Problems concerning working environments are not an issue for the Danish NSA. This type of problem is handled by the Danish working Environmental authority. (If a NSA inspector discovers such an event, he will naturally turn to the proper authority).		Issue verbal guidance	The Danish NSA would advise the IM to make a daily check at the fence until the upgrade was established.
Spain	It does not apply. This is not competence of the NSA.		Issue written guidance	-
Latvia	Take another type of formal enforcement action	Prescribe to amend the procedures how to do constructional work to ensure safe working on roof.	Issue written guidance	-
Poland	This area is considered as problematic in Poland. Supervision over buildings and installations other than necessary to provide railway traffic is in the scope of Building Control Authority (GUNB) in Poland, not the NSA. Additionally, the work safety is the field supervised by Labour Inspection (PIP). In case of noticing such a situation, NSA would inform of the matter these two institutions (GUNB and PIP).	From the NSA point of view, the division of tasks between two authorities in Poland can be considered as a significant problem not only in the field of supervision but also in the field of TSI application. The Building Control Authority acts on the basis of different law than the NSA. It makes it difficult for the Building Control Authority to refer to separate TSIs, that are not linked with building law in Poland, although this authority is responsible for technical approval of some railway constructions as platforms, station buildings, bridges etc.	It is the Building Control Authority's responsibility rather than the NSA in Poland.	If the NSA takes any action, it would probably be the verbal or written guidance.

NSA	Example 3	Comments	Example 6	Comments
Bulgaria	The NSA of Bulgaria would inform the competent authorities responsible under the Health and Safety at Work Act.		Other	The NSA would make a subsequent (follow-up) inspection to check if the IM has complied with the obligation to repair the fence.
Austria	Take another type of formal enforcement action	Inform the State Labour Inspectorate of the incident.	Issue written guidance	-
Portugal	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-	Issue written guidance	-
Czech Republic	1. NSA probably would not get this information. 2. NSA has no responsibility in this way.		1. NSA probably would not get this information. No national rules require to build this fence. 2. NSA would not take any measures.	
Netherlands	Nothing; it is outside our scope or supervision.		Other	Compliment them with a mature safety management system. Please continue.
Channel Tunnel	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)		Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	
Hungary	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)		Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	

NSA	Example 3	Comments	Example 6	Comments
Norway	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity.
Ireland	Other	Matter for the Health and Safety Authority who are enforcing agency for this. Report to them via Memorandum of understanding (MOU) agreement	Issue written guidance	
France	N/A	This topic is outside the remit of the NSA, according to Directive 2004/49/EC.	-	-
Finland	Other	NSA does not deal with occupational health and safety issues (there is another government agency for that).	Other	No formal action because fences are not compulsory.
Italy	Other	The "safety at work" is not included in the safety tasks assigned to the Italian NSA, consequently, in such a case, a warning should be sent to the competent authority.	Issue written guidance	-

Table B.38: Enforcement responses to case studies 5 and 2

NSA	Example 5	Comments	Example 2	Comments
Great Britain	Prosecute in court	-	Prosecute in court	-
Sweden	Our NSA do not deal with this kind of problems – it's another authority responsible		Take another type of formal enforcement action	Issue a formal submit and ask for action plan for maintenance and check carriages before departure – daily checks. How is information between staff and [those] responsible for maintenance
Estonia	Issue written guidance	-	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-
Lithuania	Issue a fixed fine	-	Issue a fixed fine	-
Romania	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-	Issue a fixed fine	-
Germany	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Security of the railway (fencing) is not the jurisdiction of the NSA. The operator's maintenance plan is not effective and so the action would be to repair the fence and update the SMS to prevent reoccurrence.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Further action may be taken depending on the outcome of the initial notice.
Denmark	Issue a formal enforcement notice (e.g. a formal legal	Danish Transport Authority will issue a formal enforcement notice,	Issue a formal enforcement notice (e.g. a formal legal requirement	We would give an immediate ban on the use of this type of material

NSA	Example 5	Comments	Example 2	Comments
	requirement to address a non-compliance)	and give a non-conformity deviation with requirement for action plan to ensure that similar events are not repeated. Danish Transport Authority will follow up on the subject by supervision.	to address a non-compliance)	and an order to bring the equipment in order. We would also ask the company to explain how they will ensure that the safety management system will continue to ensure that this does not happen again. If the company fails to meet the set deadlines, we will report it to police and revoke the safety certificate.
Spain	Take another type of formal enforcement action	If it is a private IM: Issue a formal enforcement notice. If it is a public IM: Carry out the enforcement action by means of a contract.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Improvement of maintenance plans.
Latvia	Issue other financial penalties	-	Financial penalty and SMS reassessment	-
Poland	Again, this area is considered as problematic in Poland. The responsibility for supervision is the responsibility of General Building Inspectorate (GUNB) rather than the NSA.	The NSA can take into consideration this problem during assessing the general risk profile of the infrastructure manager. The problem is not linked directly with the safety of railway traffic or maintenance of vehicles or infrastructure. That's why it's not the main area of the NSA interest.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Probably this issue will be examined by the NIB first and then submitted to NSA for enforcement. In case of non-compliance after issuing a NSA decision, further steps are possible (penalties, prosecution in court).

NSA	Example 5	Comments	Example 2	Comments
		If the NSA takes the action in this field it will probably be the written guidance, rather than formal decision or penalty.		
Bulgaria	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	In this case the NSA of Bulgaria, which is Railway Administration Executive Agency, would apply Art. 136 (1) of the Railway Transport Act: Art. 136. (new – SG 22/09) (1) Proprietary sanction from 5000 to 50 000 Levs shall be imposed to a railway carrier or a chief executive of the infrastructure who has failed to fulfil any obligation of his/hers ... (3) The penalty of par. 1 shall be imposed after an inspection, carried out by the 'Railway Administration' Executive Agency at its initiative or upon a submitted plea of unfaithful treatment, discrimination or affect in any other way of a carrier.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	After investigating the case the NSA of Bulgaria would issue a written obligatory prescription, in which we would inform the RU about the non-compliance and would impose fixed deadlines and ways of correction of the problem. In this case, the NSA of Bulgaria is entitled to impose the following penalty: Railway Transport Act Art. 128. (3) Any person infringing or not observing a provision of the ordinances or the other normative acts based on this Law shall be imposed a fine or a proprietary sanction in amount from 100 to 1000 BGN. In case that the formal obligatory prescription of the NSA is not complied with in the prescribed

