Veiledning

Modenhetsmodell for ledelse

	Utarbeidet av	*Bekreftet av*	*Godkjent av*
Navn	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
Stilling	Prosjektleder	Prosjektansvarlig	Enhetsleder
Dato	06/10/2017	06/10/2017	Skriv inn en dato.
Underskrift			

Dokumenthistorikk

Versjon	*Dato*	*Kommentarer*
0.14	19/07/2017	Inkludert kommentarer fra konsultasjonen
0.15	31/07/2017	Inkludert kommentarer fra konsultasjonen
0.16	06/10/2017	Etter intern gjennomgang
0.18	08/12/2017	Etter intern gjennomgang

1 Innledning

Etter bevilgning av et felles sikkerhetssertifikat eller en sikkerhetsfullmakt må nasjonale sikkerhetsmyndigheter (NSA-er) sørge for at søkeren for et felles sikkerhetssertifikat eller en sikkerhetsfullmakt har demonstrert at sikkerhetsstyringssystemet (SMS) deres er effektivt implementert og fortsetter å innfri de juridiske pliktene. Med andre ord må NSA-er utføre et nivå av kontroll av jernbanebyråenes eller infrastrukturledernes aktiviteter for å sørge for at det som ble sagt i søknaden for et felles sikkerhetssertifikat eller en sikkerhetsfullmakt, reflekterer virkeligheten.

Den europeiske unions jernbanebyrå (også heretter kalt «byrået») har utviklet denne modenhetsmodellen for ledelse (MMM) for å hjelpe NSA-er med å vurdere jernbanebyråenes og infrastrukturledernes SMS under kontrollen.

Bruken av modenhetsmodellen for ledelse kan også fungere som et «vindu» til sikkerhetskulturen til en organisasjon, og hjelpe NSA-er og organisasjonene de regulerer, med å diskutere hvordan disse organisasjonene kan forbedre sitt SMS.

Denne modellen har blitt introdusert av byrået som veiledning. NSA-er kan velge om de vil bruke den. Hvis en NSA har sin egen modell eller en annen måte å vurdere hvor bra et SMS er på, kan den bruke sin egen metode. Ingenting i dette dokumentet bestrider gyldigheten til eksisterende modeller som oppnår samme resultat.

Alle jernbanebyråene eller infrastrukturlederne står også fritt til å bruke modenhetsmodellen for ledelse på sin egen organisasjon når som helst hvis de ønsker det. Materialet er fritt tilgjengelig og kan lastes ned fra byråets nettsted. Byrået vil foreslå at et jernbanebyrå eller en infrastrukturleder bruker modellen gjennom hele femårsperioden for å utføre sin egen vurdering, preget av kontrollaktivitet, og gjennomgå funnene under fornyelsessøknaden for et felles sikkerhetssertifikat eller en sikkerhetsfullmakt. På dette punktet kan den brukes til å fremheve svakhetsområder i SMS som jernbanebyrået eller infrastrukturlederen kan ha, og gi dem mulighet til å håndtere eventuelle mangler før søknaden for et nytt felles sikkerhetssertifikat eller en sikkerhetsfullmakt sendes.

1.1 Formålet med veiledningen

Dette veiledningsdokumentet gir NSA-er en enkel modell som gjør det mulig for dem å vurdere hvor godt jernbanebyråenes og infrastrukturledernes SMS-er fungerer.

Modellen tar sikte på å bruke enkle nivåer til å kategorisere ytelsen eller kapasiteten til SMS, for å skaffe informasjonen den trenger for å gjøre en rimelig nøyaktig vurdering av hele eller en del av en organisasjons SMS, avhengig av hva NSA-en bestemmer seg for å se på under kontrollen.

Det bør merkes at modellen brukes under kontroll, og kontroll kan kun finne sted når et felles sikkerhetssertifikat eller en sikkerhetsfullmakt er bevilget. De forskjellige nivåene i modellen starter derfor fra et punkt der en organisasjon har falt under det knappe minimumet som kreves for å få bevilget et felles sikkerhetssertifikat eller en sikkerhetsfullmakt. Ved nivå 1 vil NSA-en som utfører kontrollen, være forventet å sette i gang tiltak for å rette opp situasjonen. I de mest ekstreme situasjonene kan dette innebære å trekke tilbake det felles sikkerhetssertifikatet eller sikkerhetsfullmakten eller henvise saken til sikkerhetssertifiseringsorganet, for å vurdere dette. Dette er fordi at å yte på dette nivået, vil resultere i at enhver søknad om fornyelse av et felles sikkerhetssertifikat eller sikkerhetsfullmakt vil bli avslått.

1.2 Hvem er denne veiledningen rettet mot?

Det nåværende dokumentet er rettet mot:

- *nasjonale sikkerhetsmyndigheter når de vurderer jernbanebyråers og infrastrukturlederes SMS under kontrollen;*
- *nasjonale sikkerhetsmyndigheter når de etablerer sin kontrollstrategi og -plan(er);*
- *nasjonale sikkerhetsmyndigheter når de deler informasjon mellom seg, der det er felles eller koordinert kontroll, om sikkerhetsytelsen innenfor deres respektive medlemsland;*
- *nasjonale sikkerhetsmyndigheter nå de deler informasjon med byrået etter mottak av en søknad om fornyelse eller oppdatering, der byrået er ansvarlig for utstedelse av det felles sikkerhetssertifikatet; og*
- *jernbanebyråene og infrastrukturlederne som en selvvurderingsøvelse for å evaluere sin SMS-ytelse, spesielt før de sender inn en fornyelsessøknad for sine felles sikkerhetssertifikater eller sikkerhetsfullmakter.*

1.3 Virkeområde

NSA må ha noen måter å måle kvaliteten til SMS på i praksis mot teorien som presenteres i søknadsfasen for det felles sikkerhetssertifikatet eller sikkerhetsfullmakten (for en infrastrukturleder). Byråets modenhetsmodell for ledelse kan fylle dette behovet, men alle individuelle NSA-er står fritt til å finne opp sin egen metode for å gi slik kontrollinformasjon til byrået.

Modellen er ikke ment å være det absolutte svaret på spørsmålet om hvor godt et individuelt SMS er, men heller en måte å gi strenghet og struktur til vurderingen av NSA om emnet.

1.4 Veiledningens struktur

Dette dokumentet er en del av byråets kompendium av veiledning som støtter jernbanebyråene, infrastrukturlederne, de nasjonale sikkerhetsmyndighetene og byrået i oppfylling av rollene deres og utførelse av oppgavene deres i henhold til direktiv (EU) 2016/798.

Figur 1: Kompendium av byråveiledning

Byråets modenhetsmodell for ledelse bruker den samme strukturen som Vedlegg I og II i Kommisjonens delegerte forordning (EU) …/… *[CSM-er for SMS]* for å danne en vurdering om kvaliteten til en organisasjons SMS. Den innfrir også NSAs behov for et verktøy som kan brukes til å oppfylle behovene angitt i Artikkel 7(1) i Kommisjonens delegerte forordning (EU) …/… *[CSM-er for kontroll]* for evalueringen av effektiviteten til SMS, og i Artikkel 5(2) av den samme forordningen for evalueringen av sikkerhetsstyringsytelsen til jernbanebyrået eller infrastrukturlederen. Tilnærmingen vedtatt i Artikkel 5(2) tar sikte på å skape en sterk kobling mellom vurdering og etterfølgende kontroll, muliggjøre en bedre informasjonsveksling innenfor NSA-er og mellom NSA-er og byrået (dvs. mellom de som utfører kontrollen og de som utfører vurderingen) og til slutt, bringe mer klarhet for jernbanesektoren til å forstå hvordan deres egen sikkerhetsytelse preger NSAs kontroll (dvs. prioritering av kontrollaktiviteter til områder med størst sikkerhetsrisiko).

Hver del av modellen har et formål som forklarer hva delen handler om, og i noen tilfeller noen innledende merknader for ytterligere oppklaring. For hver del indikeres 5 nivåer: Grunnleggende — nivå 1, Mestring — nivå 2, Konsekvent — nivå 3, Forventet — nivå 4 og Utmerket — nivå 5. Hvert av disse nivåene har noe tekst som forklarer hva ytelse på dette nivået mot kriterieelementene ser ut som. Brukeren må vurdere bevisene denne har fått fra intervjuer, dokumentgjennomgang osv., og gjøre en vurdering om det som passer best mot et bestemt nivå. Fra nivå 2 og oppover indikerer teksten at ytelsen skal vurderes mot det foregående nivået pluss det neste nivået, slik at nivå 4 inkluderer elementene fra nivå 3 pluss de som kommer i tillegg for nivå 4. Dette er fordi nivå 2 er det første nivået der ytelse anses å være juridisk samsvarende.

For å generere nivåene mot hvert kriterium og motta en representasjon av resultatene i diagramform må brukeren fylle ut Excel-regnearket som følger med modellen. Når du angir tallene i regneark 1, fylles radardiagrammet i diagram 1 ut. Når du er ferdig, kan det resulterende diagrammet kopieres inn i rapporten til jernbanebyrået/infrastrukturlederen.

Vedlegget presenterer en tabell som gjør det mulig å angi nivåene ved bruk av et trafikklyssystem. Igjen kan dette kopieres inn i den endelige rapporten til jernbanebyrået/infrastrukturlederen når det er ferdig. Om du vil bruke én eller begge måtene å representere funnene på, er et valg som hver NSA (eller jernbanebyrå/infrastrukturleder) må ta.

1.5 Fire ting du må vite før du bruker modellen

Det er fire ting som må huskes når du bruker en slik modell:

1) Det er et øyeblikksbilde i tid av den delen av SMS som ses på.
2) Det numeriske nivået er mindre viktig enn hva vurderingen sier om hvor godt SMS fungerer.
3) Ettersom resultatene av revisjoner/inspeksjoner av separate deler av SMS mest sannsynlig varierer, *kan funnene brukes som indikatorer for å prege den totale kapasitetsvurderingen* til et jernbanebyrås eller infrastrukturleders ytelsesgjennomsnitt. Når modellen brukes av godt opplærte ansatte, gir modellen et bilde av ytelsen til et individuelt SMS, og gir dermed et fokus for forbedring av områder som yter mindre godt. På et nasjonalt nivå kan den også gi et samlet bilde for NSA om hvor de skal rette begrensede ressurser for å forbedre sikkerhet, siden den kan vise for eksempel en systematisk svakhet for hele jernbanebransjen i et bestemt område av sikkerhetsstyring. Hvis for eksempel alle jernbanebyråenes resultater indikerer et lavt nivå for risikovurdering, kan dette være en viktig tilbakemelding for NSA når de skal utvikle kontrollstrategien.
4) Det er viktig at både NSA og organisasjonen som vurderes, er veldig tydelige i forhold til omfanget og nivået av inngrepet når de avtaler omfanget av vurderingen ved bruk av modellen. Dette er spesielt viktig siden dette vil reflektere tillitsnivået som kan legges i NSAs vurderinger.

Innhold

2 Modenhetsmodellen for ledelse og risikokontroll

Vurderingen av SMS tjenestegjør som en fullmakt for å ta en vurdering angående organisasjonens kapasitet til å kontrollere risikoene fra dens jernbanevirksomhet. Hvis SMS fungerer bra, er det en rimelig antagelse at risikoene fra organisasjonens virksomhet blir kontrollert bra. Hvis organisasjonens SMS har svake områder, er det en indikasjon på utilstrekkelig risikokontroll i disse områdene. Som et resultat er det sannsynlig at det i disse områdene vil være størst sannsynlighet for at tilstandene som vil gjøre det mulig for en ulykke eller hendelse å oppstå, eksisterer, sammenlignet med andre områder der SMS yter bra. Derfor, jo høyere poengsum under MMM, jo bedre er risikokontrollen.

2.1 Hva er et akseptabelt nivå som kan nås innenfor modellen for en NSA?

Hvis du ser på modellen nedenfor, kan det anses at når en organisasjon har nådd (nivå 3), vil den normalt yte på en måte som skal sikre at SMS leverer et passende nivå av risikostyring og -kontroll. Dette er selvfølgelig et nivå over det hvor minimum juridisk samsvar oppnås (nivå 2). Det er en god grunn til dette. På nivået for minimum juridisk samsvar er det en konstant risiko for å falle under det, til nivå 1, som er under det nivået. På nivå 3 er selvfølgelig nivå 2 nivået under, så det er noe isolering fra et uakseptabelt ytelsesnivå. Det vil imidlertid være feil for organisasjoner å sikte mot nivå 3 som nivået de skal oppnå. Formålet med modellen er å hjelpe NSA-en i en diskusjon med et jernbanebyrå eller en infrastrukturleder om svakhetsområder i deres SMS og hvor de kan **forbedre** seg. Fra et NSA-perspektiv — gitt at NSA skal fokusere ressurser på områdene med størst risiko — kan NSA, hvis det viser seg at et jernbanebyrå eller en infrastrukturleder yter på de høyere nivåene av modellen, selvsagt avgjøre å redusere kontrollen av denne organisasjonen i en periode sammenlignet med et jernbanebyrå eller en infrastrukturleder som yter på de lavere nivåene og må forbedre seg. Dette kan være et insentiv for jernbanebyråer og infrastrukturledere til å prøve å forbedre sitt SMS, slik at de kan komme på den høyere enden av spektrumet. Det er også verdt å påpeke at noen NSA-er som bruker slike modeller, har erfart at bruken av de forskjellige nivåene skaper konkurranse mellom jernbanebyråer, spesielt til å strebe etter å bli bedre i sikkerhetsstyring enn konkurrentene. Dette kan også ha implikasjoner for evnen deres til å vinne nye kontrakter i fremtiden, avhengig av forretningsmulighetene som er tilgjengelige for individuelle medlemsland.

2.2 Bruk av modellen på tvers av nasjonale sikkerhetsmyndigheter med ulike rettslige myndigheter

Den nåværende modellen er ment å hjelpe NSA-er med å vurdere evnen til jernbanebyråers og infrastrukturlederes SMS-er innenfor vilkårene til jernbanesikkerhetsdirektivet og dets tilknyttede forskrifter. Det bør også merkes at selv om dette respekteres, kan NSA også operere innenfor myndighetene tildelt dem av nasjonal lovgivning. Dette betyr for eksempel at noen NSA-er har ansvar for å sikre at yrkeshelsesaker håndteres korrekt av jernbanebyråer og infrastrukturledere innenfor deres medlemsland, og noen har ikke det. I modellen nedenfor dekkes derfor ikke yrkeshelsesaker i tekstveiledningen. Hvis en NSA imidlertid valgte å bruke modellen på tvers av sikkerhets- og yrkeshelsesaker, kan de grunnleggende prinsippene oppført nedenfor enkelt brukes på disse elementene.

2.3 Rapporter

Når en vurdering er utført, kan det skrives en rapport som oppsummerer resultatene som ble funnet. Rapporten skal spesifisere beviset som fører til konklusjonen av et bestemt nivå. Funnene kan presenteres som enten et radardiagram eller en trafikklystabell. Formålet med rapporten er å identifisere styrker og svakheter, og for å gi grunnlaget for en diskusjon med organisasjonen om hvilke områder de kommer til å forbedre over levetiden til et felles sikkerhetssertifikat eller sikkerhetsfullmakt. Når rapporten skrives, skal vurderingens dybde tydelig angis ved begynnelsen, slik at det er en forståelse av nivået som NSA har gransket SMS-ordningene i et bestemt område.

2.4 Forutsetning for bruk av modellen

Alle NSA-ansatte som bruker modellen, anses som kompetente i bruken av den. Bruk av modellen krever at de NSA-ansatte forstår delene av SMS som angitt i Vedlegg I og II i CSM for sikkerhetsstyringssystemer i tillegg til selve modellen. De ansatte må også være kompetente i egnede intervju- og inspeksjonsteknikker og være i stand til å ta en rekke informasjon fra forskjellige kilder og destillere den inn i relevante deler av SMS. I praksis bør dokumentgjennomgang, der det er mulig, utføres før intervjuer på stedet. MMM er utformet for å brukes av én kompetent person, men på grunn av logistiske problemer med å utføre flere intervjuer og gi ytterligere bekreftelse av funnene, er det god praksis å bruke flere kompetente personer som kan støtte hverandre under kontrollaktiviteten.