NSA	Example 5	Comments	Example 2	Comments
				way within the prescribed deadlines we would impose the following financial penalties: Railway Transport Act : A fine from 1000 to 10000 levs or a proprietary sanction from 5000 to 30000 levs shall be imposed to a person failing to fulfil an obligatory prescription issued by the employees referred to in Art. 117, par. 2 or a direction issued by the Executive director of the 'Railway Administration' Executive Agency within his/her powers.
Austria	Issue a fixed fine	In addition, there will be an obligation to repair the fence until it can be fixed permanently.	Issue a fixed fine	-
Portugal	Issue a fixed fine	-	Issue a fixed fine	-
Czech Republic	1. NSA probably would not get this information. No national rules require a fence to be built. 2. NSA would not take any measures.		Issue other financial penalties	1. NSA probably would not get this information. 2. NSA would issue penalty - vehicle operated in a bad condition.
Netherlands	Issue a formal enforcement notice (e.g. a formal legal	Ask for an explanation and ask for a plan how the IM wants to deal	Issue a formal enforcement notice (e.g. a formal legal requirement	

NSA	Example 5	Comments	Example 2	Comments
	requirement to address a non-compliance)	with such issues in the future. Maybe including a penalty for the first part.	to address a non-compliance)	
Channel Tunnel	Prosecute in court		Prosecute in court	
Hungary	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)		Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	If necessary revoke safety certificate
Norway	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity. Could be reported to the police. this kind of incident will be followed up by the NIB.
Ireland	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Improvement notice	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	
France	N/A	This topic is outside the remit of the NSA, according to Directive 2004/49/EC.	-	-
Finland	Other	Ask for written clarification concerning the actions the IM has taken to fix the issue.	Other	Asks for a written clarification. NSA may also investigate if NIB doesn't.

NSA	Example 5	Comments	Example 2	Comments
Italy	Issue a fixed fine	-	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-

Table B.39: Enforcement responses to case studies 4 and 8

NSA	Example 4	Comments	Example 8	Comments
Great Britain	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-
Sweden	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Prohibit traffic with the special vehicle until the RU/IM can provide the vehicle is safe again	Our NSA does not deal with this kind of problems – it's another authority responsible (workers' safety)	
Estonia	Issue other financial penalties	We would have removed such RRV's from traffic, since their repair.	Issue a fixed fine	-
Lithuania	Issue a fixed fine	-	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-
Romania	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-	Other	The exceeding of the maximum allowed service time on the locomotive is considered as incident and leads to the withdrawal of the safety certificate Part B
Germany	Take another type of formal enforcement action	Issue a written notice that would question the procedure and be followed by further action/notices to remedy the fault. Assessment costs may apply.	Other	NSA not responsible under current legislation. When detected, information is provided to the competent authority under state law (usually labour inspectorates), which carry out

NSA	Example 4	Comments	Example 8	Comments
				further investigation. If repeated violations occur, this may be a starting point for due diligence/ verification of the SMS.
Denmark	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	We would give the company a prohibition against using such equipment as well as an injunction to put things right and a non-conformity deviation because the SMS had not handled this sufficiently.	This is a shared responsibility between different authorities. For safety authority's point of view we would look at whether the company has adequate resources and how they manage and monitor these. If there aren't sufficient resources we would give the company an order to bring this in order. (If an NSA inspector discovers such an event, he will naturally turn to the proper authority).	
Spain	Other	It depends on the situation: 1) If RRVs operate in tracks under construction, it doesn't apply. 2) If RRVs operate in the national network, their 'authorisation' is removed.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Modification of 'working hours' procedure.
Latvia	Take another type of formal enforcement action	Stop the utilisation of the vehicle until problems are solved	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	-
Poland	This area is considered as problematic in Poland. The responsibility for supervision is shared between various institutions (NSA, Road Transport Inspection, the Police) and depends on the situation where	If the NSA will take any action, it can be written guidance, a formal decision or a financial penalty, depending on the situation.	Working hours are the responsibility of Labour Inspection. The NSA has the agreement with Labour Inspection on that issue. The NSA activities are more oriented on systemic solution (if RU has appropriate procedures to control working time) and Labour Inspection is more oriented on inspections in this field. Our very first experience in this field shows that it is a problem to identify the situations where the working hours are exceeded, especially because many train drivers	

NSA	Example 4	Comments	Example 8	Comments
	the problem will be identified (on rail or road infrastructure).		work usually for more than one undertaking.	
Bulgaria	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	After investigating the case the NSA of Bulgaria would issue a written obligatory prescription, in which we would inform the operator of the RRV about the non-compliance of the vehicles with the technical instructions for maintenance and operation of the vehicle and would impose fixed deadlines and ways of correction of the problem. In this case the NSA of Bulgaria is entitled to impose the following penalty: Railway Transport Act Art. 128. (3) Any person infringing or not observing a provision of the ordinances or the other normative acts based on this Law shall be imposed a fine or a proprietary sanction in amount from 100 to 1000 BGN. In case that the formal obligatory prescription of the NSA is not	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	The NSA would apply the following provisions of the RTA: Art. 136. (new – SG 22/09) (1) Proprietary sanction from 5000 to 50 000 Levs shall be imposed to a railway carrier or a chief executive of the infrastructure who has failed to fulfil any obligation of his/hers or who has in any other way treated unfaithfully, discriminated or affected another carrier. The NSA would prepare a written formal prescription with specified deadlines for solution of the problem.

NSA	Example 4	Comments	Example 8	Comments
		complied with in the prescribed way we would impose the following financial penalties. Railway Transport Act: A fine from 1000 to 10000 levs or a proprietary sanction from 5000 to 30000 levs shall be imposed to a person failing to fulfil an obligatory prescription issued by the employees referred to in Art. 117, par. 2 or a direction issued by the Executive director of the 'Railway Administration' Executive Agency within his/her powers.		
Austria	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	We would also issue a fixed fine and forbid the use of the vehicles until the violations had been eliminated.	Take another type of formal enforcement action	Inform the State Labour Inspectorate of the incident.
Portugal	Take another type of formal enforcement action	Stop immediately the vehicles and issue a formal enforcement notice	Issue a fixed fine	-
Czech Republic	1. NSA probably would not get this information. 2. It is very difficult to issue penalty or withdraw a certificate in legal way.		1. NSA probably would not get this information. 2. NSA has no responsibility in this way.	
Netherlands	Issue a formal enforcement notice (e.g. a formal legal requirement	We will forbid to use them until they are safe enough; to be	Other	Punish the RU the maximum and maybe stop them from operating

NSA	Example 4	Comments	Example 8	Comments
	to address a non-compliance)	decided by us.		until they can make a statement 'in controle' about this issue to the NSA.
Channel Tunnel	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)		Prosecute in court	
Hungary	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)		Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	
Norway	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity.	Issue a formal enforcement notice (e.g. a formal legal requirement to address a non-compliance)	Information can be used at the next planned supervision activity.
Ireland	Other	Notify the Health and Safety Authority - Body charged with overseeing work vehicle issues.	Other	Notify Health and Safety Authority - occupational health issue. Improvement Plan. Contravention of SMS.
France	-	-	N/A	This topic is outside the remit of the NSA, according to Directive 2004/49/EC.
Finland	Other	NSA asks for a written clarification and may issue a written guidance.	Other	This is OSH issue, which belongs to another government agency.
Italy	Issue a fixed fine	-	Issue a fixed fine	-