2.5 Hvordan brukes modellen?

MMM-modellen er ikke en erstatning for vurderingen av personen som utfører kontrollen. Det er heller et hjelpemiddel for å ta en vurdering som muliggjør skarpere fokus og en bedre forbindelse mellom den, beviset som vurdering er basert på, og elementene til et SMS. Den vil derfor hjelpe de som utfører kontrollen, til å presentere funnene for jernbanebyråer og infrastrukturledere, og for jernbanebyråer og infrastrukturledere til å forstå hvorfor de funnene har oppstått. Hvis for eksempel intervjuer, dokumentgjennomganger og feltarbeid viser at en organisasjon ikke har et robust dokumentgjennomgangssystem, kan dette flagges som en svakhet for SMS av NSA-en som utfører kontrollen, og beviset for dette kan diskuteres med organisasjonen og hjelpetiltak kan avtales. NSA-en kan også bruke svakheten i dokumentgjennomgangssystemet til en organisasjon til å fremheve problemer med intern revisjon og overvåking, siden disse skal finne slike problemer.

Modellens forskjellige overskrifter tilsvarer de forskjellige delene av SMS som angitt i Vedlegg I og II i CSM for krav for sikkerhetsstyringssystemer. Dette betyr at det er en direkte forbindelse mellom denne modellen, som brukt i kontroll, og vurderingen utført av NSA eller byrået (som opptrer som sikkerhetssertifiseringsorgan), som er nødvendig før et felles sikkerhetssertifikat eller en sikkerhetsfullmakt bevilges. Dette betyr også at forsiktig og planlagt bruk av denne modellen som et kontrollverktøy av en NSA, kan oppfylle funksjonen om å sjekke at organisasjonen som har blitt bevilget et felles sikkerhetssertifikat eller en sikkerhetsfullmakt, har et SMS som leverer hva det sa det gjorde ved søknaden for levetiden til et felles sikkerhetssertifikat eller en sikkerhetsfullmakt. Så resultatet av MMM er viktig informasjon for organisasjonen og sikkerhetssertifiseringsorganet, ettersom det vil være relevant for søknader for fornyelsen av felles sikkerhetssertifikater og sikkerhetsfullmakter. Det noteres også at de enkelte elementene til SMS som angitt i modellen, alle er forbundet sammen og danner en samlet helhet. Dette betyr at NSA-en i vurderingen av de samlede funnene kan vurdere ytelsesspørsmålet til SMS innenfor de individuelle elementene, men den kan også vurdere hva dette betyr for den samlede ytelsen.

En NSA kan bruke MMM umiddelbart etter bevilgningen av et felles sikkerhetssertifikat eller en sikkerhetsfullmakt, for å gi et grunnlinjebilde av ytelsen til et sikkerhetsstyringssystem ved begynnelsen av levetidsperioden til det felles sikkerhetssertifikatet eller sikkerhetsfullmakten. Informasjonen som samles inn ved dette trinnet kan deretter danne grunnlaget for planlagt kontroll for den gjenværende perioden til det felles sikkerhetssertifikatet eller sikkerhetsfullmakten. Denne tilnærmingen kan være passende der den involverte organisasjonen har hatt tidligere SSC/SA og derfor har noe erfaring med arbeidet til sitt SMS. For en ny konkurrent på markedet uten tidligere erfaring med SMS kan umiddelbar kontroll med MMM ikke gi mye mer informasjon enn det som ble funnet ut på vurderingstrinnet, ettersom SMS er nytt og uprøvd. Alternativt, når det felles sikkerhetssertifikatet eller sikkerhetsfullmakten er bevilget, kan kontrollmyndigheten som bruker informasjon videresendt fra vurderingsmyndigheten om interesseområder for kontroll, planlegge bruken av MMM over levetiden til det felles sikkerhetssertifikatet eller sikkerhetsfullmakten og ta hensyn til behovet for å gi tid for å prøve ut organisasjonens SMS i praksis.

NSA-en rådes til å bruke resultatene til MMM som en tilbakemelding for kontrollstrategien (og følgelig kontrollplanene). I praksis betyr dette kanskje at mindre kontroll gis til organisasjoner eller deler av organisasjoner som får høye nivåer på MMM, enn de som gis mer moderate nivåer totalt eller på bestemte områder. Selv om denne tilnærmingen er en legitim bruk av informasjonen fått for å prioritere risikoer, skal den avveies mot den relative risikoen for den samlede virksomheten. For eksempel kan et fraktselskap som spesialiserer seg i transport av farlig gods, få nivå 4 og 5 på MMM og kan derfor anses som å ha et svært modent SMS, og likevel vil det fortsatt være passende å utøve nøye kontroll av det, gitt naturen til risikoene tilknyttet virksomheten.

Når et nivå tilordnes et element basert på beviset, er det sannsynlig at kontrollen vil identifisere både positive og negative sider. Det må derfor tas en avgjørelse om hvorvidt et høyere eller lavere nivå på skalaen skal tildeles. En vurdering må så klart tas på grunnlag av beviset som er tilgjengelig. Hvis dette peker mot et høyere heller enn et lavere nivå, så bør dette reflekteres i avgjørelsen som tas. Hvis beviset er tvetydig, bør personen som utfører kontrollen, søke etter mer bevis i løpet av målrettet nåværende og/eller fremtidige kontrollaktiviteter (f.eks. virkelighetskontroller/-inspeksjoner for å gjøre en mer nøyaktig vurdering, eller et lavere nivå skal brukes fordi det ikke finnes bevis som støtter et høyere nivå). Når avslutningsmøtet med jernbanebyrået/infrastrukturlederen holdes, kan vanskeligheten med å ta en avgjørelse tas opp og jernbanebyrået/infrastrukturlederen gis en mulighet til å fremlegge ytterligere bevis. Du bør imidlertid være forsiktig hvis du gjør dette. En slik handling bør være en uvanlig hendelse heller enn standarden, siden det å tillate ytterligere bevis kan føre til at jernbanebyrået/infrastrukturlederen håndterer problemer på dette trinnet i stedet for å fikse dem innenfor omfanget til handlingsplanen påfølgende kontrollaktiviteten.

Spørsmålet om hvor mye bevis som kreves for å gjøre en nøyaktig vurdering, er vanskelig å svare på. Beviset vil i de fleste tilfeller være en kombinasjon av intervjuer, dokumentarisk bevis, feltobservasjon og resultatene av hendelses-/ulykkesundersøkelser på gitte tidspunkter, datoer og steder. Grunnlaget for vurderingen må være bevisene som er funnet. Så hvis jernbanebyrået/infrastrukturlederen argumenterer at det som ble funnet, ikke er representativt, så forandrer ikke det resultatet, siden det som ble funnet, ble funnet. At det var mulig å finne en løsning som jernbanebyrået/infrastrukturlederen ikke anerkjenner, indikerer i seg selv at det er problemer med hvordan SMS fungerer. At jernbanebyrået/infrastrukturlederen motsetter seg dette, er også et signal om at ikke alt er som det skal. Hvis et antall beviser peker til at et område under inspeksjon blir administrert på en bra måte, vil det være legitimt å stoppe å lete etter bevis på det punktet. Hvis beviset i motsetning ikke gir den overbevisningen, men det ikke er mulig å fastsette hvorfor, skal det letes etter ytterligere bevis. Det er ikke nødvendig å undersøke alle prosesser og prosedyrer fra det høye nivået til de detaljerte arbeidsinstruksjonene for å trekke konklusjoner om systemet fungerer effektivt eller ikke. Nok informasjon fra dokumentgjennomgang og intervjuer må trekkes frem for å konkludere med et rimelig nivå av sikkerhet hva bildet ser ut som i praksis. . Det bør huskes på at en rapport laget ved bruk av MMM, til syvende og sist er en rapport laget av en kompetent person, som bruker modellen til å støtte sin profesjonelle vurdering, og basert på et utvalg av dokumenter, intervjuer og annen informasjon er det usannsynlig at det representerer et absolutt bilde av en organisasjons ytelse, siden dette vil kreve gjennomgang av all informasjon som er relatert til organisasjon og intervjuer med hver person som arbeider for organisasjonen, og eventuelle organisasjoner som har kontakt med den.

Generelt sett ses det etter bevis på at området som er under granskning, a) administreres på en sikker måte, b) at denne administreringen er logisk og knyttet til måten som SMS er ment å fungere i henhold til den opprinnelige søknaden for et felles sikkerhetssertifikat eller sikkerhetsfullmakt, og c) organisasjonen er klar over hva som foregår. Hvis a) eksisterer uten b) eller c), kan det sies at sikkerhet blir administrert av flaks heller enn av en logisk plan, noe som tydelig antyder et mangelfullt SMS.

Det er ekstremt viktig at når funnene presenteres til organisasjonen som har blitt vurdert, blir det gjort veldig tydelig hvilket nivå vurderingen har vært. Det skal noteres i rapporten hvilke bevis man har sett, og hvilke personer som har blitt intervjuet. Der eksempler på manglende dokumentasjon blir funnet, skal disse også legges ved rapporten.

Hvis modellen brukes til å vurdere bestemte områder av SMS, så skal områdene som ikke vurderes, tydelig identifiseres i omfanget av studien, og skal ikke gis et nivå i den endelige rapporten med mindre tilstrekkelig bevis dukker opp fra områdene i omfanget av studien til å kommentere dem. For eksempel: Mens en studie utføres om aktivaforvaltning, blir det tydelig at det er et svakt kompetansestyringssystem. I dette tilfellet vil det være legitimt å gi et nivå til dette området, selv om det ikke var hovedfokuset for revisjonen som bruker modellen.

Personen eller personene som utfører kontrollen, skal gjennomføre nok intervjuer/dokumentgjennomganger/feltarbeid til å være sikre på at de har et godt bilde av hva som foregår. Bildet må ikke være komplett, men nok bevis må være samlet inn for å rettferdiggjøre punktet der jernbanebyrået/infrastrukturmodellen plasseres i modellen. For et lite jernbanebyrå / en liten infrastrukturleder bør intervjuer av overordnet nøkkelpersonale være nok til å etablere hvor organisasjonen sitter når det gjelder for eksempel ledelse. For et stort jernbanebyrå / en stor infrastrukturleder med flere baser og en ledelsesstruktur med flere lag, vil det være vanskeligere å få et komplett bilde, og flere valg må tas angående hvem som skal intervjues på et overordnet nivå. I disse forholdene vil det være legitimt å ta et vertikalt snitt gjennom organisasjonen, muligens på årlig basis, og se på forskjellige områder hver gang og intervjue et passende antall personer ved hvert ledelsesnivå for å kunne danne et veloverveid overblikk over emneområdet.

For store og komplekse organisasjoner vil det være passende å bruke modellen til å få et samlet bilde av hvordan organisasjonen drives, for eksempel ved å se på dokumentasjon på høyt nivå og intervjue overordnede ledere, før modellen brukes til å se på diskret aspekter av aktiviteten deres, for eksempel vedlikehold av kjøretøyer på flere anlegg. I et slikt tilfelle for en velkjent organisasjon med et godt SMS, skal det være mulig å se at oppfatningen/dokumentasjon på høyt nivå reflekteres på samme måte i hvert av vedlikeholdsdepotene som ble sett på. Dette betyr ikke at det ikke kan være forskjeller mellom selve depotene, men ganske enkelt at den samlede strukturen i nøkkelelementene er den samme og drives på samme måte. Tilsvarende vil man for en organisasjon som yter dårlig, forvente å se forskjeller mellom oppfatningen som den generelle ledelsen har av hvordan organisasjonen drives ved vedlikeholdsdepotnivået, og det i selve depotene, i tillegg til betydelige forskjeller mellom selve depotene som kan omdannes til sikkerhetsrisiko, f.eks. forskjeller i periodisiteten til undersøkelsen av lignende kjøretøy uten noen forklaring for hvorfor dette kan være, mens ledelsen kun gjenkjenner én slik vedlikeholdsstruktur.

Nummereringssystemet i modellen er der for å hjelpe med kategoriseringen av modenhet for ledelse. Det å få en viss poengsum burde ikke ses på som et mål i seg selv. Når funnene presenteres for et jernbanebyrå/infrastrukturleder, er det svært viktig å understreke dette poenget og legge vekt på at resultatene er vurderingen til personen som utfører kontrollene, basert på bevisene sett på et bestemt tidspunkt og sted.

Noe motstand kan forventes fra jernbanebyråene eller infrastrukturlederne som motsetter seg «nivået», og i det tilfellet er det viktig å legge vekt på at det er NSAs oppfatning basert på beviset som er sett og hørt, og de er berettiget til en annen oppfatning basert på sin egen kunnskap om organisasjonen. Hvis jernbanebyrået/infrastrukturlederen prøver å håndtere problemet ved å gi mer bevis, må det tas et valg om hvorvidt dette skal godtas, som notert ovenfor, og endre funnene som et resultat, eller å påpeke at funnene er de som ble funnet på tidspunktet for kontrollen. Alt bevis som leveres etter kontrollen, som gir en mer positiv oppfatning, skal generelt sett sendes inn som en del av beviset for å oppfylle handlingsplanen avtalt mellom organisasjonen og NSA.

Ved avslutningsmøtet skal det legges vekt på at poenget med øvelsen er å hjelpe jernbanebyrået/infrastrukturlederen med å forbedre deres SMS. Handlingspunkter skal identifiseres for å håndtere eventuelle mangler når det kommer til juridiske krav, dvs. ved nivå 1 og forbedringspunkter identifisert for nivå 2 og høyere. Disse skal avtales med jernbanebyrået/infrastrukturlederen, og jernbanebyrået/infrastrukturlederen skal forplikte seg til å produsere en tidsbundet handlingsplan som tar

tak i disse, og som gir detaljer om hvem som vil være ansvarlig for hva og når endringene skal leveres, slik at NSA kan følge opp disse som hensiktsmessig.

Modellen er der for å hjelpe med å utføre kontrollen, den er ikke der for å erstatte profesjonell vurdering. Den gir ikke det eksakte svaret på hva som oppdages under kontrollen, og den indikerer heller ikke hva som skal gjøres med det. Alle iverksettelseshandlinger som kan følge kontrollen ved bruk av modellen, er opp til NSA å avgjøre, basert på de rettslige myndighetene som NSA har, men støtter seg tydelig på bevisene oppdaget under MMM-revisjonen. For å hjelpe NSA-er med å finne ut hvilke iverksettelseshandlinger som kan være passende, har byrået produsert en ledelsesmodellveiledning for iverksettelse.

Modellen kan også brukes til å se på funn fra ulykkesundersøkelser eller selskapets revisjonsrapporter. I dette tilfellet skal funnene i rapporten analyseres for å se hva de sier om SMS. Når de relevante kriterieelementene har blitt identifisert, kan en vurdering tas ved bruk av modellen angående organisasjonens modenhet basert på funnene i revisjonen eller ulykkesundersøkelsesrapporten. For en enkelt rapport forteller kanskje ikke dette deg veldig mye om organisasjonens sikkerhetsstyringskapasiteter, men hvis den utføres som en øvelse én gang i året eller hvert andre år der flere rapporter kan undersøkes, kan det være et kraftig verktøy for å identifisere områder av organisasjonens SMS der problemer fortsetter å oppstå.

3 Modellnivåer

Strukturen som brukes, er en skala fra 1 til 5 der 1 representerer svak ytelse av styringssystemet, og 5 representerer en utmerket styringsytelse.

3.1 Definisjon av prestasjonsnivåer

Nivå 1 — Grunnleggende

På dette nivået har organisasjonen som vurderes, et sikkerhetsstyringssystem, men det er tydelig at det er mangler som bringer ytelsesnivået under det som var påkrevd for bevilgning av et felles sikkerhetssertifikat eller sikkerhetsfullmakt. Prosedyrer og instruksjoner for å håndtere sikkerhetsaktiviteter eksisterer, men i løpet av kontrollen er det åpenbart at det er alvorlige problemer angående hvor logiske disse er som en helhet. Individuelle risikoer kontrolleres, men den samlede prosessen som håndterer dette, er svak. Organisasjonen drives i praksis på en måte der det ser ut til å være større uforenligheter med det som er beskrevet i SMS. Retningslinjer, prosedyrer og instruksjoner ser ut til å brukes på måter som ikke tilsvarer de angitt i SMS, og derfor blir ikke risikoene fra virksomheter levert av organisasjonen eller dens entreprenører nødvendigvis tilstrekkelig kontrollert. På dette nivået skal NSA vurdere tiltak for å bringe organisasjonen tilbake til juridisk samsvar (se *byråets veiledning for ledelsesmodell for iverksettelse* for mer informasjon om hvordan denne prosessen kan fungere).