Table B.40: Summarising the safety performance of RUs/IMs

NSA	As a safety REPORT for each RU/IM	As a safety RATING for each RU/IM	Other, please specify:
Great Britain	Yes	No	For the key RUs/IMs there would be an annual assessment report, but not for the smaller undertaking.
Sweden	No	Yes	First rating when assess and award permits for RU /IM. Revise rating of some IM after supervision.
Estonia	No	Yes	No
Lithuania	Yes	No	No
Romania	Yes	No	No
Germany	No	No	File / Documentation per RU / IM.
Denmark	Yes	No	No
Spain	No	No	It will be summarised in an outcome report.
Latvia	Yes	No	No
Poland	No	No	Still bear in mind that all supervisory activities are based on the national requirements. The 'Regulation on the controls performed by the President of UTK' specifies the way of documenting the control process. Regular controls (including the SMS controls) finish with reports containing information on observed problems and recommendations, which have to be fulfilled in a specified time. In case NSA encounters serious safety breaches it is possible to retain a vehicle from operation or close a section of a railway line. Every year NSA prepares a safety report in line with ERA template and another specific report for the minister responsible for transport, based on data collected from companies. The first report is available to all interested parties. Data are presented on the basis of problems, not companies.

NSA	As a safety REPORT for each RU/IM	As a safety RATING for each RU/IM	Other, please specify:
Bulgaria	Yes	No	No
Austria	Yes	No	No
Portugal	No	No	No
Czech Republic	Yes	No	No
Netherlands	Yes	Yes	Yes - A mix of both rating and report.
Channel Tunnel	Yes	No	
Hungary	No	No	As a decision for each RU/IM.
Norway	No	No	Not very systematically.
Ireland	Yes	No	No
France	-	-	By tracking incidents, SAI and IPS.
Finland	Yes	No	
Italy	-	-	The safety performance indicators for each RU/IM are underway. The indicators concerning the accidents are already available.

Table B.41: Summarising the safety performance of the Member State

NSA	As a safety REPORT for the Member State	As a safety RATING for the Member State	Other, please specify:
Great Britain	Yes	No	No
Sweden	Yes	No	No
Estonia	Yes	No	No
Lithuania	Yes	No	No
Romania	Yes	No	No
Germany	Yes	No	No
Denmark	Yes	No	No
Spain	Yes	No	No
Latvia	Yes	No	No
Poland	Yes	No	See earlier answers. Two reports are worked out each year by UTK. Both are based on problems and performance of the market in general, not separate RUs / IMs.
Bulgaria	Yes	No	No
Austria	Yes	No	No
Portugal	Yes	No	No
Czech Republic	Yes	No	No
Netherlands	No	Yes	No

NSA	As a safety REPORT for the Member State	As a safety RATING for the Member State	Other, please specify:
Channel Tunnel			NA - NSA / IGC annual report based channel tunnel infrastructure – not for the member state.
Hungary	Yes	No	No
Norway	No	No	No
Ireland	Yes	No	No
France	Yes	No	We considered that the answer to that question could affect the annual safety report (produced by the EPSF).
Finland	Yes	No	
Italy	Yes	No	

Table B.42: Dissemination of performance monitoring

NSA	Made publicly available?	Shared with stakeholders?	Shared directly with any other parties?	If shared directly with any other parties, please specify:
Great Britain	Yes	Yes	Yes	
Sweden	Yes	Yes	No	
Estonia	Yes	Yes	No	
Lithuania	Yes	Yes		
Romania	Yes	Yes	No	
Germany	Yes	Yes	No	
Denmark	-	-	-	-
Spain	Yes	No	Yes	ERA
Latvia	Yes	Yes	No	
Poland	Yes	Yes	No	The information in the reports mentioned above is directly shared with the minister responsible for transport. The safety report prepared on the basis of ERA template is published in the Official Journal of the Minister responsible for transport.
Bulgaria	Yes	Yes	No	
Austria	Yes			
Portugal	Yes	Yes	Yes	Ministry of Transport, NIB, RUs, IM
Czech Republic	Yes	No	No	

NSA	Made publicly available?	Shared with stakeholders?	Shared directly with any other parties?	If shared directly with any other parties, please specify:
Netherlands	Yes	Yes	Yes	
Channel Tunnel	Yes	Yes	Yes	
Hungary	Yes	Yes	No	
Norway	No	Yes	Yes	To some extent, on request
Ireland	Yes	Yes	No	
France	Yes	Yes	Yes	We considered that the answer to that question could affect the annual safety report (produced by the EPSF).
Finland	Yes	No	No	
Italy	Yes	Yes	No	

Table B.43: NSA perspectives on the effectiveness of the regulatory framework

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	NL	"I think working with the Safety Management System makes the culture in a company different, and us visiting the companies from top to down to the floor makes a big safety awareness. We like to promote the fact that everyone—anyone—in the company has a responsibility towards safety, so not only the directors, but also the people on the working floor. So working with Safety Management Systems gives us a reason to work with these companies, and to promote this message. We think that there's a lot of safety awareness in these companies, because they're working with Safety Management Systems and because of our supervision on them." *Our opinion: This is a positive outcome for the SMS-based approach. The NSA's focus on promoting the SMS-based approach through supervision may be a factor in the reported awareness of safety that is apparently evident throughout the market that the NSA supervises.*			2			2	
I	Rail	NL	"I think they [RUs] are very aware of their responsibility to act in a safe way, and to think about what is a safe way. So the question for me of whether the companies are aware of the Safety Regulatory Framework is actually two questions: Are they aware of their role in safety… of what they can do in their responsibility, yes, they are very [aware]; And if you ask are they aware of the regulatory framework—the rules, the acts, the laws, the demands—no: they are not that much [aware]. But I think this is not important for the safety, because rules sometimes are not good for decisions. Sometimes you have people and companies that perhaps don't think for themselves. Because each situation is different and we want them to be good enough to understand their responsibility and their job—they [should] decide for themselves what's best for safety. And rules sometimes imply that you don't have to think for yourself—just follow the rules. So… I think they're [RUs] very good in acting safe, but they're not good in acting as the rules want them to do." *Our opinion: This insight into market awareness of the safety regulatory framework is indicative of this NSA's approach to supervision and enforcement. It has a clear focus on safety outcomes and is aware that responsibility for safety is ultimately to be handled by RUs and IMs (and not the NSA).*			2			3	
I	Rail	S	The NSA believes the safety regulatory framework is only quite effective. Experience from audits suggest RUs/IMs do not fully understand the concept of an SMS: "Often that we can come out on the audit and see that they have not changed the document since their application. That's not a living system; you can only see on the dates of the documents, 'oh my God they have done nothing'."			1			1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			Given that the network conditions and the RUs/IMs themselves are constantly evolving, the NSA believes that the safety regulatory framework should be updated with greater speed and frequency to reflect any changes. The NSA believes that it can play a part in this: "In their documentation they have old legislation, they have old regulation, they have not been aware about the changes and they have a responsibility to go and search information and go to our website and see. Perhaps we can do something to help them be better; share information better. Especially the small companies; the big companies who have big safety departments it's not a problem but smaller companies it's difficult. We see, very often, at least I think almost every audit no compliance with the legislation and regulations in their documentation because of the changes and they have not taken care of it." *Our opinion: This NSA reports that document reviews do not provide a complete picture of compliance and sometimes, especially with smaller RUs/IMs, the SMS may not be implemented or developed effectively in practice. The NSA acknowledges that it could do more to demonstrate good practice and assist the market with understanding its obligations.*							
I	Rail	D	The NSA believes the safety regulatory framework is 'quite effective' for the following reasons: "That's… a qualitative judgement. It's [the regulations] been on the table since 1994, since the German railway reform. It has improved since then. We have, let's say, a very active and growing railway market with many participants, a high share of, let's say, private railway undertakings, not the formal state railway, and the safety level did not decrease over the years despite the market evolving and changing and new market players appearing and so on. So, that's why we think it's quite effective. To say it's very effective, I don't know. Maybe something was missing but at least it's quite effective, we think. There are some improvements which are to come, for example, verification of charge of maintenance which might close a gap that we have today. So, there is still room for improvement. Maybe that was the reason to say quite effective." *Our opinion: The NSA is aware that the European framework is still developing and it sees that these developments will act to address concerns about the marketplace and its operations. That the NSA also sees the market requesting workshops and guidance supports its view that it is not fully aware of the framework currently.*			1			1	

Table B.44: Approaches to evaluation

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
D	OSH	DK	Changes to use of consultancy notices – these had been issued alongside repeated notices. The dutyholder would then have to consult with a WEA representative about the matter. This was not found to be working, especially as the dutyholder would often rectify the breach in advance of the consultancy, mean that the process was not used effectively. Consultancy notices are no to be issued only when: • the Danish Working Environment Authority identifies complex working environment problems that are difficult to solve. • the Danish Working Environment Authority identifies serious working environment problems that are difficult to solve. • the Danish Working Environment Authority assesses that an enterprise may be experiencing problems relating to the psychosocial working environment which need to be examined. • the Danish Working Environment Authority has made five or more decisions concerning violation of regulations on the working environment - the so-called multi-improvement notices. In other words, consultancy notices are only issued when the Danish Working Environment Authority assesses that enterprises need to consult an authorised health and safety consultant. *Our opinion: It is good practice to continuously evaluate the supervision and enforcement processes that are used. NSA are advised to monitor their processes for effectiveness and, if a process is found not to add any substantial safety benefit, the NSA should be open to changing the process to better deploy resources. This example shows that the safety authority has opened consultation with partners to attempt to reduce bureaucracy associated with consultancy notices and ensure that the process is better at doing what it is supposed to do, which is getting advice to dutyholders who would stand to benefit from it.*							3
D	OSH	A	Survey of employers and their employees who had been subject to inspections/controls at least once by the Labour Inspectorate in the preceding 2 years. Survey asked about professional competence and fairness of the Inspectorate, as well as its cooperation and humanity. By surveying both employer and employee, the survey seeks to identify whether both parties share the same opinion of action taken by the Inspectorate. *Our opinion: This is akin to a customer satisfaction survey. It seems to be good practice to ask independently (and after the event) how the affected parties felt about the action and the conduct of the safety authority. If the Inspectorate acts upon feedback, it shows a willingness to satisfy several of the supervision principles. Surveying employers and employees is an effective way of identifying whether management is detached from its staff and whether positive or negative approaches are shared across*	2	2		3		2	2

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			all levels of the company. This can provide insight into the 'safety culture' of an organisation and the extent to which SMS is ingrained effectively across the workforce.							
D	Rail	GB	"Every six months we take a random sample out of the computer and look at 10% of the investigations that have happened within that six-month period, the key being, are we following the process. But critically for that review, is the outcome what we would have expected to see? And that starts a peer review of, you know, the experienced people, so I lead that panel, so between the three of us we would have 60 years of experience of health and safety regulation. Is it clear why they've reached that conclusion? Is it the right conclusion? Discuss. But that's all to be open and, say, but based on principles of enforcement policy… and some of the other processes we've got in the enforcement management model. Have those been followed? Have we got the right conclusion as far as we can tell – yes or no? So, you know, that's our mechanism for evaluating whether we're being proportionate and targeted and consistent, and if we find that we are not, it gets fed back into from the process or the training of staff… has it worked well – yes, or no, and if it hasn't, what have we got to do to make sure that it works correctly in future?" *Our opinion: As described, this random peer review process demonstrates good practice.*	3	3				3	
D	Rail	GB	"And then we also do annual reviews of the types of enforcement that have happened over the organisation during the year and how that compares with previous years in terms of the spread of notices being served and the type of issues, and the type of regulations they're using." *Our opinion: As described, these measures to improve consistency, proportionality, targeting and prioritising are good practice.*	1	1				1	1
D	Aviation	F	Safety Report 2009 outlines the National Safety Plan, which concerns regulation, operator supervision and safety promotion. This is coordinated by the Safety Management Coordination Office. There is some info on SMSs, for example in 2009 15 airfields undertook an SMS audit, and DSAC (the Security Directorate of Civil Aviation) provides training on implementing an SMS and carrying out airport safety impact assessments. *Our opinion: Safety Reports, if published, provide an opportunity to review activities over a period and*		1	1			1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			disseminate to the market.							
D	Aviation	L	Questionnaire asking for feedback on the website and its contents. *Our opinion: Surveys are good practice for collecting feedback.*			2			2	
D	OSH	GB	Monitoring performance: the authority monitors its own performance by checking: • Milestones within the delivery plan are on track and being delivered. • Ratio of relevant positive/negative messages within the media. • Percentage of prosecutions which result in a conviction and corresponding levels of fines and media coverage. • Number of enforcement notices issued. • Number of web hits for the online risk assessment toolkits. *Our opinion: Within this list are several good practice examples: having a business plan with defined, measurable and achievable objectives; monitoring the frequency and type of enforcement action taken; and monitoring the external response to supervision and enforcement activity, both in terms of the industry's response (e.g. accessing materials) and the response of the wider public (e.g. in the media).*			2	3			
D	Rail	GB	Measuring NSA performance: an improvement in performance has been reported based on "more notices being served, more prosecutions, greater involvement I think with cases being reported to EMM on a monthly basis… the quality of notices has gone up. You used to look at… nuts and bolts on the ground, you know. This gate hasn't been maintained. Oh, right, whereas now… they're far more into… that gate hasn't been maintained because the safety management system isn't working for these reasons, A, B and C, etc, all around safety management systems so, you know, the quality of those oversees has improves no end. The same for targeting… of prosecutions; they're far more focussed on why the failure happened so that if people looked in and went sorry, what are you prosecuting them for that, they can go actually it's really clear; this, this and this." *Our opinion: Performance is based on quality of investigations and a focus on SMS. It is good practice for NSA to develop a way of assessing their performance. This report cannot be prescriptive about the criteria that should be used but can offer examples such as those listed in this quote. The GB NSA supplements this approach with the RM3, which challenges each RU and IM to continuously improve.*			2	3		2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			The model explains to RUs/IMs what the NSA will look for when assessing what the SMS should deliver and it is then the role of the RU/IM to find a way to deliver. This model can provide a further measure of the NSA's performance. *CSIs should also be considered. One approach would be to consider the trend in CSIs alongside the maturity of the RUs/IMs. This could be a benchmark measure of evaluation.*							
I	Rail	NL	The NSA did a customer satisfaction survey of RUs. The outcome was that the NSA was reported to be very competent and there were no issues raised with the way it operates. *Our opinion: It is good practice for NSA to survey the industry that is being supervised to collect feedback on their performance.*			2	2		2	
I	Rail	DK	The Danish NSA defines in its strategy how it evaluates its own performance. It has long- and short-term outcome targets: • Long-term outcome target: the number of serious accidents must not rise. The NSA will measure this as a moving five-year average. Supervisory work by the NSA will take into account trends in the accident data and seek to intervene at an early stage to prevent the growth of accidents in a particular area. To achieve this, the outcome measures will include monitoring precursors to accidents and safety-related irregularities (these data are the NSA's incident database). "The supervisory work has more direct scope for influence with regard to these parameters." • Short-term outcome target: the undertakings shall be strengthened. "The long-term outcome target is not sufficiently closely related to the results of the [NSA's] actual supervisory activities to be the sole candidate for evaluating whether the supervision is satisfactory." In recognition of this issue, the NSA has will measure more frequently its efforts to "maintain, and ideally enhance, the ability of the undertakings to manage their own risks". Three indicators will be used to measure this target: 1. Regulatory compliance within the undertakings. This is the classic supervisory task. 2. Learning within the undertakings. The supervision will assess whether the undertakings' safety management systems ensure ongoing internal learning from errors, incidents, accidents, etc. Continual learning will directly improve the risk management of the undertakings. 3. Assessment of the Danish Transport Authority's own regulation. Effective and clear rules promote the undertakings' regulatory compliance and limit their risks.			3	3		3	3