Nivå 2 — Mestring

På dette nivået yter organisasjonen på nivået for minimum juridisk samsvar, dvs. SMS fungerer på et nivå som var tilstrekkelig for at et felles sikkerhetssertifikat eller sikkerhetsfullmakt ble bevilget ved vurderingstrinnet. Det skriftlige sikkerhetsstyringssystemet eksisterer og blir brukt til å kontrollere sikkerhetsrisikoer, men det mangler struktur og koordinering. Systemet er logisk generelt sett, men det finnes mangler og noen tilnærmingsuforenligheter i forskjellige områder. Organisasjonen mestrer hovedsakelig sikkerhetsansvaret sitt, men det er så vidt. Det vil ikke kreve mye å skape et betydelig problem og falle tilbake til nivå 1, fordi mangelen på integrasjon mellom prosedyrer og risikohåndtering kan bli et betydelig problem når det kommer til tekniske, driftsmessige og organisatoriske risikoer. Noen områder innenfor virksomheten yter bedre på sikkerhetsstyring enn andre. Risikoer kontrolleres mer av handlingene til personer som arbeider for organisasjonen, enn gjennom utformingen av SMS. En brannslokkingstilnærming til risikohåndtering er den normale situasjonen, noe som gjør at selskapet drives reaktivt til ulykker eller hendelser heller enn å proaktivt iverksette tiltak for å forhindre dem.

Nivå 3 — Konsekvent

SMS er utviklet for å skape en systematisk og konsekvent tilnærming til håndteringen av risiko. Alle elementene er på plass og fungerer, og alle sikkerhetsaspekter vurderes. Noe vurdering gis til forbedringen av sikkerhetskulturen innenfor organisasjonen gjennom utviklingen av en forbedringsstrategi for sikkerhetskultur. Selv om organisasjonen er konsekvent, prøver den ikke å forutse risikoer på forhånd, og kulturen innenfor organisasjonen er heller ikke utviklet nok til å selvstendig opprettholde prosessen for risikohåndtering. Brannslokking har gitt etter for en mer veloverveid tilnærming til risikohåndtering, men det vil ikke ta veldig mye (f.eks. det å ikke håndtere viktige prosesser eller prosedyrer over tid) før organisasjonen faller tilbake til mestringsmodus.

Nivå 4 — Forventet

Som for nivå 3, og i tillegg håndterer SMS konstant risiko proaktivt. Her overvåker organisasjonen forløpere for risiko og iverksetter tiltak på forhånd, der mulig, for å forhindre at farlige hendelser oppstår. Organisasjonen er forpliktet til å utvikle en sikkerhetskultur, arbeidsstyrken er engasjert i innsatsen for å håndtere sikkerhet på en logisk og fremtidsrettet måte. På dette nivået er det virkelig ledelse fra toppen av organisasjonen, og de ansatte i organisasjonen har tro på og respekterer ledelsens tilnærming. Det går mye

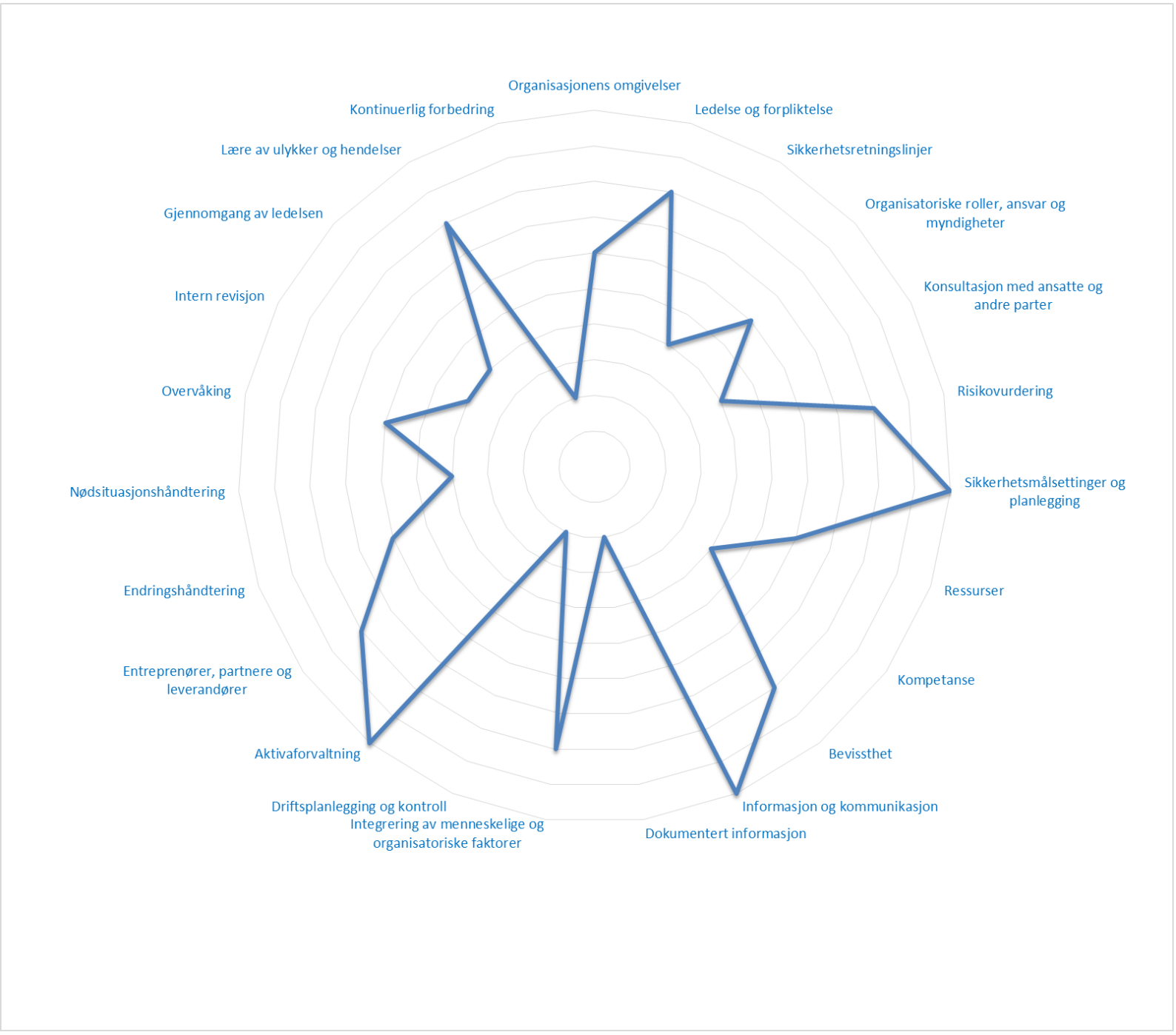
innsats i jevnlige gjennomganger av ytelse og å forstå naturen til risikoene organisasjonen står overfor, og hva som kan gjøres med det.

Nivå 5 — Utmerket

Som for nivå 4, og i tillegg er sikkerhetsstyringssystemet konstruert på en måte som muliggjør kontinuerlig forbedring. Organisasjonen søker aktivt ut muligheter til å forbedre sikkerhet, og utvikler positivt dens sikkerhetskultur ved å bruke informasjon fra både innenfor jernbanesektoren og utenfor den. Organisasjonen måler sin egen ytelse mot andres, både innenfor jernbanesektoren og utenfor. Det finnes bevis for at organisasjonen er klar over problemer den har eller kan ha i fremtiden, og prøver aktivt å håndtere dem gjennom SMS. På dette nivået er organisasjonen sikker på dens evne til å håndtere risikoene den møter, og ser utover for å lære opp de som den har kontakt med, og i tillegg prøver den å ta lærdom fra andre felt som kan inkorporeres i virksomheten. Sikkerhet er en vesentlig del av organisasjonens virksomhet.

3.2 Rapportere resultatene til modellen

Resultatene til modellen kan angis som et radardiagram (sett inn kobling til kalkulator for Excel-regneark her) eller som et trafikklyssystem som vist i eksemplene i Figur 2 og Tabell 1 nedenfor. Begge kartlegger SMS-kravene for Kommisjonens delegerte forordning (EU) …/… *[CSM-er for SMS]* mot de 5 prestasjonsnivåene, ved å sette inn det relevante ytelsesnivået for å få et svært visuelt bilde av sikkerhetsytelsen til organisasjonen.



Figur 2: Eksempelrepresentasjon av modellresultatene i radardiagram.

Tabell 1: Trafikklyssystem etter nivå.

PDCA-elementer fra SMS	*Nivå 1*	*Nivå 2*	*Nivå 3*	*Nivå 4*	*Nivå 5*
Organisasjonens omgivelser					
Ledelse					
Ledelse og forpliktelse					
Sikkerhetsretningslinjer					
Organisatoriske roller, ansvar og myndigheter					
Konsultasjon med ansatte og andre parter					
Planlegging					
Tiltak for å håndtere risiko					
Sikkerhetsmålsettinger og planlegging					
Støtte					
Ressurser					
Bevissthet					
Informasjon og kommunikasjon					
Dokumentert informasjon					
Integrering av menneskelige og organisatoriske faktorer					
Drift					
Driftsplanlegging og kontroll					
Aktivaforvaltning					
Entreprenører, partnere og leverandører					
Endringshåndtering					
Nødsituasjonshåndtering					
Ytelsesevaluering					
Overvåking					
Intern revisjon					
Gjennomgang av ledelsen					
Forbedring					
Lære av ulykker og hendelser					

Tabell 1: Trafikklyssystem etter nivå.

PDCA-elementer fra SMS	*Nivå 1*	*Nivå 2*	*Nivå 3*	*Nivå 4*	*Nivå 5*
Kontinuerlig forbedring					

Det bør imidlertid forstås at grensene mellom de forskjellige nivåene defineres i overgangen fra nivå 1 til nivå 2, fordi nivå 1 ikke er nivået for minimum juridisk samsvar mens nivå 2 er det. Overgangen fra gul til grønn når du går fra 2 til 3, er imidlertid en mer ugjennomsiktig grense ettersom organisasjonen er juridisk samsvarende, men forbedrer seg i sin SMS-kvalitet og -ytelse.

For å bruke denne modellen må organisasjonen som kontrolleres, ha et sikkerhetssertifikat, siden kontroll kun kan finne sted når et sertifikat er bevilget. Det modellen prøver å gjøre, er å hjelpe personen som utfører kontrollen, med å ta en vurdering om hvor bra sikkerhetsstyringssystemet er i praksis. Nivå 1 anses å være et nivå under minimum juridisk samsvar, og derfor et nivå der forbedring kreves for å unngå å motta sanksjoner fra NSA for å ikke oppfylle tilstandene som et felles sikkerhetssertifikat eller sikkerhetsfullmakt ble bevilget under.

Fra nivå 2 (minimum juridisk samsvar) og oppover er det utvikling fra et nivå til et annet. Av denne grunn ses ikke nivå 2 som kumulativt i delen nedenfor, men nivå 3–5 gjør det, dvs. når du når nivå 2, er du i samsvar med dine grunnleggende juridiske krav. Ved nivå 3 har du nådd en rimelig og konsekvent standard for sikkerhetsstyringssystem og kan opprettholde dette over tid, slik at du kan bygge på dette for å oppnå høyere nivåer. Ved å bruke trafikklyssystemet kan du enkelt se i store trekk at nivå 1 (det røde) tilsvarer dårlig ytelse, nivå 2 (det gule) er tilstrekkelig og konsekvent til utmerket etter hvert som du går opp til nivå 3, 4 og 5 (det grønne).

Vedlegget viser systemet med fem nivåer tegnet inn mot trafikklyset for tydelighet, med generelle utsagn som indikerer hvordan hvert nivå ser ut i praksis. Pilen nedenfor tabellen er en påminnelse om at grensene mellom nivåene ikke er faste:

- **Grønn** når rangeringen er lik nivå 3, 4 og 5 og ytelsen anses som konsekvent, forventet eller utmerket;
- **Gul** for nivå 2 der ytelsen anses som mestring;
- **Rød** for nivå 1 der ytelsen anses som grunnleggende.

4 Modenhetsmodellen for ledelse

4.1 C — Organisasjonens omgivelser

Formål

For å få et felles sikkerhetssertifikat eller sikkerhetsfullmakt må søkeren beskrive typen, omfanget og området for virksomheten, vise hvordan den identifiserer de alvorlige risikoene den står overfor, identifisere «interesserte parter», indikere hvordan den overholder de juridiske sikkerhetspliktene og hva disse er, og forklare omfanget til dens SMS. Formålet med dette er å angi omfanget og skalaen til virksomheten for vurderingspersonen. Fra et kontrollperspektiv vil det være viktig å sjekke at garantiene som ble gitt i dette området av en søker, for eksempel forståelsen av risikoen og hvordan denne håndteres i SMS, reflekteres i den daglige driften av virksomheten.

Innledende notater

Det er kritisk viktig at en organisasjon kan formidle til sikkehetssertifiseringsorganet den korrekte typen, omfanget og området til virksomheten. Dette er fordi disse elementene angir grensene for virksomheten, og organisasjonens SMS bør reflektere dette. Av den grunn er dette elementet det første i beslutningstakingskriteriene, ettersom det tilrettelegger for alt som følger etter. Fra et kontrollperspektiv er det derfor svært viktig at virksomhetens virkelighet reflekterer nøyaktig posisjonen som ble erklært ved vurderingen, for hvis den ikke gjør det, er implikasjonen at vurderingen ble utført med ufullstendig informasjon.

Det å identifisere alvorlige risikoer i dette tilfellet betyr at søkeren skal vise at de på bakgrunn av analysen er klar over hvilke av risikoene de står overfor, som er de viktigste. Dette hjelper med å angi omgivelsene for organisasjonen, og viser vurderingsmyndigheten at de forstår miljøet de arbeider i. Aktivitetene til andre parter utenfor jernbanesystemet kan også påvirke sikkerheten til virksomheter, og da må de også tas hensyn til i risikovurderingen.

4.1.1 C1 — Organisasjonens omgivelser

Nivå 1

På dette nivået er grunnleggende beskrivelser på plass, og typen, omfangsområdet og/eller virksomhetens karakter er rimelig tydelige, men i praksis ser det ut til å være forskjeller i omfanget til SMS sammenlignet med vurderingen, og det er tvil om alle alvorlige risikoer har blitt tilstrekkelig registrert. Det finnes tvil om hvorvidt organisasjonen effektivt overholder alle juridiske bestemmelser, som den påstår at den gjør. Det ser ut til at ikke alle interesserte parter reflekteres korrekt i SMS-ordningene.

Nivå 2

På dette nivået er alle beskrivelsene på plass, men det finnes imidlertid bekymringer for at omfanget og skalaen til virksomheten ikke er godt beskrevet. Kartleggingen av juridiske og andre krav som påvirker interesserte parter, er til stede, men det er problemer med den. Det er funnet noen interesserte parter som ikke ble dekket av den opprinnelige SMS-innsendelsen, og det er noe bevis for at alvorlige risikoer til tider ikke er tilstrekkelig kontrollert med følgende implikasjoner for effektiviteten til SMS.

Nivå 3

Nivå 2 pluss at på dette nivået er beskrivelsen av virksomheten, SMS og de alvorlige risikoene som organisasjonen står overfor, i samsvar med det som ses i praksis. Organisasjonen er tydelig klar over hva den gjør og hvilken retning den går i. Det er tydelig oversikt over hvilken lovgivning som gjelder, og hvem de interesserte partene er.

Nivå 4

Nivå 3 pluss at organisasjonen prøver å utvikle seg og lære å presentere seg selv bedre til interesserte parter og få kontakt med dem for å utvikle sikrere prosedyrer og prosesser innenfor sitt SMS. Heller enn å kun liste opp lovgivningen den må overholde, prøver organisasjonen aktivt å engasjere seg med de relevante tilsynsmyndighetene for å utvikle strategier for å oppfylle juridiske krav. Grenser med andre deler av virksomheten forstås og håndteres på en tydelig måte

Nivå 5

Nivå 4 pluss at organisasjonen er en ledestjerne for andre organisasjoner i hvordan den presenterer seg selv. Organisasjonen er tydelig om sin egen karakter og sitt juridiske ansvar, og prøver å utvikle dette ved å bygge på sine sterke sider og utnytte erfaringen ikke bare fra jernbanebransjen, men også utenfor den.

4.2 L — Ledelse

Formål

Å sikre at organisasjonen styres og ledes på en effektiv måte.

Å sikre at sikkerhetsretningslinjene tydelig uttrykker forventingene til toppledelsen, definerer nøyaktig hva organisasjonen ønsker å oppnå, hvordan den vil oppnå det (gjennom atferden vist av ledelsen) og hvordan ledelsen kan vite når forventingene er oppfylt. Effektiv ledelse kan ses som å gi retningen, organisasjonen, ressursene og evnen til å innføre den rette kulturen i virksomheten for å oppnå de ønskede målene. Ledelsen skal styre virksomheten effektivt, slik at sikkerhetsmål ikke kompromitteres av konkurrerende virksomhetsprioriteter. Ledelsen skal gjøre det klart for de ansatte hva sikkerhetsmålene er og hvordan de skal oppfylles.

Å sikre at organisasjonen (spesielt styret) effektivt utfordrer om sikkerhetsretningslinjer og deres tilknyttede aktiviteter er korrekte, på plass og effektive. Å sikre at meldinger er konsekvente, tydelige og utformet for å skape det beste miljøet for sikkerhetsstyring.

Innledende notater

Dårlig ledelse har forårsaket mange høyprofilerte sikkerhetssvikter. En organisasjons tilnærming til sikkerhet reflekterer ofte holdningene til de som tar forretningsbeslutninger, og det leder meningene og holdningene til de ansatte som arbeider i organisasjonen.

De samlede retningslinjene, de tilknyttede prosedyrene og det følgende sikkerhetsklimaet etablert av overordnet ledelse er nødvendige for å angi og opprettholde organisasjonens tilnærming til sikkerhet. Retningslinjene skal gi en tydelig forståelse av hvordan organisasjonen har tenkt å håndtere sikkerhet. Ledelsesteamet og andre ledere skal også gå foran som et eksempel og handle på måter som forsterker meldingene i retningslinjene. Sikkerhetsordninger for jernbaner er integrert i virksomheten.

4.2.1 L1 — Ledelse og forpliktelse

Ledelse og forpliktelse handler om at organisasjonens ledere angir retningen og en positiv og fremtidsrettet agenda for de ansatte som arbeider for dem, for å håndtere risikoer på tvers av forretningsprosesser. Ledelsen angir tonen og kulturen for hvordan organisasjonen oppfører seg både internt og med de som har kontakt med den. Det er de i ledelsesstillinger som har størst påvirkning på organisatorisk kultur, organisasjonens struktur og effektiv drift av organisasjonen, og det er derfor viktig at de kan kommunisere meldingene sine til de som arbeider for dem. Ved vurdering av dette området under kontroll bør NSA-ansatte vurdere, der det er mulig, om det finnes motstridende prioriteter mellom sikkerhetsstyringen og andre forretningsprosesser.

Nivå 1 — Grunnleggende

Prosedyrer og sikkerhetsmålsettinger er utdaterte eller har ikke blitt kommunisert innenfor organisasjonen, og det er lite bevis på forståelse av dem.

Det finnes ikke noe bevis for at ansatte blir konsultert angående sikkerhetsproblemer, og ansatte har ingen forbindelse med ledelsen.

Sikkerhetsstyringssystemet eksisterer på et svært enkelt nivå (for eksempel, selv om menneskelige faktorer vurderes, er systemet som er på plass for å gjøre det, svakt), og det er ikke forbundet med organisasjonens daglige virksomhet.

Det finnes lite bevis for interesse i sikkerhetsproblemer fra ledelseskjeden, produksjon er viktigere. Det er vanskelig å finne ressurser som takler risikohåndteringsproblemer, ettersom organisasjonen ikke ser viktigheten av å bruke dem på denne måten.

Ledelsens forpliktelse til sikkerhetskultur mangler, og det er lite kunnskap i organisasjonen om sikkerhetskulturkonseptet eller hvorfor sikkerhetskultur er viktig for å oppnå en sikker og effektiv organisasjon. Sikkerhet oppfattes som separat fra forretningsmålene til organisasjonen, og defineres i form av samsvar med forskrifter og tekniske eller prosedyremessige løsninger. Sikkerhet administreres og ledes av en selvstendig sikkerhetsavdeling som oppfattes som å være hovedsakelig ansvarlig for organisasjonens sikkerhetskultur. Ledelsens forpliktelse til og kommunikasjon av sikkerhetsmål og -prioriteringer er begrenset i den grad at de er ukjente i organisasjonen. Sikkerhet oppfattes som noe som må gjøres, heller enn noe som er til fordel for organisasjonen. Det er liten ledelse i streben etter en positiv sikkerhetskultur.

Hendelser og ulykker «kommer til å skje» — en fatalistisk kultur dominerer. Menneskelige feil i det problematiske området identifiseres alltid som årsaken uten at det gjøres forsøk på å undersøke videre. Det er ingen rettferdig kultur, og personale som er involvert i hendelser og ulykker, blir ofte gjort til syndebukker. Ledelsen og ansatte er generelt sett uinteressert i sikkerhet, og bruker muligens sikkerhet kun som grunnlaget for andre diskusjoner, for eksempel lønn, arbeidstimer osv.

Ytelsesnivået er under det for minimum juridisk samsvar, og NSA bør derfor vurdere hvordan organisasjonens ytelse kan bringes opp til minimumet som kreves.

Nivå 2 — Mestring

Det er et skille mellom sikkerhetsrelaterte prosesser og forretningsprosesser. Den organisatoriske kulturen varierer mellom de forskjellige funksjonene til organisasjonen.

Ledelsen fremskaffer ressurser, men er ikke nok til å oppfylle forpliktelsen til å gjøre et positivt bidrag til sikkerheten og organisasjonskulturen.

Ledelse anerkjennes som viktig for styringen av sikkerhet, men hvordan dette er reflektert i SMS, ser ut til å være litt inkonsekvent og uklart.

Sikkerhet ses som en forretningsrisiko som kan påvirke organisasjonens økonomiske mål negativt. Sikkerhet defineres fortsatt, som på nivå 1, i form av samsvar med forskrifter og tekniske eller prosedyremessige løsninger. Den generelle tilnærmingen til sikkerhet er reaktiv fra overordnet ledelse til arbeiderne. Ledelsens forpliktelse ses som halvhjertet, at de reagerer når noe har gått galt heller enn å iverksette proaktive tiltak for å forbedre ting.

På dette nivået oppfyller organisasjonen minimumsnivået som du forventer for bevilgningen av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at ansatte aktivt er involvert i å gå gjennom og revidere sikkerhetsretningslinjene og sikkerhetsmålene og hvordan de brukes.

Starten av en utvikling av en positiv organisatorisk kultur kan observeres. Kunnskap og metoder for menneskelige faktorer begynner å vurderes på en systematisk måte i utviklingen av organisasjonens forretningsprosesser.

Sikkerhet ses av ledelsen som viktig, men produksjon blir noen ganger prioritert. Grunnleggende elementer for sikkerhet er på plass og organisasjonen beveger seg mot et proaktivt forebyggingsperspektiv, i stedet for samsvar med regler og forskrifter. Organisasjonen vet at involvering av alt personale er viktig for videre forbedring, og flertallet er villige til å bidra positivt. Flertallet av de ansatte tar personlig ansvar for sin egen sikkerhet. Sikkerhet drives frem av kampanjer og tilsynskontroll, hovedsakelig ovenfra og ned, men med noe involvering av de ansatte.

Sikkerhetsstyringssystemet er konsekvent i kontrollen av de fleste risikoer som organisasjonen utsettes for.

Nivå 4 — Forventet

Nivå 3 pluss at sikkerhetsmål støttes av handlingene til alle som handler i ledelseskjeden.

Det er en realisert forpliktelse til kontinuerlig forbedring av effektiviteten til risikokontroller. Det finnes bevis på omfattende samarbeid gjennom hele ledelseskjeden. Det finnes bevis på at sikkerhetsrisikoer vurderes når man ser på forretningsrisikoer.

Retningslinjer på overordnet nivå:

- *blir gjennomgått og revidert for å drive frem forbedringer på en forutsigbar måte; og*
- *blir tolket på samme måte av alle deler av organisasjonen som bruker dem.*

Organisasjonen ser utover og prøver å forbedre seg, den organisatoriske kulturen er generelt sett positiv, og det er muligheter for ansatte i noen områder til å bidra proaktivt til utviklingen av sikkerhetsstyringssystemet.

Ressurser blir vanligvis gjort tilgjengelige for styringen av sikkerhet, men det er fortsatt noen begrensninger.

Ledelsen forstår at sikkerhet og produktivitet henger sammen, og sikkerhet er førsteprioritet når det er tvil. Ledelsen er forpliktet til sikkerhet og tildeler betydelige ressurser til proaktive sikkerhetstiltak, for eksempel risikovurderinger, hendelses- og ulykkesundersøkelser og endringshåndteringsprosesser. Viktigheten av sikkerhet anerkjennes gjennom hele organisasjonen, og de ansatte er positivt engasjert i sikkerhetsinitiativer. Sikkerhetsytelse er fokusert på både ledelende og hemmende indikatorer som bruker alle tilgjengelige data.

Nivå 5 — Utmerket

Nivå 4 pluss at sikkerhetsretningslinjer inkluderer selskapets sikkerhetsmålsettinger, som spres i organisasjonen. Det finnes prosedyrer for å tildele tilstrekkelige menneskelige, økonomiske og tekniske ressurser for å støtte oppnåelsen av disse målsettingene, og ledelsen overvåker implementeringen av de nødvendige sikkerhetskravene. Effektiviteten til sikkerhetsretningslinjene evalueres, og resultatene tas med i betraktningen i den neste revideringen. Sikkerhetsmål brukes til å utfordre organisasjonen til å oppnå forretningsytelse og styre forretningsrisikoer som er i tråd med den beste ytelsen til de organisasjonene som yter best innenfor og utenfor jernbanesektoren.

Det anerkjennes at styring av sikkerhetsrisikoer ikke er en separat funksjon, men en nødvendig del av en produktiv, konkurransedyktig og lønnsom organisasjon.

Sikkerhetsrisikoer anerkjennes som en risiko for hele forretningsytelsen, og sikkerhetsstyringssystemet er effektiv når det kommer til å kontrollere eksisterende risikoer og forutse nye.

Sikker produksjon er høyeste prioritet, og sikkerhet er forbundet med forretningsytelse. Ledelsens forpliktelse til sikkerhet er høy, og organisasjonen gjør alt den kan for å finne sterkere og mer bærekraftige løsninger på sikkerhetsproblemer. Lærdom tas i bruk daglig. Ansatte forstår og støtter sikkerhetsinitiativer, og at sikkerhet er en livsstil. Organisasjonen fremmer sikkerhet på jobb og hjemme, og tildeler passende ressurser til å gjøre det.

4.2.2 L2 — Sikkerhetsretningslinjer

Effektive sikkerhetsretningslinjer angir en tydelig retning som organisasjonen skal følge. De bidrar til alle aspekter av en virksomhets ytelse som del av en forpliktelse til kontinuerlig forbedring. Sikkerhetsretningslinjene er et viktig dokument for å vise hvordan organisasjonen håndterer sitt sikkerhetsansvar, og sin ledelse og forpliktelse til korrekt sikkerhetsstyring.

Nivå 1 — Grunnleggende

Retningslinjeerklæringen er utdatert eller har ikke blitt kommunisert innenfor organisasjonen.

Det finnes ikke noe bevis for at ansatte blir konsultert.

Det er liten anerkjennelse av rollen som personen spiller i leveringen av et sikkert og effektivt driftsnivå.

Organisasjonen overholder de forskriftsmessige minimumsstandardene.

Dette nivået av ytelse er under minimumsstandarden som bør forventes.

Nivå 2 — Mestring

Sikkerhetsretningslinjene er oppdatert og kommunisert innenfor organisasjonen, men lokale ledere og tilsynsførere har motsigende tilnærminger eller tolkninger. Dette resulterer i at retningslinjene brukes på forskjellige måter på tvers av organisasjonen.

Retningslinjene ses ikke som vesentlige for å opprettholde sikkerhet.

Det er noe anerkjennelse av verdien som forbedring av den menneskelige rollen kan bringe til virksomheten, men dette er inkonsekvent.

Ytelsesnivået oppfyller minimumsnivået av krav for å få bevilget et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at sikkerhetsretningslinjene og andre tilknyttede retningslinjer brukes som et fokus for ledere, noe som resulterer i at de blir tolket på samme måte av alle ansatte.

Ansatte er aktivt er involvert i å gå gjennom og revidere sikkerhetsretningslinjene hvordan de brukes.

Det er et tydelig fokus på problemer av menneskelige faktorer innenfor organisasjonen og en anerkjennelse av den viktige rollen som mennesker spiller i leveringen av en sikker og effektiv organisasjon og leveringen av forretningsmålsettinger.

Nivå 4 — Forventet

Sikkerhetsretningslinjene er konsekvente med handlingene til alle som handler i ledelseskjeden.

Sikkerhetsretningslinjene inkluderer en realisert forpliktelse til kontinuerlig forbedring av effektiviteten til risikokontroller. Det finnes bevis på omfattende samarbeid gjennom hele ledelseskjeden, som anerkjenner verdien til menneskene ved levering av forbedret ytelse.

Kapasiteten til menneskelige faktorer er målt, skreddersydd og proporsjonal til modenheten og kompleksiteten til organisasjonen, og er fokusert på forbedring over tid.

Sikkerhetsretningslinjene og eventuelle tilknyttede retningslinjer:

- *er konsekvente med hverandre;*
- *blir gjennomgått og revidert for å drive frem forbedringer på en forutsigbar måte; og*
- *blir tolket på samme måte av alle deler av organisasjonen som bruker dem.*

Nivå 5 — Utmerket

Sikkerhetsretningslinjene brukes til å utfordre organisasjonen til å oppnå forretningsytelse som er i tråd med ytelsen til de organisasjonene som yter best.

Sikkerhetsretningslinjene anerkjenner at styring av sikkerhetsrisikoer ikke er en separat funksjon, men en nødvendig del av en produktiv, konkurransedyktig og lønnsom organisasjon.

Sikkerhetsrisikoer anerkjennes som en risiko for forretningsytelsen.

Den menneskelige rollen anerkjennes som å være nødvendig for suksessen til organisasjonen, og vurderes ved hver gjennomgang av drifts- og forretningsutvikling.

Organisasjonen ser utover og ser etter eksterne muligheter til å utvikle dens effektivitet, og vurderer menneskelige faktorer når den gjør det.

4.2.3 L3 — Organisatoriske roller, ansvar og myndigheter

Formålet med dette kravet er at organisasjonen som kontrolleres, skal demonstrere at organisasjonen er strukturert og hvordan ansvaret er fordelt for å oppfylle organisasjonens selskapsmål og sikkerhetsretningslinjer. Det kan være lag av arbeid som støtter dette fra retningslinjeperspektiver og strategiske perspektiver.

Risikokontroller skal passe praktisk inn i ledelsesstrukturer, slik at det er tydelig hvor ansvaret ligger. De skal også anerkjenne og håndtere risikoer som kontakt med entreprenører, partnere og leverandører utgjør, på en effektiv måte.

Disse elementene er viktige for å forstå hvor bra organisasjonens sikkerhetsstyringssystem kontrollerer risiko. Søkeren skal demonstrere hvordan de tilordner kompetente ansatte til aktiviteter, hvordan de sikrer at de ansatte har en tydelig forståelse av rollene og ansvaret sitt, og hvordan personer holdes ansvarlig for ytelsen sin. At den organisatoriske strukturen og enkeltpersoners roller og ansvar finner en balanse mellom samsvar og en sikkerhetskultur — en tenkende kultur heller enn at sikkerhet kun drives frem av samsvar for samsvars skyld.

Nivå 1 — Grunnleggende

Organisasjonens ledelsesstrukturer har ingen sammenheng med sikkerhetsmålsettingene, slik at ansattes ansvar ofte blandes sammen.