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			The NSA acknowledged that the short-term targets are measured by "primarily qualitative" indicators and its objective for both long- and short-term outcomes is to develop more precise indicators. "We will have to make a way of measuring the learning curve in the companies and that is what we are working on this year actually." In addition, the NSA measures its own performance in the 'number of audit days'. This has replaced 'number of inspections', reflecting the shift in focus from checking regulatory compliance to supervising through audits. 'Audit days' is the time spent by the NSA working directly with undertakings; 'overhead time' is associated with any audit day in the form of planning, coordination, committing results to paper, subsequent dialogue with the undertaking, etc. The NSA's target is to increase the number of audit days as this is the primary mechanism that the NSA has available to influence short- and long-term outcomes. *Our opinion: the NSA has established clear outcome measures and has demonstrated the direct and indirect influence of its supervisory activity. This information is published in its strategy which is available on its website. The approach taken is consistent with good practice, particularly as the NSA has adjusted its evaluation process to reflect working with a new regime of SMS auditing, where RUs/IMs have direct responsibility for delivering safety. It has also set a range of targets that enable it to measure its own performance and the performance of the sector.*							
I	Rail	A	This NSA does review its enforcement decisions at least yearly. They look at the following items: • Has there been any change in the type of enforcement action taken? • Have experts been consulted before taking action (on technical issues)? • Was the action sufficient – is there scope to use "less means" or "stronger action"? It also plans to review its forthcoming strategy at least every 6 months so that it can adapt to changing priorities during the year. *Our opinion: It is good practice to review decisions and revise supervision strategies on a regular basis. However, the approaches described here do indicate a reactive approach to consistency and proportionality, where potential changes in enforcement decisions are observed over time and adjustments made if necessary. This contrasts with an approach that reviews enforcement decisions against a decision-making framework before they are issued to the RU/IM.*	1	1		1		1	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	BG	"We periodically analyse our activity. If the response, for the respective units of our National Safety Authority perform, how they prepare reports, and these reports are analysed thoroughly, and as a result, we can make measures. Our NSA can, on the basis of the results of this control activity, the further performance of the activity is planned. Monthly there is reports, and every three months there is summarised estimation of the activity of the NSA. And these inspections are made on the basis of approved plans, which are approved by the management. Under certain circumstances, these plans can be changed. We are making working meetings, which are regularly done every three months, and during these meetings, with the staff, the activity is analysed. These reviews involve discussions of the current problems concerning the whole activity, and the newly occurred problems are presented to the management, with the aim of eliminating the deficiencies, and on this basis an analysis of the activity is made." *Our opinion: The NSA has a review system that is fairly regular and appears to guide future supervision activity and refine the supervision methods used.*	1	1		1		1	1
I	Rail	S	The NSA has fortnightly meetings for its staff (from the RU department) to discuss outputs from the audit checklist: "So it's discuss, so we are having similar decision and the team came back from an audit, can have experience on that audit and maybe it was a programme here, 'how have you taken care of that?', and assessing the certification, and what should we do? Should we take this another step or is it all right, so we try to have this regular meeting like that." The NSA is considering a computerised checklist that will record such items electronically in the future to ease the review process. *Our opinion: Whenever a system is used to guide audits and supervisions, it is good practice to monitor the outputs from that system, share and discuss experiences and consider whether the system is being used consistently by all staff and whether the parameters that are set are still appropriate.*	2	2		2		2	

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
I	Rail	S	The NSA has assessed that its performance has improved as a result of more structured process monitoring, which is essentially the introduction of weekly meetings to discuss the guidelines used by staff and issues related to risk-based supervision plans. *Our opinion: By frequently monitoring its own performance, the NSA has been able to improve. It is good practice for such reviews to be a regular feature and for NSA to act upon the findings of such reviews.*		2		2			
I	Rail	S	The NSA is confident in its approach as it receives positive feedback on its enforcement activity from RUs: "Even if they have several pages of non-compliance with regulation they are very positive with our supervision and they think it's a way of learning themselves to being better. We have a very good communication between us, I think, and they appreciate even if we revoke their licence they are some way positive because they understand, 'of course, this was not good, this we should have another way. Yes, we see now that this was really bad and we can understand that you can guarantee the safety, we have to make another to take part of this and make it better' and so on." *Our opinion: The dialogue between the NSA and its RUs/IMs appears to be at a level which is sufficient to encourage a shared objective of delivering safety. In reviewing its own performance, the NSA considers feedback from the market.*			2	2			
I	Rail	PL	The NSA does not evaluate whether it is being proportionate or consistent in its enforcement. It explained why: "There's no such requirement for any periodic review in Polish law. For the time being, it's only European law which requires self-assessment on the part of the NSA, if they are proportionate and consistent in their decisions." *Our opinion: It is not good practice if NSA avoid reviewing their own performance. The European framework should be adopted in its entirety.*	-1	-1		-1			
I	Rail	GB	Stakeholder engagement: In 2009 the NSA commissioned a survey of industry stakeholders to explore their: • knowledge, understanding and perceptions of ORR; • reasons behind their attitudes: why they feel the way they do about ORR; key influences on their	2	2	3	2			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			perceptions; • appreciation of the context in which ORR operates: the degree to which they appreciate the challenges ORR faces; and • how this understanding influences perceptions of ORR as a whole; hopes and expectations for the future; what they want ORR to do differently or better; how they would like to see ORR evolve. A number of in-depth interviews were carried out with a range of influential figures in the rail industry. The findings are summarised online and indicated that, "Stakeholders' experience of ORR's people, communications and decisions suggests that it meets its functional obligations successfully but does not always go beyond these; or goes beyond them in unwanted ways." The response from the NSA was as follows: "We have restructured our organisation and now have a new directorate dedicated to external affairs, including stakeholder relations. As we develop our approach we aim to deal with our many stakeholders in a more proactive, strategic and planned way." *Our opinion: Stakeholder surveys of this type (interview-based) provide substantial detail and often work well alongside quantitative surveys of larger samples. The NSA discovered a number of problems with its stakeholder engagement, including perceived biases in favour of certain RUs/IMs and regions. Some of the criticisms raised by the survey are particularly relevant to supervision and enforcement, with comments suggesting that the NSA can be slow, inflexible, appear to make uninformed decisions and is often reactive rather than proactive. This latter point is perhaps supported by the NSA's own admission that about 50% of its activity is proactive (compared with up to 90% for other NSA). Another concern was that stakeholder engagement was sometimes seen to be a perfunctory process, with the NSA paying 'lip service' to the views of stakeholders but ultimately proceeding as originally intended. The NSA has demonstrated good practice by publishing the findings of the survey so that the market has feedback on the process and is aware of the changes that the NSA has set itself as targets to deliver. Survey rated NSA against many of the principles of supervision.*							
I	Rail	D	The German NSA does not have a defined process for evaluating if it is supervising and enforcing in accordance with the principles. However, it did refer to the formal appeals procedure: "We have a procedure… where anyone affected by a decision from EBA can complain against that. The first step is complaining at EBA. Then we have to review our decision. The second step is to refer that to the court. If the case still is not okay, in the view of the addressee of our decision, that's one way how we see if our decisions are maybe disproportionate. If most of our decisions are referred to the court and then the court says that was not okay, review your decision, then we know that our			2	2			

I/D	Sector	MS	Examples	Proportionality	Consistency	Transparency	Accountability	Cooperation	Targeting	Prioritisation
			measures are disproportionate. Then we have, with the addressees of our supervision, with the ones we supervise, we have in some areas yearly, in some other areas less frequent but some kind of review talks. So we meet them again after one year, say what we have supervised, what we have found, what we did to have an exchange on what happened in the last year. This is a way to get the feedback from the infrastructure managers and supervisors, how they feel about what we do." *Our opinion: Although the NSA does not have a formal evaluation process, it does respond to the frequency and content of appeals as a way of determining whether it is supervising in accordance with the principles it applies. It also initiates 'review talks' with RUs/IMs on an annual basis in most cases. These reviews enable it to engage with stakeholders and get feedback on its performance.*							
I	Rail	D	The NSA believes its performance has improved because it strives to continuously improve. The measurement of this improvement is 'qualitative' and does rely upon feedback from the formal appeals procedure. *Our opinion: It is a basic good practice requirement for NSA to have a culture of improvement.*				1			

Appendix C Recommendations

This Appendix presents all of the recommendations from the report, grouped according to six core NSA activities and attributes related to supervision. This study provides baseline recommendations for good practice (highlighted in orange) and progressively higher levels of good practice (indicated by yellow and then green highlights).

NSA structure and organisation

NSA staffing and structure

It is recommended that NSA should implement:

- Good internal communication between the activities of assessment and supervision, irrespective of how the NSA is structured.
- A process for providing independent or peer reviews of any decisions made during assessment and/or supervision activities.
- A consistent knowledge base when selecting staff for specific supervision tasks – e.g. when assigning a supervision or assessment task to staff, those staff might ideally include one person with good prior knowledge of the RU/IM in question, and one with little prior knowledge; if so, this approach should be applied consistently. This is especially pertinent for NSA that loosely define the structural division of staff for these activities.
- A single decision-making policy across all supervision teams within the NSA. This will help to avoid generating market confusion by allowing fundamentally different decision-making processes to emerge as a result of staffing divisions within the NSA.
- Cooperation with other government safety authorities to deliver consistent supervision and enforcement across all rail-related activities, including those that are not directly under the remit of the NSA (e.g. the construction of rail infrastructure when there is no mainline traffic).
- A process for consulting with the NSA budget holder to ensure that the NSA has a remit and resources to at least fulfil the tasks assigned to it by the Safety Directive.
- A system for staff to efficiently store and exchange information about each RU/IM to facilitate good communication between assessment and supervision (and across any other staffing divisions).
- A structured approach to supervision (e.g. guided by an NSA-wide strategy) so that targeted activity is not directed solely by findings from assessment/ reassessment.
- A structured decision-making process.
- An organogram to show the market how the NSA is structured Making the structure of an NSA public may help to explain any differences that the market may experience when dealing with different departments (although such differences should still be addressed internally).
- A single committee to oversee and harmonise NSA supervision and other activities. The committee could be represented by senior figures from each division of the NSA.

NSA strategy

A further route to delivering effective assessment and supervision is to ensure that each NSA has a general strategy to guide it. It is recommended that NSA strategies should:

- Be published online at the very least.
- Cover at least an annual period.
- Outline supervision and enforcement policy. This should include methods of engaging with the market and the decision-making policies, with the latter having inputs and decision points for the RUs/IMs as well as the NSA. The latter appears clearest when defined in a diagram.
- Outline a range of goals (both short- and long-term) with a strategy for measuring and achieving them. Strategies may target change over a period of several years.
- Organise strategic goals thematically to better engage the market.
- Consider a longer-term strategy (covering multiple years).
- Ensure the strategy is informed by top-down and bottom-up data inputs.
- Use multiple methods of dissemination (e.g. posters, presentations, videos) to target RUs/IMs widely, and at all staffing levels.
- Establish measurable service standards (e.g. related to how the NSA will respond during assessment and supervision activities) by which the NSA can verify that it is fulfilling its commitments to the market. NSA should be mindful that they are also there to serve the market by providing services such as assessments and the principle of transparency requires that NSA are clear about what the market can expect of them.
- Describe the principles that will be followed by the authority. It is desirable specify how the NSA has interpreted the regulated principles of supervision, and indicate how these will be delivered.
- Adopt 'action plans' to describe how strategic goals will be achieved. Such actions plans can be renewed several times in the lifetime of a (longer-term) strategy.
- Adopt an inclusive approach to strategy development and delivery that engages the marketplace (e.g. through conferences, national / regional events, online pledges).
- Create organisational structures to deliver the strategy (e.g. create working groups, formed from NSA and market members, tasked with delivering specific goals).