Der delegering av ansvar oppstår, blir ikke de ansatte gitt autoritet eller ressurser til å utføre det. Noen ansatte som er gitt ansvar, er muligens ikke klar over det eller har ikke den nødvendige kompetansen til å utføre det. Jobbeskrivelser reflekterer ikke nøyaktig måten personer faktisk utfører rollene og ansvaret på.

Tilordningen av roller og ansvar på tvers av organisasjonen er vilkårlig og ikke forbundet med organisasjonens driftsmål.

Ytelsesnivået er under det som bør forventes fra en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Det finnes en beskrivelse av strukturen til organisasjonen, inkludert tilordning av roller og ansvar innenfor sikkerhetsstyringssystemet. Planer er på plass for å identifisere hvordan arbeid faktisk gjøres innenfor organisasjonen.

Organisasjonens struktur betyr at de fleste risikoer håndteres av personene eller teamene som utfører arbeidet, men noen risikoer er delt slik at det er, eller kan være, konflikt mellom sikkerhet og andre målsettinger.

Det ser ut til å være lite overensstemmelse mellom aktivitetene til individuelle forretningsenheter eller med bredere mål for organisasjonens forretningsmålsettinger.

Det ser ut til å være lite overensstemmelse i de organisatoriske strukturene, tilordningen av ansvar og den tilknyttede kulturen som er nødvendig for å levere dem effektivt.

Organisasjonen oppfyller minimumsnivået av samsvar for å få bevilget et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at den organisatoriske strukturen på tvers av forskjellige elementer er konsekvent med ansvaret som tydelig er tilordnet på tvers av forretningsenheter.

Samlede retningslinjer og prosedyrer som dekker roller og ansvar, er konsekvente med de til de relevante forretningsenhetene.

Det finnes kriterier for å delegere og tilordne ansvar og oppgaver der nødvendig kompetanse og ferdigheter er identifisert. Disse kriteriene brukes og derfor er sikkerhetsoppgaver tydelig tilordnet, og de ansatte som utfører dem, har passende kompetanse, autoritet og ressurser til å levere dem.

Der delegering av ansvar utføres, er det en systematisk tilnærming til hvordan det gjøres. De ansatte er kompetente og gis tilstrekkelige ressurser og autoriteten til å utføre dem.

Der nye eller endrede roller og ansvar blir vurdert, er det en analyse av saker med menneskelige faktorer i forhold til endringen og måten pliktene faktisk utføres på innenfor organisasjonen.

Nivå 4 — Forventet

Som for nivå 3 nedenfor, men med tydelige koblinger mellom elementene til den organisatoriske strukturen fra toppen til bunnen av organisasjonen, ikke bare på arbeidsnivåer.

Samlede retningslinjer og prosedyrer er utformet for å komplettere hverandre på tvers av forretningsenhetene for å fremme de strategiske målsettingene til organisasjonen.

Ansatte med sikkerhetsansvar holdes ansvarlig for ytelsen sin på en rettferdig og konsekvent måte. Organisasjonens kultur gjør det mulig for ansatte med sikkerhetsansvar å påvirke hvordan oppgavene utføres og forbedringer gjøres.

Som et resultat av å forstå hvordan arbeidet faktisk utføres, er det en innretting av individuell og felles innsats for driftsytelsesmål.

Nivå 5 — Utmerket

Som for nivå 4 pluss effektive gjennomganger av organisasjonsstrukturens roller og ansvar, på alle nivåer, mot oppnåelsen av strategiske målsettinger og forretningsmålsettinger.

En formell gjennomgangsprosess er på plass for å sikre at roller og ansvar forblir gyldige, oppdaterte og integrerte med organisasjonen, strategien og miljøet som er i endring. Organisasjonen vurderer konsekvent mennesket i systemet som en standard del av gjennomgangsprosessen.

4.2.4 L4 — Konsultasjon med ansatte og andre parter

Suksessfulle organisasjoner vil aktivt involvere de ansatte for å oppmuntre dem til å bruke sin kunnskap og erfaring og bygge forpliktelse til å oppnå delte målsettinger. Slike organisasjoner vil aktivt støtte og oppmuntre involvering og konsultasjon på forskjellige måter.

Undersøkelse av dette aspektet vil også gi en indikasjon til tilsynsmyndigheten om hva sikkerhetskulturen er innenfor organisasjonen, og hvor aktivt de involverer relevante tredjeparter i styringen av sikkerhet i områder der risikoen er delt.

Nivå 1 — Grunnleggende

Det er lite eller ingen konsultasjon.

Ansatte forstår ikke hvordan de bidrar til sin egen sikkerhet og sikkerheten til personene de arbeider med.

Organisasjonen oppfyller ikke standarden som forventes for minimum juridisk samsvar.

Nivå 2 — Mestring

Ansatte forstår at de er ansvarlig for sin egen sikkerhet og sikkerheten til kolleger, men dette er ikke konsekvent på tvers av organisasjonen.

Det er noe konsultasjon angående helse- og sikkerhetssaker, men den ser ikke ut til å utføres på en systematisk måte og den involverer heller ikke alle ansatte.

Organisasjonen oppfyller den juridiske minimumsstandarden som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at organisasjonen har prosedyrer for å sikre at ansatte konsulteres angående sikkerhetssaker.

Ansatte forstår hvordan de bidrar til sin egen sikkerhet og sikkerheten til jernbanen, og de får tilbakemelding på bidraget sitt.

Personer i lignende roller bruker standarder på samme måte.

Nivå 4 — Forventet

Organisasjonen har retningslinjer for å prøve å involvere ansatte på alle nivåer i organisasjonen, og det er en tydelig struktur som disse retningslinjene kan kommuniseres gjennom. Arbeidere og ansatte konsulteres når avgjørelser om risikokontrolltiltak tas.

Organisasjonen konsulterer regelmessig de ansatte på en rekke måter, for eksempel gjennom spørreundersøkelser, seminarer, møter med ledere og sikkerhetsturer.

Ansatte er motiverte til å levere forretningsmålsettinger og demonstrerer en konsekvent forståelse av hvordan dette oppnås.

Ansatte føler seg i stand til å ta avgjørelser innenfor et målsettingsrammeverk.

Personer i lignende roller bruker standarder konsekvent.

Ansatte forstår behovet for endring og bekrefter at de konsulteres angående hvordan endringene introduseres.

Nivå 5 — Utmerket

Organisasjonen utnytter potensialet til sine ansatte og andre interesserte parter fullt ut, og involverer dem aktivt i utviklingen av delte verdier og en kultur av tillit, åpenhet og egenmakt.

Organisasjonen bruker involveringen av ansatte til å samle inn ideer for forbedring og ta dem i bruk.

Ansatte viser at de forstår hvordan de bidrar til å oppnå organisasjonens mål. Den forståelsen er konsekvent med organisasjonens relevante retningslinjer og visjonen til ledelsesteamet.

Ansatte viser en forpliktelse til å overgå de målene ved å følge eksisterende prosesser, og indikerer hvor de kan forbedres.

4.3 PL — Planlegging

Formål

Å sikre at organisasjonen kan definere og implementere risikokontroller som gjør det mulig for forretningen å drive virksomhet på en sikker måte. At den planlegger driften sikkert og med behørig hensyn til velferden til sine egne ansatte og andre som påvirkes av aktivitetene.

Innledende notater

God planlegging er utgangspunktet for håndteringen av risiko. Organisasjonen skal ha korrekte prosedyrer på plass for å gjøre det mulig for organisasjonen å oppfylle sine juridiske plikter, og til å prestere som en virksomhet som oppfyller sine målsettinger effektivt. God planlegging vil betydelig forbedre måten en organisasjon håndterer sikkerhet på, ved å sikre at den har de rette ressursene, inkludert kompetente ansatte som utfører oppgavene. Dette vil føre til effektiv risikokontroll og effektivt arbeid.

4.3.1 PL 1 — Risikovurdering / planlegge for endring

Dette elementet går til kjernen av SMS, det er rettet mot å få søkeren til å vise hvordan deres systemer identifiserer og kontrollerer risikoene de står overfor. Kontroll skal brukes til å få søkeren til å vise hvordan de bruker resultatene av risikovurderingen i praksis til å forbedre risikokontroll, og hvordan de sjekker dette over tid. Det er viktig å huske at dette elementet ikke takler håndtering av risikoene fra endringer direkte (det er et annet element), men er relatert til det. Det bør også merkes at det er et spesifikt krav om at risikovurdering skal ta fatt i problemer relatert til menneskelig ytelse, for eksempel håndtering av jobbdesign og tretthetsrisiko. Fra et kontrollperspektiv skal derfor bevis letes etter for å bevise at disse problemene er håndtert innenfor risikovurderingsprosessen.

Systemet tilknyttet planlegging av risikokontroller og å sette dem på plass, bør koordineres for å sikre at de overholder relevante lover og lar organisasjonen oppfylle sine målsettinger effektivt.

Nivå 1 — Grunnleggende

Selskapet har en prosess for vurdering av risikoer, men den blir ikke brukt og oppdatert konsekvent, med det resultat at gamle driftsregler eller -praksiser brukes til å kontrollere risikoer når risikoen er endret.

Risikovurderinger blir ikke fullført eller gjennomgått for alle relevante aktiviteter til virksomheten.

Risikovurderinger er upassende for deres tiltenkte bruk. Det er en tydelig misforståelse av formålet med risikovurderinger og hvordan de skal utføres.

Risikokontrollene brukes på en dårlig måte, og lite overvåking utføres på effektiviteten til kontrollene som er på plass.

Risikoene som oppstår fra problemer med menneskelige faktorer, vurderes ikke i løpet av risikovurderingen. Det er ikke noe oppfattet forretningsbehov for å håndtere slike problemer.

Organisasjonen yter på et nivå som er under det som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Det finnes lite bevis innenfor risikovurderingsprosessen på at sikkerhetsrisikoer vurderes på tilstrekkelig måte ved håndtering av endring.

Nivå 2 — Mestring

Risikovurderinger er utført, men samlet koordinering er en bekymring.

Kontrolltiltak innenfor en aktivitet inkluderer ikke alltid tiltakene identifisert av risikovurderingen.

Risikovurdering brukes ofte kun for å demonstrere at risikokontrollene som allerede er på plass, er tilstrekkelige.

Risikovurderinger brukes kun til å identifisere hvor risikokontroller behøves, men organisasjonen har ikke tilstrekkelige kontroller på plass.

Opplæring i risikovurdering har blitt gitt til alle ansatte som trenger det, på det passende nivået som kreves for forskjellige ansvarsnivåer.

Det finnes bevis på bruken av risikokontroller og overvåkingen av dem.

Det anerkjennes at problemer med menneskelige faktorer skal vurderes i løpet av risikovurderingen, men måten dette gjennomføres på, er en bekymring. Som en konsekvens kontrolleres ikke slike problemer så godt som de burde gjennom SMS.

Det finnes bevis på at sikkerhetsrisikoer vurderes innenfor endringshåndteringsprosessen.

Organisasjonen yter ved minimumsnivået for samsvar for en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at organisasjonen har tydelige retningslinjer for bruk av risikovurderinger og hvilke risikoer som vil bli tolerert og hvorfor dette er akseptabelt.

Risikohåndtering brukes på en konsekvent måte i forskjellige deler av organisasjonen, inkludert innenfor endringshåndteringsprosessen. Ledere forstår rollen sin i prosessen.

Det er effektiv bruk av risikokontrollene og fjerning av risiko ved kilden.

Koordinering av vurderinger er konsekvent, og de gjennomgås regelmessig.

Risikoer og tilknyttede kontrolltiltak kommuniseres tydelig til ansatte.

Risikovurderingsprosedyrer danner en del av endringshåndteringsprosessen.

Det er et enkelt system på plass for kontroll av effektiviteten til risikokontroller introdusert som et resultat av risikovurderinger, på en jevnlig basis.

Det er konsekvente prosesser på plass for å identifisere risikoene tilknyttet menneskelige faktorer under risikovurderingsprosessen. Der det er nødvendig, kan virksomheten benytte spesialistekspertise til å muliggjøre dette.

Nivå 4 — Forventet

Nivå 3 pluss at risikovurderinger er bygget inn i andre aspekter av virksomheten for å sikre at det er en systematisk tilnærming til risikokontroll.

Alle nivåer av arbeidsstyrken, og eksterne organisasjoner, kan bidra til risikovurderinger.

Risikovurderinger, inkludert fjerning av risiko ved kilden, er en del av endringsprosessen og organisasjonskulturen.

Gjennomganger danner en del av prosessen for risikovurdering.

Prinsipper for risikohåndtering brukes intelligent på alle nivåer.

Det er et mer komplekst system på plass for kontroll av effektiviteten til risikokontroller som introduseres som et resultat av risikovurderinger, på en jevnlig basis.

Problemer med menneskelig faktorer er fullt integrert i SMS-prosesser for risikovurdering og endringshåndtering. De som er ansvarlige for å utføre risikovurderinger, får tilbakemelding på ytelsen sin.

Nivå 5 — Utmerket

Nivå 4 pluss at risikovurderingen brukes til å drive frem kontinuerlig forbedring i organisasjonens risikoprofil.

Tilnærmingen til risikohåndtering er innført og brukt konsekvent gjennom hele organisasjonen. Risikoer vurderes grundig, og de vurderes i god tid før endringer finner sted.

Fjerning av risiko ved kilden er en del av en konsekvent tilnærming og reflekteres i organisasjonens retningslinjer.

Det er proaktive prosedyrer på plass for utvikling av risikokontrolltiltak sammen med andre enheter med ansvar for risikokontroll der det er tverrgående problemer.

Informasjon om menneskelige faktorer fra risikovurdering brukes i hele virksomheten til å drive frem kontinuerlig sikkerhetsforbedring. Resultatene av vurderingene deles, der relevant, med entreprenører, partnere og leverandører som en del av målet med å utvikle effektiviteten til organisasjonens virksomhet.

4.3.2 PL 2 — Sikkerhetsmålsettinger og planlegging

For å sikre at organisasjonen oppfyller juridiske krav og sikrer kontinuerlig forbedring innen sikkerhet, at det kommuniseres til de ansatte og tros på av ledelsen, er det nødvendig å ha sikkerhetsmålsettinger som oppfyller SMART-kravene (se nedenfor).

Organisasjonen må demonstrere at den har fornuftige målsettinger og en prosess for å implementere og overvåke oppnåelse av dem i løpet av levetiden deres. Sikkerhetsmålsettinger må være «spesifikke, målbare, oppnåelige, realistiske og tidfestede» (SMART). Både kortsiktige og langsiktige målsettinger bør angis og prioriteres sammen med brede forretningsmålsettinger. Motstridende prioriteter skal håndteres slik at sikkerhetsmålsettinger ikke lider i forhold til andre forretningsbehov. Målsettinger angitt på forskjellige nivåer eller for forskjellige deler av en organisasjon, skal innrettes slik at de støtter de generelle målsettingene til organisasjonens retningslinjer. Personlige mål kan også avtales med enkeltpersoner for å sikre at målsettinger oppfylles.

Nivå 1 — Grunnleggende

Det er få eller ingen sikkerhetsmålsettinger

Eventuelle sikkerhetsmålsettinger som finnes, er ikke SMART eller prioriterte.

Hvis sikkerhetsmålsettinger ikke oppfylles, tolereres det og ingen tiltak iverksettes for å håndtere manglene som gjorde at de ikke ble oppfylt.

Personlige mål er ikke relatert til målsettingene til organisasjonens samlede retningslinjer.

Organisasjonen yter på et nivå som er under det som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Det finnes sikkerhetsmålsettinger. Noen kan være SMART og prioriterte, men målsettinger i forskjellige deler av organisasjonen er ikke tydelig innrettet og kan være i konflikt med hverandre, og som en konsekvens støtter de ikke alltid de samlede målsettingene til organisasjonens retningslinjer.

Personlige mål er hovedsakelig innrettet med målsettingene til organisasjonens samlede retningslinjer.

Det er kontroller på fremgang med oppnåelsen av sikkerhetsmålsettinger.

Organisasjonen oppfyller minimumsstandarden som forventes for juridisk samsvar.

Nivå 3 — Konsekvent

Nivå 2 pluss at sikkerhetsmålsettinger angis og en sikkerhetsplan finnes som illustrerer hvordan organisasjonen vil oppnå målsettingene sine.

Sikkerhetsmålsettingene som er angitt, tar hensyn til gjeldende juridiske og andre krav.

Forsøk gjøres for å angi SMART-målsettinger og for å prioritere målsettinger og mål og bringe dem på linje med hverandre.

Systemer er på plass for å følge opp oppnåelse av målsettinger.

Oppnåelse av målsettinger er ikke godt innrettet med gjennomgangsprosessen, dvs. gjennomganger tar ikke hensyn til de angitte målsettingene.

De ansatte er klar over relevansen og viktigheten til aktivitetene sine, og hvordan de bidrar til oppnåelsen av sikkerhetsmålsettinger og planlegging for å håndtere sikkerhetsrisikoer.

Nivå 4 — Forventet

Nivå 3 pluss at målsettingene er SMART, prioriterte og på linje med hverandre for å støtte de samlede retningslinjene.

Sikkerhetsstyringssystemet sikrer at sikkerhetsmålsettinger er angitt og oppnåelse målt.

Oppnåelse eller ikke-oppnåelse registreres og brukes til å hjelpe med kontinuerlig forbedring.

Systemer er på plass for å følge opp potensiell og faktisk ikke-oppnåelse av sikkerhetsmålsettinger.

Nivå 5 — Utmerket

Nivå 4 pluss at organisasjonen sammenligner ytelsen mot andres ytelse, innenfor og utenfor jernbanebransjen, for å sikre at målsettingene representerer utmerkethet.

4.4 S — Støtte

Formål

Formålet med dette kravet er å sikre at organisasjonen vier nok ressurser, inkludert kompetente ansatte, for å gjøre det mulig for dens SMS å kontrollere risiko i henhold til målsettingene.

Å angi roller og ansvar for å oppfylle organisasjonens sikkerhetsmålsettinger.

å sikre at viktig informasjon er tilgjengelig for de som tar avgjørelser.

Å sikre at organisasjonens ordninger og handlinger fremmer en kultur som gjør utmerkethet i risikokontroll mulig.

Innledende notater

Dokumentasjonen for sikkerhetsstyringssystemet må kontrolleres strengt, håndteres og gjennomgås jevnlig slik at kun den nyeste versjonen av et bestemt dokument som kreves for sikkerhetskontroll, er i omløp. Alle endringer i dokumentasjonen som er resultat av prosessen for kontinuerlig forbedring i risikokontroll, må implementeres i rett tid.

Det er viktig at sikkerhetsstyringssystemet inkluderer et omfattende og implementert kompetansestyringssystem, og at riktige kommunikasjonsordninger er på plass, både fra ledelsen til ansatte og motsatt, og til andre som er avhengig av kommunikasjon fra organisasjonen for å håndtere sikkerheten til sine egne organisasjoner. Dette er fordi disse elementene støtter effektiviteten til SMS. Det å ha kompetente personer på plass for å utføre oppgavene som kreves av dem, minimerer mulighetene for at feil vurdering tas, noe som støtter funksjonene til SMS. Samtidig vil det å sikre at kommunikasjonssystemet både ovenfra og ned og nedenfra og opp gjennom organisasjonen fungerer, sikre at viktige meldinger høres i tide av de rette personene.

4.4.1 S1 — Ressurser

Effektiv bruk av ressurser er et viktig element i ethvert sikkerhetsstyringssystem. Det er ikke nok å ha prosesser på plass, de må også fungere, og dette vil kreve anskaffelse av nok ressurser til å la dette skje effektivt.

Nivå 1 — Grunnleggende

Organisasjonen skaffer ressurser for å gjøre det mulig for sikkerhetsstyringssystemet å fungere, men dette gjøres ikke på en systematisk måte. Det ser heller ut til å være en stykkevis tilnærming. Resultatet er at spredningen av ressurser på tvers av organisasjonen, er ujevn, og noen deler har nok ressurser og noen har for få.

Organisasjonen har falt under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

På dette nivået er organisasjonen bedre i stand til å styre ressurser for å muliggjøre fullføringen av oppgaver. Tilordningen av ressurser anses som et viktig element for sikkerhetsstyringssystemet. Ledelsen av organisasjonen gjennomgår ressurser jevnlig.

Organisasjonen yter på det grunnleggende nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at på dette nivået kan organisasjonen demonstrere at det er nok ressurser, og at tilordningen av disse er konsekvent på tvers av alle delene i virksomheten. Fraværet av visse ansatte er ikke et betydelig

problem ettersom dette håndteres innenfor SMS-prosessene. Organisasjonen begynner å tenke på hvordan den kan bruke ressurser mer effektivt.

Nivå 4 — Forventet

Som for nivå 3, men her forutser organisasjonen fremtidige behov for organisasjonen, slik at den er forberedt på forhånd på kommende endringer og har ressursene på plass for å håndtere dette.

Nivå 5 — Utmerket

Nivå 4 pluss at her håndterer organisasjonen ressurser på en svært proaktiv måte og bruker dem fleksibelt på tvers av organisasjonen i streben etter større sikkerhet og effektivitet.

4.4.2 S2 — Kompetanse

Det er viktig for ledelsen av ansatte med sikkerhetsansvar over tid at en organisasjon har et kompetansestyringssystem, som danner et element i sikkerhetsstyringssystemet. Det er gjennom denne mekanismen at ferdighetene til ansatte evalueres, utvikles, opprettholdes og overvåkes, slik at sikkerhet ikke blir kompromittert.

Organisasjoner trenger et effektivt system for håndtering av kompetanse, for å bidra til å sikre at de ansatte har passende kompetanse. En viktig del av enhver kompetansestyringsprosess (CMS) er opprettholdelse av kompetanse. Dette involverer et omfattende program for kontinuerlig faglig utvikling (CPD) der mer erfarne ansatte kan lære om nye sikkerhetsutviklinger og sikre at de overholder dem.

Hvordan kompetansestyringssystemet driftes, kan avsløre mye informasjon om sikkerhetskulturen til en organisasjon. Et godt gjennomtenkt kompetansestyringssystem vil inkludere ansatte som faktisk utfører arbeidet, slik at de som best forstår oppgaven kommer med innspill til designen av CMS, noe som hjelper både enkeltpersonene og organisasjonen å yte bedre. Et fungerende CMS er en viktig indikatorer på en organisasjons sikkerhetskultur.

Nivå 1 — Grunnleggende

Kompetansestyringssystemet er dokumentert, men ikke tydelig implementert. Det er ikke koblet til designen av arbeidsoppgaver. Det er en uklar tilnærming til hvordan kompetansen til ansatte skal håndteres.

Ansatte kan være kompetente eller ikke, men det er ingen konsekvent prosess for å identifisere dette.

Opplæringsbehov håndteres vilkårlig med prioritering av umiddelbare behov over langsiktig utvikling.

Organisasjonen yter på et nivå som er under det som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Opplæring finner sted på individuelle forretningsenheter stort sett «på jobben», innenfor et kompetansestyringssystem. Minimumsnivået for samsvar med juridiske krav for rekruttering, utvelging og opplæring finnes. En utvelgingsprosess for sikkerhetskritiske roller er på plass.

Retningslinjer for rekruttering, utvelging og opplæring er ikke en del av et logisk system og er ikke koblet til de strategiske målsettingene til organisasjonen, og gjør ikke stort mer enn å tilfredsstille juridiske krav.

Det er noe identifikasjon av opplæringsbehov, men opplæringstilordning er ofte tilfeldig og diktert av tilgjengeligheten til både opplæringen og det relevante personalet heller enn som en del av en strukturert tilnærming.

Organisasjonen oppfyller minimumsnivået for samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at organisasjonen har et effektivt dokumentert kompetansestyringssystem på plass. Dette dekker kompetansene som kreves for å oppfylle organisasjonens strategiske målsettinger og for å håndtere risikoer. Organisasjonen er i stand til å fullt ut utnytte de ansattes kompetanser der den vet disse.

Organisasjonen kan organisere og utvikle opplæringsprogrammer for de ansatte som utfører sikkerhetskritiske plikter, noe som sikrer at relevante behov oppfylles og at kompetansen til ansatte opprettholdes.

Tilbake til arbeid-ordninger finnes for ansatte etter ulykker/hendelser eller langvarige fravær fra arbeid, inkludert identifisering av behov for ytterligere opplæring der dette kreves.

Rekrutterings- og utvelgingsprosesser er omfattende (f.eks. psykometriske og oppgavebaserte) og er stort sett konsekvente, og de velger generelt sett passende personer for de ulike rollene som kreves.

Opplæringssystemet leveres av kompetente personen til et definert program basert på behovene til en bestemt rolle. Opplæring inkluderer respons til normale og degraderte driftsmoduser.

Det er forståelse av behovet for å koble kompetansestyringssystemet til designen av oppgaven.

Nivå 4 — Forventet

Nivå 3 pluss retningslinjer om rekruttering, utvelging og opplæring har tydelige koblinger med de strategiske målsettingene til organisasjonen som spres ned til individuelle målsettinger for ansatte. De er basert på en nøyaktig vurdering av oppgaver (oppgaveanalyse), som mater et tydelig og logisk kompetansestyringssystem. Mentoring brukes og endringer av roller er godt gjennomtenkt.

Opplæringssystemet er omfattende og koblet til de påkrevde kompetansene som trengs for å fungere effektivt i bestemte roller.

Rekrutteringsprosesser er omfattende og fokusert på det optimale ferdighetssettet for en bestemt rolle. De støttes av en periodisk gjennomgang (samt gjennomgangen når personale forlater organisasjonen), for å sikre at de korrekte personene rekrutteres etter hvert som organisasjonen endrer og utvikler seg.

Nivå 5 — Utmerket

Nivå 4 pluss at organisasjonen forstår kompetansene til de ansatte og utnytter fullt ut de ansattes potensial. Organisasjonen involverer de aktivt gjennom delte verdier og en kultur av tillit, åpenhet og egenmakt.

Organisasjonen bruker involveringen av ansatte til å samle inn ideer for forbedring og ta dem i bruk. Planlegging av menneskelige ressurser utføres for å sikre forretningskontinuitet.

Det er en visjon som ser fremover og utover, som har til hensikt å sikre at de korrekte personene rekrutteres og gis passende opplæring og utvikling for å sikre at ferdighetssettene opprettholdes på et nivå som gjør det mulig for organisasjonen å vokse og utvikle seg, samtidig som sikkerhetsytelse opprettholdes og forbedres.

4.4.3 S3 — Bevissthet

Bevissthet betyr å gjøre de ansatte klar over sikkerhetsretningslinjene til organisasjonen og hvordan de bidrar til sikkerhet innenfor organisasjonen, farene og risikoene som de må være klar over, og resultatene av undersøkelser av ulykker og hendelser. Det dekker også å gjøre ansatte klar over implikasjonene av å ikke bidra mot implementeringen av sikkerhetsstyringssystemet, både fra deres synspunkt og organisasjonens synspunkt. Dette elementet gir derfor viktig informasjon om sikkerhetskulturen til organisasjonen.

Nivå 1 — Grunnleggende

Her har organisasjonen gjort sikkerhetsretningslinjene tilgjengelige for ansatte, og gir de ansatte litt grunnleggende informasjon om risikoer og farer. Resultatene av hendelsesundersøkelse kommuniseres ikke systematisk til alle ansatte, og det er ikke noe koordinert forsøk på å bekrefte at ansatte forstår hva ansvaret deres og ansvaret til organisasjonen er.

Organisasjonens ytelse er under det som forventes for juridisk samsvar.

Nivå 2 — Mestring

På dette nivået gis mer informasjon til de ansatte, men det ser ut til at den ikke er i et konsekvent format, og meldingene som gis, er ikke tydelige på tvers av organisasjonen. Organisasjonen forsøker å sikre at de ansatte forstår rollen sin i utviklingen av sikkerhet innenfor sikkerhetsstyringssystemet.

Organisasjonens ytelse oppfyller minimumsnivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at prosessen for kommunikasjon av sikkerhetsretningslinjene til ansatte og kommunikasjonen til ansatte om rollene deres, er konsekvent, og meldingene forstås av de ansatte. Noe overvåking utføres for å sikre at de ansatte har tatt til seg informasjonen, og at de forstår viktigheten til rollen deres i å sikre at SMS fungerer effektivt.

Nivå 4 — Forventet

Som for nivå 3 pluss at organisasjonen proaktivt prøver å fremme bevissthet om organisasjonens roller og ansvar og de ansattes roller og ansvar. Organisasjonen prøver aktivt å fremme fordelene ved forbedret sikkerhetsytelse til de ansatte.

Nivå 5 — Utmerket

Som for nivå 4 pluss at organisasjonen prøver å forbedre bevissthet ikke bare blant sine egne ansatte om organisasjonen og ansvaret deres, men prøver også å kommunisere dette til sine entreprenører, leverandører og andre som den har kontakt med.

4.4.4 S4 — Informasjon og kommunikasjon

Samsvar med dette elementet er utformet for å vise at søkeren har demonstrert i søknaden sin at de har på plass egnede metoder for å identifisere sikkerhetsrelatert informasjon på forskjellige nivåer, og for å kommunisere den i rett tid og til de rette personene. At de analyserer fremtiden for å sikre at gjeldende risikokontroller forblir relevante og oppdaterte og kan identifisere nye trusler og muligheter fra eksterne påvirkninger (politiske, sosiale, miljømessige, teknologiske, økonomiske og juridiske). At de er i stand til å sikre at informasjonen når de korrekte ansatte (spesielt sikkerhetskritiske ansatte) innenfor organisasjonen som må reagere på den. Dette vil inkludere hvordan de leverer relevant sikkerhetsrelatert informasjon til andre interesserte parter som de har kontakt med.

Ordningene skal sikre at alle ansatte som tar avgjørelser eller utfører en oppgave, har riktig informasjon, i form av:

- bedriftsmeldinger om viktigheten til sikkerhet;
- prosedyrer for utveksling av informasjon med de relevante interessentene;
- prosedyrer og standarder relatert til sikkerhet;
- saklige data og intelligens; og

- instruksjoner og rapporter.

Nivå 1 — Grunnleggende

Det er lite forsøk på å kommunisere passende sikkerhetsinformasjon. Hvis prosedyrer er på plass, tar ansatte avgjørelser basert på egen vurdering.

Lite informasjon om sikkerhet samles inn eller deles.

Ledere snakker ikke med ansatte som ikke er i ledelsen, eller gjør det på en ineffektiv måte.

Deling av informasjon og kommunikasjon innenfor organisasjon er vilkårlig og kan ikke spores.

Det er liten anerkjennelse av den viktige rollen som effektiv kommunikasjon spiller når det kommer til påvirkningen av menneskelig atferd og følgelig sikkerhetsytelsen.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Prosedyrer og standarder relatert til risikokontroller er tilgjengelig for ansatte.

Noe informasjon mottatt fra ansatte brukes til å veilede avgjørelser.

Ledere gir instruksjoner og mottar rapporter relatert til kontrollering av risikoer, men det ser ut til å være mangel på konsistens.

Det er noe anerkjennelse av viktigheten til sikkerhetskritisk kommunikasjon i leveringen av sikker driftsytelse. Det finnes bevis på utviklingen av forsikringsplaner for å sjekke dette.

Organisasjonen yter ved minimumsnivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at skriftlige forretningsmålsettinger, -standarder og -prosedyrer for kontroll og kommunikasjon av betydelige risikoer er i formater som er egnet for brukere.

Saklig informasjon brukes til å dele opplevelser og veilede fremtidig ytelse og avgjørelser.

Ledere gir instruksjoner, noe som forsterker prosedyrer for å bidra til å oppnå sikkerhetsmålsettinger.

Ansatte rapporterer ytelsen og erfaringen sin fordi organisasjonen oppmuntrer dem til å gjøre det.

Kommunikasjon i organisasjonen er regelmessig og til en definert prosedyre både opp og ned ledelseskjeden.

Roller og ansvar for personer med plikter til å kommunisere informasjon på tvers av organisasjonen, skal tydelig defineres.

Overvåking og vurdering av kommunikasjon utføres regelmessig.

Nivå 4 — Forventet

Nivå 3 pluss at alt er på linje med hovedsystemene for risikokontroll.

Den riktige informasjonen er tilgjengelig for å ta avgjørelser.

Effektive prosedyrer for innsamling av tilbakemelding er på plass der det er relevant, for å sikre at kommunikasjon forstås og at de forstår de ansattes reaksjon til kommunikasjonen. Relevante ansatte får tilbakemelding og resultatene brukes til å prege et kommunikasjonsprogram for hele organisasjonen.