Regulatory frameworks

Conflicts between national and European legislation were reported to create market confusion. To avoid this, NSA are recommended to:

- Have a statutory function to update or propose national laws and standards.
- Have a legal structure to permit enforcement of all relevant EU legislation.
- Incorporate relevant EU legislation within the national legislative framework to avoid any doubt regarding what items should apply to the market.

Complaints procedures

It is recommended that complaints policies are:

- Documented on the NSA website.
- Routinely issued to RUs/IMs during regulatory contact and supervision activities.
- Supported by a clear internal process whereby complaints can be escalated up the line management chain within the NSA if they cannot be resolved initially.
- Facilitated by online forms and accessible contact information for the NSA.
- Geared towards resolving complaints early in the process by providing RUs/IMs an opportunity to feedback on any enforcement decisions before they are formalised.

Cooperation

NSA are also required to have cooperation agreements with each other. It is recommended that NSA:

- Assign and publicise a point of contact for cooperation purposes (e.g. a dedicated email, telephone number and/or member of staff). Provide details of this online or share directly with all NSA.
- Be open and proactive about information exchange (especially with regard to RUs that are operating across borders).
- Liaise with each other regarding the reassessment of safety certificates that are nearing the end of their validity and consider timing to minimise the impact on interdependent Part A and Part B certificates for RUs operating across borders.
- Organise collaborative meetings with other NSA that currently share cross-border traffic, or have markets that would like to expand across borders.
- Agree on how to supervise collaboratively in a way that overcomes language differences and enables NSA to collect the necessary evidence.
- Proactively offer basic information to each other regarding Part A assessments if it is pertinent to an RU's application for a Part B certificate in another Member State.
- Undertake joint supervision activities with other NSA.
- Cooperate with other domestic and European non-rail safety authorities that may influence parts of the rail industry to ensure a coordinated approach.
- Listen to market requirements — where are there demands for NSA to collaborate to improve cross-border trade? (E.g. maintenance covenants to cover cross-border standards for maintenance of rolling stock).
- Proactively offer supervision and investigative support to other NSA on matters of shared interest (e.g. incidents in another Member State that involve a domestic RU).

Competency for supervision and enforcement

It is recommended that NSA:

- Ensure staff are trained to a universal level in essential skills such as auditing techniques.

- Ensure new staff are competent to supervise at the required level before being permitted to work independently. It is recommended that new staff are shadowed by experienced staff and 'signed off' when they have demonstrated the required skills.
- Set competence management as a strategic goal.
- Provide targeted technical training in rail systems (knowledge should be sufficient to supervise but not to subsume the responsibility that RUs/IMs have for safety under the SMS-based approach).
- Source training efficiently by going in-house or, if appropriate, via the rail market.
- Monitor staff competence (e.g. with examinations, case study assessments).
- Consolidate training courses with other domestic government safety authorities.
- Introduce internal online competence management systems to facilitate ongoing staff development and review.

Planning supervision

It is recommended that NSA:

- Consult with the budget holder (typically the Ministry) to discuss what can be achieved with the allocated resources.
- Present a case for the resourcing it needs based upon the supervision activities that are planned. Without a plan for supervision, it would be difficult for either party to determine accurately the level of resource required.
- Plan supervision for specific RUs/IMs based on an assessment of RU/IM capability.
- Supplement supervision planning by reviewing relevant incident data.
- Do **not** plan supervision based solely on distributing NSA resources equally across RUs/IMs.
- Distribute planned supervision activities across the periodicity of the certificate/ authorisation to allow more regular supervisory contact with RUs/IMs.
- Implement a systematic, quantitative approach to assessing the capability of an RU/IM, and its risk relative to other RUs/IMs, and use this to plan supervision.
- Access models of incident precursors to plan supervision that will address the events and actions that are believed to lead to incidents.

Supervision practices

Supervision methods

It is recommended that NSA:

- Audit using core methods of document checks (including examining SMS outcomes), interviews with a range of staff at RUs/IMs and frontline inspections.
- Check the whole SMS for each RU/IM at least once in a five-year period of validity for a safety certificate/authorisation.
- Allocate at least 50% of inspections to proactive supervision.
- Check individual parts of the SMS (if not the whole SMS) for each RU/IM more than once during a five-year period of validity for a safety certificate/authorisation.
- Follow an adaptive approach to scheduling supervision. A broad range of intervals between whole and partial checks of the effectiveness of the SMS for each RU and IM could be adopted based on the activities and capabilities of RUs/IMs.
- Plan supervision so that 80% of inspections are proactive.

Delivering supervision

It is recommended that NSA:

- Adopt a structured approach to decision-making for enforcement that is common to all NSA. The approach should calculate the compliance gap and direct NSA toward a proportionate response.
- Be accountable for their decisions and demonstrate transparency by implementing and documenting an appropriate decision-making model. No specific model is recommended but it should enable each NSA to use a 'compliance gap' approach.
- Monitor delivery of audits to check they are in line with the planned programme.
- Develop and publish decision-making criteria.
- Develop over the longer term—and collectively with other NSA and ERA—a detailed European model for decision-making in enforcement.
- Request organograms or similar from each RU/IM Plan to help plan interviews with staff at all levels in an RU/IM when conducting an audit.
- Survey the market to understand how effective supervision is and how delivery could be improved.
- Consider if technology can facilitate supervision by, for example, enabling RUs/IMs to submit information and documents online.
- Consider if supervision methods can give RUs/IMs an opportunity to learn from the expertise of the NSA (e.g. by issuing guidance initially rather than enforcing). This is especially pertinent when managing the transition to an SMS-based approach.
- Implement an internal advice structure so that NSA staff can obtain senior guidance with ease.

- Include subcontractors in audits to estimate how effectively an RU/IM implements its SMS throughout its operations.
- Empower individual inspectors to make enforcement decisions.
- Manage resources in a way that matches staff expertise with the type of supervision activity. This should enable staff with a range of skills to be deployed so that no activities are neglected, whether they are high or low risk.
- Implement a whistle blowing policy to obtain honest feedback from the market.
- Consider multiple methods of sharing decision-making criteria and supervision strategies with the market.