Kommunikasjon overvåkes og resultatene brukes til å prege et kommunikasjonsprogram for hele organisasjonen.

Nivå 5 — Utmerket

Nivå 4 pluss at kvaliteten på kommunikasjonen og ordningene for dem gjennomgås regelmessig mot identifiserte gode praksiser i andre sektorer. Informasjon deles proaktivt med organisasjoner som byrået har kontakt med, i tillegg til med entreprenører.

Utvekslingen av informasjon dokumenteres.

Det er en kommunikasjonsvisjon som ser utover, som deles både internt og eksternt med relevante partnere, leverandører og entreprenører.

Rollen til menneskelige faktorer i kommunikasjonen forstås tydelig og organisasjonen har et tydelig mål om å kontinuerlig forbedre kommunikasjonsytelsen.

4.4.5 S5 — Dokumentert informasjon

Utmerkede organisasjoner fremlegger et pålitelig register av viktige avgjørelser, og informasjon som er samlet inn i løpet av årene, for å demonstrere at de kontrollerer risiko på alle nivåer.

For å sikre at informasjon om risikokontroll, arbeidsprosesser og kunnskapen fra revisjoner og hendelser kommuniseres til de relevante ansatte i rett tid og på en effektiv måte, må en organisasjon ha et dokumentert styrings- og kontrollsystem som leverer dette.

Dette elementet inkluderer dokumentasjonen til sikkerhetsstyringssystemet, oppretting og oppdatering av dokumenter og kontrollen av dokumentert informasjon.

Nivå 1 — Grunnleggende

SMS-dokumentasjonen er utarbeidet. Den dekker ikke alle aktivitetene til selskapet, og den oppdateres ikke jevnlig etter enhver type endring som krever at den oppdateres.

Dokumentasjonen distribueres eller deles ikke på korrekt måte. Organisasjonen bruker ikke SMS som «arbeidsinstruksjoner», men driftspraksisene er forskjellige og ofte koblet til de personlige minnene til de ansatte og historisk praksis uten referanse til tidens gang og endringer som kan kreves som et resultat.

Dokumentasjonen brukes kun til sertifisering/autorisasjon.

Dokumentkontrollsystemer er svake, noe som fører til at forskjellige deler av virksomheten bruker forskjellige versjoner av dokumenter.

Organisasjonen faller under ytelsesnivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Jernbanebyrået/infrastrukturlederen arbeider vanligvis i henhold til prosedyrene og instruksjonene angitt i SMS. Noen avvik er mulig. Det finnes noen registreringer av informasjon om viktige risikokontroller, men registreringene er inkonsekvente.

Det finnes en årlig sikkerhetsrapport, som sendes til den nasjonale sikkerhetsmyndigheten, som inkluderer den organisatoriske strukturen, sikkerhetsmålene for følgende år og hvorfor disse er valgt. Den vil også inkludere informasjon om intern undersøkelse av ulykker og hendelser, detaljer om sikkerhetsindikatorene valgt til å overvåke ytelsen mot mål og om det er noen åpne anbefalinger fra nasjonalt etterforskningsorgan.

Dokumentkontrollsystemet er generelt sett pålitelig, men det er fremdeles problemer med versjonsnummerering og oppdatering av dokumenter på en systematisk måte.

Organisasjonen yter ved minimumsnivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at det er registreringer av prosesser og standarder for hovedrisikoene.

Det holdes registre over viktig informasjon og avgjørelser som sannsynligvis vil være verdifulle i fremtiden.

Det finnes en beskrivelse av relaterte aktiviteter til sikkerhetsstyringsprosessene og samhandlingen mellom disse prosessene i SMS. Ansatte implementerer sikkerhetsstyringsprosessene på en konsekvent måte.

Det finnes en oversikt over kontraktsprosesser og andre forretningsavtaler, inkludert detaljer om hvordan sikkerhetsrisikoer kontrolleres. Det finnes en gjeldende liste over entreprenører, partnere og leverandører med en beskrivelse av typen og omfanget av tjenesten levert, som oppdateres når nye oppgaver tilordnes.

Dokumentstyringssystemet er pålitelig og i stand til å sikre at kun den nåværende versjonen av et dokument er i omløp.

Nivå 4 — Forventet

Nivå 3 pluss at omfattende registre over sikkerhetsrelaterte prosesser, risikoene tilknyttet dem og standarder, avgjørelser og informasjon er tilgjengelig for brukere og beslutningstakere.

Dokumentkontroll er kompleks nok til å flagge når dokumenter kommer til å trenge oppdatering, og hvem som er ansvarlig for dette.

Nivå 5 — Utmerket

Nivå 4 pluss at prosessen utnyttes til å gjøre styringssystemet enda mer effektivt. SMS reflekterer de faktiske driftspraksisene til jernbanebyrået/infrastrukturlederen. SMS er et levende dokument i kontinuerlig utvikling for å forbedre sikkerheten, og er ikke en administrativ byrde.

Dokumentkontrollsystemer arbeider mot å forbedre og utvikle SMS, og ses som et nyttig verktøy i å sikre konsistens i formålet til SMS.

S6 — Integrering av menneskelige og organisatoriske faktorer

Nivå 1 — Grunnleggende

Ledelsens forpliktelse til menneskelige og organisatoriske faktorer (HOF) mangler, og det er lite kunnskap i organisasjonen om HOF-konseptet eller hvorfor HOF bør brukes for å oppnå en sikker og effektiv organisasjon. Det finnes en HOF-strategi, men det er mange mangler og den dekker ikke alle de relevante prosessene. HOF-strategien er ikke tilpasset til den organisatoriske strukturen og prosessene. Det finnes dokumenterte prosesser for HOF på noen områder, men ikke for alle, f. eks. er det ingen metoder for integrering av HOF i risikoanalyser. Det finnes ingen beskrivelser av HOF-roller og -ansvar, HOF-kompetanse mangler og ressurser tilordnes ikke HOF. HOF-strategi og HOF-prosessene som er på plass, brukes ikke fullt ut i praksis.

Nivå 2 — Mestring

HOF-strategien dekker alle relevante prosesser innenfor organisasjonen, men strukturen er utydelig og prosessene til noen HOF-områder er bedre beskrevet enn andre. Det er ikke tydelig når og hvordan HOF skal brukes. Det finnes beskrivelser av tilordnede HOF-roller og -ansvar, men det er ikke nok ressurser tilordnet. Det er en mangel på forståelse av konseptet HOF, og når og hvordan HOF-metoder skal brukes. HOF-strategi og HOF-prosesser brukes der det kreves, men innvendinger mot at det behøves, blir tatt opp. HOF-perspektivet ses ikke som viktig for å oppnå sikkerhet og effektivitet i organisasjonen.

Nivå 3 — Konsekvent

Nivå 2 pluss at en systematisk HOF-tilnærming brukes i alle deler av organisasjonen. HOF-strategi, -prosesser og -metoder brukes for det meste, men ikke alltid, og ressurser tilordnes til HOF. HOF-kompetansekrav for forskjellige roller er beskrevet og oppfylt. HOF blir vurdert i endringshåndtering. HOF er et kjent konsept for

alle i organisasjonen, og alle forstår viktigheten av å bruke en systematisk tilnærming til menneskelige og organisatoriske faktorer for å oppnå sikkerhet og effektivitet i organisasjonen.

Nivå 4 — Forventet

Nivå 3 pluss at en systematisk HOF-tilnærming brukes konsekvent i alle deler av organisasjonen. HOF-tilnærmingen er en naturlig del av alle prosesser. Fokuset er ikke på å oppfylle de juridiske HOF-kravene, men i stedet på å bruke HOF-tilnærmingen på en måte som oppfyller selskapets mål. Alle i organisasjonen ser fordelene for sikkerhet, effektivitet og kvalitet ved bruk av en HOF-tilnærming. Kapasiteten til HOF er målt, skreddersydd og proporsjonal til modenheten og kompleksiteten til organisasjonen, og er fokusert på forbedring over tid.

Nivå 5 – Utmerket

Nivå 4 pluss at organisasjonen er en ledestjerne for andre organisasjoner i hvordan den presenterer seg selv. Organisasjonen er tydelig om sin egen karakter og sitt juridiske ansvar, og prøver å utvikle dette ved å bygge på sine sterke sider og utnytte erfaringen ikke bare fra jernbanebransjen, men også utenfor den. Organisasjonen jobber aktivt for å fremme viktigheten av å håndtere problemer med menneskelige faktorer i sikkerhetsstyring.

4.5 OP — Drift

Formål

Korrekt styring av driftsaktiviteter, kontakter og endring gjør det mulig for organisasjonen å oppfylle sitt juridiske ansvar, respondere fleksibelt på endrende omstendigheter og å innføre positiv atferd hos de ansatte. Dette vil igjen gjøre det mulig for organisasjonen å oppfylle sine forretningsmålsettinger og -behov.

Innledende notater

Denne delen består av delene til SMS som håndterer kontakter (med entreprenører, leverandører og nødtjenester for eksempel), styringen av aktiva over tid og håndteringen av endring. Det er viktig for alle organisasjoner å styre disse områdene effektivt til fordel for virksomheten som en helhet. Det er den delen av SMS som håndterer de praktiske aspektene av å drive et jernbanebyrå eller en infrastrukturleder. Denne delen har tydelige koblinger til den samlede overvåkingen av effektiviteten til SMS. Dette området består også av de delene av virksomheten som har størst kapasitet til å forårsake skade på omdømmet, gjennom utilstrekkelig styring av entreprenører, leverandører og kontakter. Denne delen har også sterke koblinger til den tekniske spesifikasjonen for interoperabilitet — drift, TSI-OPE, som spesifiserer driftsprosedyrer som skal følges på tvers av funksjonelle driftsområder. Siden nasjonale sikkerhetsmyndigheter må bekrefte samsvar med TSI-OPE, er det nødvendig å sjekke disse elementene under kontroll.

4.5.1 OP1 — Driftsplanlegging og kontroll

Formål

Organisasjonen må sikre at tekniske krav og driftskrav som oppstår som følge av risikovurdering, tar hensyn til de relevante tekniske spesifikasjonene for interoperabilitet relatert til driften og undersystemer for trafikkstyring. Der nasjonale regler gjelder, oppfylles disse av planleggingen, implementeringen og gjennomgangen av de passende driftsprosessene.

En organisasjon med høy ytelse vil ha robuste systemer på plass for å oppnå samsvar med tekniske forskrifter og driftsforskrifter og har en kultur som støtter dette, og den vil alltid prøve å forbedre seg gjennom hensyn til innovasjon i jernbanesektoren og på tvers av andre bransjer.

Nivå 1 — Grunnleggende

Driftsaktiviteter utføres uten referanse til langsiktige strategier og andre forretningsbehov. Der driftsaktiviteter involverer kompetansen til og styringen av ansatte, håndteres dette på en vilkårlig måte.

Prosessene for risikovurdering brukes ikke korrekt for driftsaktiviteter. Det er lite eller ingen design av prosedyrene som reflekterer driftskontrollproblemer, slik at de reflekterer virkeligheten til jobben og ikke en idealisert versjon av den.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Det er begrenset eller ingen samsvar med de grunnleggende driftsprinsippene angitt i TSI-OPE.

Nivå 2 — Mestring

Organisasjonen tar hensyn til relevante tekniske spesifikasjoner for interoperabilitet og nasjonale regler der relevant, men dette er ikke systematisk, og tilleggstiltak er ikke tydelig basert på resultatene av risikovurderingen.

Ansatte er klar over de lokale rollene og ansvaret for driftsaktiviteter som påvirker dem, men er ikke involvert i planleggingen eller organiseringen av dem.

Noe design av arbeidsprosedyrer for drift, spesielt sikkerhetskritiske prosedyrer, utføres, men dette er ikke systematisk.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

TSI-OPE overholdes, men ved minimumsnivået som aksepteres.

Nivå 3 — Konsekvent

Nivå 2 pluss at prosessen for risikovurdering, når den brukes på driftsaktiviteter, konsekvent tar hensyn til styringen av prosesser og prosedyrer designet for å sikre at togbaner, for eksempel, er planlagt korrekt, og at risikoene tilknyttet de ansatte som driver dem, dekkes tilstrekkelig.

Prosessene for kompetansestyring, informasjon og kommunikasjon brukes konsekvent på driftsprosesser.

Det finnes en konsekvent prosess for å sikre at prosedyrer reflekterer virkeligheten til oppgaven.

TSI-OPE overholdes konsekvent på tvers av driften av organisasjonen.

Nivå 4 — Forventet

Nivå 3 pluss at det er systemer på plass for håndtering av driftsaktiviteter som er basert på risikovurdering på tvers av hele organisasjonen. Disse systemene tar hensyn til de dynamiske effektene som driftsaktiviteter i ett driftsområde (f.eks. signalsystemkravene vil ha en påvirkning på hvordan nødvendig banevedlikehold leveres), har på andre områder og prøver å forutse disse for å fjerne risiko.

Ansatte på tvers av organisasjonen slutter seg til en kultur som lar dem bidra positivt til driftsaktiviteter og eventuelle endringer som gjøres til dem.

Kommunikasjon og informasjonsdeling av driftsaktiviteter er robust, og effektiviteten til prosessen overvåkes av den overordnede ledelsen.

Driftsprosedyrer inkluderer kontaktordninger mellom forskjellige oppgaver, og dette inkluderer kontraktroller. Noe datainnsamling utføres, som brukes til å fastsette menneskelig ytelse.

De grunnleggende driftsprinsippene angitt i TSI-OPE begynner å brukes som en måte å drive et dynamisk driftselement i sikkerhetsstyringssystemet på.

Nivå 5 — Utmerket

Nivå 4 pluss at organisasjonen kontinuerlig ser etter måter å forbedre driftsaktivitetene på, via «analyse av fremtiden» innenfor og utenfor jernbanebransjen. Ansatte på alle nivåer er involvert i denne prosessen og kan bidra til den.

Organisasjonen er proaktiv i vurderingen av fremskritt i forståelsen mellom prosedyrer og oppgavevirkeligheten, og prøver å bruke disse til å forbedre sikkerheten og effektiviteten til virksomheten.

De grunnleggende driftsprinsippene angitt i TSI-OPE er en viktig del av sikker togdrift og fremmes aktivt av organisasjonen som en god praksis blant kolleger.

4.5.2 OP2 — Aktivaforvaltning

Vellykket forvaltning av aktiva involverer identifisering av aktivaene som organisasjonen eier og forvalter. Det inkluderer også å ha systemer på plass for å sikre at aktiva forblir i god tilstand i løpet av levetiden, og at de kun brukes i det tiltenkte driftsområdet, slik at organisasjonen kan oppfylle sine forretningsmålsettinger på en sikker og effektiv måte. Denne delen referer spesifikt til alle sikkerhetskritiske aktiva. Referanse til aktivaforvaltning betyr i denne konteksten forvaltningen av levetiden til aktivumet fra design til avhending.

Til slutt bør organisasjonen demonstrere at den har brukt en tilnærming sentrert rundt mennesker ved hvert trinn av livssyklusen til aktivumet.

Nivå 1 — Grunnleggende

Aktivt og reaktivt vedlikehold utføres i henhold til tidsplaner, men det finnes ikke et omfattende aktivaregister, slik at organisasjonen ikke kan være sikker på at alle aktiva vedlikeholdes i en sikker tilstand.

Aktiva er designet med begrenset referanse til fremtidige vedlikeholdsbehov, implikasjoner for menneskelige faktorer eller evnen til å avhende aktivumet på en sikker måte når livssyklusen er fullført.

Det er få eller ingen kriterier for designet av nytt utstyr.

Planen for aktivaforvaltning har mangler, slik at det ikke er mulig å være sikker på at aktivumet har blitt korrekt vedlikeholdt i løpet av levetiden.

Informasjon om tilstanden til aktivumet utveksles, men den er ufullstendig.

Systemet som er på plass for forvaltning av aktiva, håndterer samsvar med de viktige kravene for interoperabilitet der dette er aktuelt.

Selv om personer er opplært, er det lite bevis på at det finnes et omfattende kompetansestyringssystem.

Registre for forvaltningen av aktiva er ikke oppdatert.

Det finnes ikke noe system for registrering av begrensninger på bruk, og systemet for fjerning og retur av elementer til tjeneste er ufullstendig.