Delivering enforcement

Website communication

To develop their website communication further, it is recommended that NSA:

- Publish all key documents and NSA processes, policies, and procedures online. Exceptions to this may include sensitive procedures or plans that may give RUs/IMs information that might enable them to influence supervision findings.
- Provide online links to direct RUs/IMs to relevant and useful external information sources.
- Make resources and tools available for download (e.g. audit checklists). Resources can be catalogued innovatively (e.g. alphabetically, thematically, by help topic) to assist users in finding what they need.
- Feature information and guidance on key industry issues on their website.
- Publish news and current information about the sector. Some RUs and IMs in the market may not be as well-connected as others and so a central source of news and information for the market can be valuable.
- Adopt innovative website structures to catalogue information (e.g. according to themes) in order to assist users when searching.
- Providing foreign language translations of all or part of the website and its contents to facilitate users from other countries. Language differences can be a barrier to cross-border cooperation so NSA may wish to prioritise translation for languages of neighbouring Member States or those with which they share the most rail trade.
- Publish enforcement decisions and actions.

Other communication

It is desirable for NSA to find additional ways of communicating with the market beyond using a website. It is recommended that NSA:

- Meet regularly with RUs/IMs outside of formal supervision activity (e.g. by hosting informal meetings for RUs/IMs to attend and openly discuss current issues).
- Assign specific staff to specific RUs/IMs as a primary liaison. Arrangements of this type add another layer to the supervision regime and provide an opportunity for the NSA to discuss with individual RUs/IMs issues that may have emerged from operational observations or during recent inspections. Frequently changing the point of contact that an RU/IM has with an NSA helps to avoid the potential for bias in the supervision process.
- Establish ways in which the authority can supervise and enforce with transparency. This can involve creating and even publishing a set of procedures that staff must follow (e.g. explaining decisions to RUs/IMs, providing written confirmation afterwards).
- Use a variety of media for internal and external communications, matched to the needs of the market and to the internal needs of the NSA.
- Issue monthly incident reports to the market. This practice ensures that all RUs and IMs are aware of the latest safety issues in the marketplace, irrespective of whether they were involved directly.
- Host and participate in conferences with stakeholders.
- Develop a strategy for communication. A communication strategy provides focus for the NSA; often it is not possible to reach all of the market, all of time so it becomes necessary to segment the market into target groups. The strategy should be reasonably long-term and should identify which stakeholders will be targeted, what the content of the communication will be (and/or the process for developing this content) and how/when the communications will be issued. A strategy should also address any uncertainty within an NSA regarding how it communicates.
- Collect feedback from the market (e.g. via survey) to identify the most effective methods of communication.
- Issue leaflets for when there is supervisory contact to remind RUs/IMs of their rights and obligations during the process. Even if information is provided elsewhere and at other times, during an inspection it is pertinent to have this information in an accessible format to remind or inform those who are affected by the supervision activity of their rights. It should be considered that those RU/IM employees specifically affected by supervision activities may not be familiar with the NSA's procedures.
- Update the industry on progress with the NSA strategy. This helps to maintain focus and momentum.
- Use posters and media campaigns to highlight important issues for the industry. Campaigns that target members of the public are more likely to fall under the remit of RUs/IMs or other government departments but campaigns that target RUs/IMs and their employees may be within the scope of an NSA.
- Offer targeted in-depth guidance to RUs/IMs on key topics.

Issuing guidance

NSA that issue guidance to the market should consider that:

- Guidance can be collated to form packages or 'kits' to assist with specific topics (e.g. a new application, an audit).
- Guidance can use case study examples. Real world examples of how individual RUs/IMs have met the requirements of the safety regulatory framework can be useful to share amongst other RUs/IMs.
- Guidance can comprise 'tools' for use by RUs/IMs, such as checklists and even online courses.
- Detailed audit guidance can include sharing the questions and requirements that will be used for SMS auditing and providing accompanying tools such as forms for creating hazard logs and carrying out gap analysis.
- Guidance can direct the market towards the pertinent points in the regulatory framework by issuing summaries.

Enforcement methods

It is recommended that NSA:

- Use a standardised report form for all cases that may lead to enforcement action. This can improve consistency of decision-making and provide a clear record for accountability purposes.
- Report all enforcement action to the executive board of the affected RU/IM to ensure that remedial action filters through all levels of the organisation and is not localised to the part of the organisation where the breach occurred.
- Issue an enforcement policy statement to the market to explain the purpose of enforcement and what principles and procedures the NSA will follow. Although these principles exist in the regulations, there is value in each NSA describing to the market how it will enforce in accordance with these principles.
- Specify applicable financial penalties and (at least internally) define the criteria for applying each financial penalty to ensure consistency.
- Ensure each of the enforcement measures available to the NSA are accessible so that the full range of powers/penalties can be applied as appropriate. Some NSA report a reluctance to use specific enforcement measures due to administrative complexity.
- Ensure that dialogue between the NSA and the affected RU/IM is a part of any enforcement activity to ensure that each party has an opportunity to explain its case and consider fully all of the evidence available.
- Combine enforcement measures to increase the available range and proportionality (e.g. prosecuting an RU/IM in conjunction with issuing an improvement notice).
- Apply a suitable level of discretion for some enforcement measures due to the wider impact they may have (e.g. prosecutions). The GB OSH authority described how they would use discretion when considering prosecution as it was reported to be an effective way to draw attention to the need for compliance and maintenance of legal standards.

- Consider bringing forward full SMS reassessment for an RU/IM that has committed serious regulatory breaches or non-compliances. This may be appropriate if the alternative of revoking the safety certificate or authorisation is too disruptive. It sends a serious message to the RU/IM and still ensures that the organisation makes fundamental changes.
- Review the existing range of enforcement measures. Establish a working group to do this if the current national regulatory framework does not provide a clear, consistent legal basis for enforcement under the European regime of operations. The working group would include the NSA and the Ministry that has authority for national regulations.
- Differentiate financial penalties according to RU/IM factors (e.g. size). If the factors on which differentiation is decided are valid, this may be a way of delivering proportionate enforcement, which would also be consistent if it was in accordance with a defined policy.
- Introduce an innovative system for indicating to the market and to the public the level of compliance each RU/IM has achieved with its SMS. It is important that the process and criteria used are transparent.

NSA self-evaluation and continuous improvement

It is recommended that NSA:

- Establish basic review procedures. Regular staff discussions, random peer reviews of cases, and structured annual case reviews are suggested as a minimum requirement. Reviews should be targeted, with measurable outcome criteria.
- Develop a culture of self-evaluation and improvement.
- Survey marketplace satisfaction with NSA supervision and enforcement. Survey staff at a range of levels within RUs/IMs and include RUs/IMs that have been subject to enforcement measures. It is important for NSA to understand market satisfaction, both in general and after supervision/enforcement has taken place. Surveys can inform the future policies and procedures of an NSA. Survey findings should be published along with a response to core issues from the NSA, with appropriate commitments to action.
- Link evaluation data to strategic goals to present a coherent development cycle.
- Respond to market feedback on procedures by changing them if they are overly burdensome and ineffective. NSA may win or lose market support according to how responsive they are to valid market concerns.
- Monitor how NSA activity is presented in the media.
- Monitor usage of NSA guidance and tools that are provided online (e.g. number of 'hits').