Aktivadesign konsentrerer seg om kommersiell tilgjengelighet heller enn å reflektere behovene til brukeren.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Det finnes planer for inspeksjon og vedlikehold av de fleste, men ikke alle aktiva.

Inspeksjonenes hyppighet er spesifisert, men ikke alltid på en risikobasis.

Manglende gjennomføring av inspeksjon blir ikke tydelig håndtert, og derfor blir inspeksjonene hengende etter.

De samlede retningslinjene for forvaltning av aktiva har ikke tydelig til hensikt å forbedre sikkerheten. Noen aktiva er designet med referanse til sikkerhetsfordeler, inkludert håndtering av problemer med menneskelige faktorer, men disse er isolerte eksempler og utgjør ikke en del av en omfattende plan.

Det er prosessen for inspeksjon av aktiva som driver aktivaforvaltningen, ikke tilstanden til aktivaene. Informasjon deles, men gir ikke et komplett bilde av aktivumet fra design og utover. Informasjon om hvordan og når aktivumet skal avhendes, er begrenset.

Det finnes et bedre aktivaregister med indikasjoner på bruken av begrensninger på bruk for utstyr som returnerer til tjeneste.

Design er avhengig av en kombinasjon av fornuft, driftserfaring og personlig preferanse heller enn en strukturert tilnærming.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at aktivaregisteret er oppdatert, og inspeksjons- og vedlikeholdsplaner er basert på risiko og følges.

Det kan være noen gjenværende inspeksjoner, men dette anerkjennes og håndteres med reduseringstiltak på plass for å redusere risikoen.

Det er noe gjennomgang av inspeksjonenes hyppighet, og noe evne til å tilpasse seg til endringer i aktivaenes tilstand.

Aktiva brukes for det tiltenkte formålet, samtidig som designets driftsstatus opprettholdes og problemer med drift i normale og degraderte tilstander håndteres. Designregistre eksisterer for de fleste aktiva, som inkluderer vurdering av menneskelige faktorer, og informasjon fra disse utgjør en del av grunnlinjen som inspeksjoner utføres mot. De fleste aktiva har avhendingsplaner med en tydelig bane til administrert fjerning fra aktivabasen.

Tilgjengelige designstandarder for menneskelige faktorer og beste praksiser brukes. Det finnes et testsystem for design som inkluderer problemer med menneskelige faktorer. Sluttbrukere har en interesse i definisjonen av kravene og testprosessen. Håndtering av endringsprosesser (se 4.5.4 OP4 Endringshåndtering) inkluderer problemer med menneskelige faktorer som en del av vurderingen av designet.

Nivå 4 — Forventet

Nivå 3 pluss at inspeksjonenes hyppighet gjennomgås systematisk, er risikobasert og systemet muliggjør fleksibilitet for at det kan tilpasse seg endringer i aktivaenes tilstand på kort og lang sikt.

Designregistre eksisterer for alle aktiva, og alle aktiva har en tydelig bane til administrert avhending. Det finnes en tydelig mekanisme for inkorporering av informasjon om endret aktivatilstand innenfor prosessen for forvaltning av aktiva og avhending av utgåtte aktiva.

Heller enn å reagere på endringer i aktivatilstanden, prøver organisasjonen å foregripe endret aktivatilstand, ved å for eksempel bruke ekstern aktivaovervåking, og kan ta i bruk de nødvendige ressursene for å håndtere dette.

Organisasjonen har en tydelig plan for designet og forvaltningen av fremtidige aktiva som forbedrer sikkerheten.

Tilbakemelding fra sluttbrukere om eksisterende design brukes til å planlegge nye aktiva. Vurderinger av menneskelige faktorer er en vesentlig del av designprosessen.

Nivå 5 — Utmerket

Nivå 4 pluss at gjennomganger av inspeksjonshyppigheter og -planer inkluderer informasjon fra utenfor organisasjonen eller jernbanebransjen.

Organisasjonen prøver å utvikle retningslinjene for aktivaforvaltning i henhold til bransjens og globale beste praksiser i feltet.

Organisasjonen har et omfattende aktivaforvaltningssystem som følger aktiva fra design til tjeneste til avhending. Organisasjonen bruker det nyeste tankesettet innen aktivaforvaltning for å sikre at sikkerhet forbedres og utvikles over tid.

Eksterne aktivaforvaltningssystemer gir detaljert informasjon om tilstanden til alle aktiva, og dette mates inn i organisasjonens retningslinjer for risikohåndtering for å opprettholde aktivumet i en egnet tilstand.

Det finnes et omfattende kompetansestyringssystem som utvikler ansatte som er ansvarlige for aktivaforvaltning, og sikrer at de får tilstrekkelig opplæring og har den nødvendige kunnskapen og erfaringen til å utføre arbeidet som de er ansvarlige for.

Design er basert på en fortrolig kunnskap om hva aktivumet er for og hvordan det brukes. Organisasjonen prøver å bruke beste praksiser i menneskelige faktorer for å anskaffe, introdusere, opprettholde og avhende aktiva.

4.5.3 OP3 — Entreprenører, partnere og leverandører (kontaktordninger)

Organisasjoner må effektivt administrere sikkerheten til sine entreprenører, partnere og leverandører og de som påvirkes av aktivitetene til organisasjonen, der de aktivitetene utføres.

Det er ikke bare et spørsmål om risikovurdering, og det krever heller ikke en liste over alle risikoer eller kategorier av relevante risikoer, men det krever at søkeren viser hvordan systemene og prosedyrene i sin helhet er designet og organisert for å tilrettelegge for identifikasjon, vurdering og kontroll av disse risikoene. Bruk av velformulerte kontrakter er en generelt sett akseptabel måte å håndtere risikoer på. Men hovedansvaret for å administrere entreprenører og sjekke levereringen deres mot de angitte spesifikasjonene ligger hos jernbanebyrået/infrastrukturlederen. Bruk av entreprenører eller underleverandører betyr ikke at jernbanebyrået/infrastrukturlederen delegerer noe av ansvaret sitt for å sikre at de avtalte tjenestene utføres etter standardene spesifisert før drift.

Søkeren skal demonstrere at denne har prosesser på plass for å fastsette kompetansen til entreprenører og andre leverandører, og til å vurdere sikkerhetsytelsen deres som en del av anskaffelsesprosessen.

Hovedelementene til entreprenørkontroll inkluderer:

- en tydelig definisjon av kontraktordninger;
- å gi en tydelig spesifikasjon av jobben;
- å velge entreprenøren;
- å gjøre entreprenøren kjent med anleggsområdet (hvis aktuelt);
- kontroll av produktsikkerhet og -kvalitet;
- arbeidstillatelse (hvis aktuelt);
- overlevering ved slutten av jobben; og
- overvåking og gjennomgang av ytelsen.

Hvis noen av eller alle elementene ovenfor mangler eller er ufullstendige, vil dette være en viktig tilbakemelding for avgjørelse av en organisasjons modenhetsnivå.

Nivå 1 — Grunnleggende

Den potensielle påvirkningen på sikkerhetsytelsen til selskapet ved bruk av en entreprenør er ikke vurdert og de følgende organisatoriske endringene håndteres ikke korrekt. Organisasjonen gjør få forsøk på å identifisere eller samarbeide med andre organisasjoner med hensyn til delte risikokontroller. Kontraktordninger, der de eksisterer, tar ikke sikkerhetsbegrensninger med i betraktningen og entreprenøren er ikke klar over sikkerhetsansvaret sitt. Prosedyrer for å oppnå dette er svake eller finnes ikke. Kulturelt sett er det en tendens til å ikke dele informasjon som angår risikokontroll.

Ingen informasjon samles inn eller deles, og dette kreves ikke i kontraktordningene.

Entreprenører utnevnes når nødvendig. Men når entreprenører velges, er det få overveielser annet enn kostnader. For eksempel er en tidligere entreprenørs sikkerhetsytelse ikke et utvelgingskriterium i løpet av anskaffelsesprosessen. Det er lite planlegging av arbeidet og lite vurdering av ansvaret for risikokontroll når det avgjøres hvordan arbeidet skal gjøres.

Det er lite overvåking av entreprenørene, eller gjennomgang av den fullførte kontrakten.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Prosedyrer identifiserer faktisk kontakt mellom forretningsenheter på arbeidsnivå. Det er samarbeid med de andre organisasjonene over prosedyrer og standarder som skal implementeres, men dette er ikke systematisk. Disse brukes av ansatte for noen delte risikokontroller, som på dette nivået har blitt identifisert.

Noen elementer av et risikokontrollsystem er på plass for entreprenørkontroll, men det ser ikke ut til å være en systematisk prosess fra utvelging til gjennomgang etter kontrakt.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at organisatorisk kontakt med entreprenører, partnere og leverandører er systematisk identifisert.

Prosedyrer og standarder er på plass for å kontrollere delte risikoer, med hvilken part som er ansvarlig for hva, tydelig identifisert.

Det finnes skriftlige målsettinger for systemsikkerhet, og disse vurderes når kontraktordninger utarbeides.

Det foregår regelmessige diskusjoner med andre organisasjoner som de har kontakt med, for å avtale målsettinger, standarder, prosesser og ordninger.

Det finnes metoder for deling av informasjon på arbeidsnivå.

Kommunikasjon utenfor organisasjonen er tilfredsstillende, for å sikre at alle som tar avgjørelser relatert til risikokontroll med kryssorganisatoriske grenser, har riktig informasjon (i form av prosedyrer og standarder), saklige data og intelligens og instruksjoner og rapporter.

Viktigheten til entreprenørkontroll anerkjennes, og dette reflekteres i organisasjonens relevante retningslinjer.

Entreprenører velges etter evnen til å fullføre arbeid sikkert og til en tilfredsstillende standard.

Entreprenørens ytelse overvåkes under kontrakten, og passende ytelsestiltak brukes effektivt for å spore oppnåelsen.

Nivå 4 — Forventet

Avgjørelser og ordninger er konsekvente med all informasjonen gitt i nivå 3.

Det finnes ordninger for deling av informasjon gjennom hele organisasjonen for å fremme effektive gjennomganger og kontinuerlig forbedring.

Det er en systematisk tilnærming til entreprenørkontroll.

Effektive prekvalifiseringsordninger tar en balansert tilnærming, inkludert vurdering av sikkerhetsytelsen til potensielle entreprenører.

Det er en tydelig forståelse av ansvaret på alle nivåer av kontraktarbeidet. Gode arbeidsforhold mellom klienten og alle entreprenører leveres gjennom effektive kontaktordninger.

Ytelsestiltak og gjennomganger etter kontrakt veileder avgjørelser om valg av entreprenører for ytterligere arbeid.

Det finnes et system for å sikre den nødvendige sporbarheten til relevante avgjørelser, kommunikasjon osv.

Nivå 5 — Utmerket

Nivå 4 pluss at organisasjonen ser til andre sektorer og land for å identifisere systemsikkerhetsproblemer og -utviklinger for å mate til deres styringsordninger for entreprenører, partnere og leverandører der aktuelt.

Samarbeid mellom byrået og deres entreprenører, partnere og leverandører brukes for å få best mulig oppnåelse av delte målsettinger.

God praksis deles med andre organisasjoner, inkludert entreprenører, partnere og leverandører.

Forsyningskjeden for entreprenøren leverer sømløst alle organisasjonens målsettinger.

Entreprenørens hoved- og sikkerhetsaktiviteter er på linje med organisasjonens.

Det er ingen forskjell i behandlingen av entreprenørers ansatte og selskapets egne ansatte — alle mottar samme opplæring og informasjon for å sikre sikkerheten deres.

4.5.4 OP4 — Endringshåndtering

Formålet med endringshåndtering er å sikre at endringer innenfor organisasjonen er tilstrekkelig planlagt, gjort i henhold til EU-krav og sjekket for å hjelpe organisasjonen med å oppnå sine forretningsmålsettinger. Effektiv endringshåndtering vil kontrollere risikoene som endringen forårsaker, og vil hjelpe organisasjonen med å sikre at riktig avgjørelse tas for å forbedre virksomheten uten at sikkerheten reduseres.

Prosessen skal gjøre det mulig for risikoer å vurderes på en proporsjonal og robust måte, inkludert saker med menneskelige faktorer der aktuelt, i tillegg til for rimelige kontrolltiltak som skal tas i bruk.

Nivå 1 — Grunnleggende

Noen typer endringer anerkjennes og aspekter ved det håndteres.

Ikke alle risikoer tilknyttet en endring identifiseres, og vurderes dermed ikke.

Effekten endringen har på organisasjonens kultur, vurderes ikke.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Viktigheten med endringshåndtering forstås, og det er en liten grad av kontroll over alle typer endringer.

Endringer planlegges, men er ikke alltid tilstrekkelige.

Systemet for planlegging for endringer er ikke tydelig, noe som fører til at risikoer blir identifisert eller kontrollert etter en endring, i stedet for før endringen finner sted.

Det er liten vurdering av virkningene en endring har på organisasjonens kultur.

Roller og ansvar for å håndtere endringer og de tilknyttede sikkerhetsrisikoene er ikke tydelige definert.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at det er en effektiv tilnærming til håndtering av enhver prosessendring, organisatorisk eller teknisk endring.

Det kan være en strukturert tilnærming til endring, som involverer et antall trinn i endringshåndteringssystemet.

Det er en konsekvent tilnærming til risikovurdering og risikokontroll før og etter endringen gjøres. Risikovurdering er en viktig del av endringshåndteringsprosessen.

Nivå 4 — Forventet

Nivå 3 pluss at en gjennomgang utføres etter at en endring gjennomføres, for å også vurdere effekten endringen har hatt på kulturen til organisasjonen.

Det finnes en omfattende logg over problemer, for å fange opp utviklinger etter hvert som de oppstår under endringen.

Det anerkjennes at involvering av de ansatte i endringsprosesser er viktig og bringer fordeler.

Det finnes en prosedyre for planlegging, implementering og kontrollering av endringer til sikkerhetsstyringssystemet etter hvert som de oppstår under endringen.

Det anerkjennes at involvering av de ansatte i endringsprosesser er viktig og bringer fordeler.

Endringshåndteringsprosessen inkluderer virkningene av foreslåtte endringer på partnere, leverandører og andre som organisasjonen har kontakt med.

Nivå 5 — Utmerket

Nivå 4 pluss at det også er en forståelse av at endringen påvirker andre aspekter av virksomheten. Det fører til at risiko blir koblet med sikkerhetsrisiko under og som et resultat av enhver endring.

Antagelser gjort om og under endringen, testes, og korrekte beredskapstiltak iverksettes hvis det viser seg at antagelsene ikke er nøyaktige.

4.5.5 OP5 — Nødsituasjonshåndtering

Robuste systemer for nødsituasjonsplanlegging er viktige for alle pliktinnehavere, og må dekke informasjonen som må leveres til nødtjenestene for å gjøre det mulig for dem å tegne opp deres responsplaner for alvorlige hendelser.

Elementer av nødsituasjonsplanlegging inkluderer:

- identifisere overskuelige nødsituasjoner som kan oppstå;
- utvikle ordninger for å svare på de nødsituasjonene;
- gi tilstrekkelig opplæring og sikre at de nødvendige ressursene er tilgjengelige; og
- teste planer, med andre personer og organisasjoner som nødvendig.

Nivå 1 — Grunnleggende

Det er lite organisatorisk identifikasjon av mulige nødsituasjoner og hvordan man skal reagere hvis nødsituasjoner oppstår.

Organisasjonen er avhengig av at nødtjenester håndterer alle aspekter av en nødsituasjon, og har ikke noen ordninger på plass med andre aktører som kan være involvert i håndteringen av alvorlige hendelser, annet enn å ringe dem og la dem takle hendelsen.

Organisasjonen faller under nivået som forventes av innehaveren av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Organisasjonen følger regler og praksiser forespurt av eksterne organer/organisasjoner, for eksempel infrastrukturlederen eller andre jernbanebyråer, og har på plass et system for å håndtere nødsituasjoner.

Større nødsituasjoner som kan oppstå, identifiseres, og det er noen planer på plass for å håndtere dem.

Ansatte får kun opplæring i nødrespons når det er helt nødvendig.

Det finnes prosedyrer for nødrespons ofte produsert av andre organer/organisasjoner og tatt i bruk internt.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at potensielle nødsituasjoner som oppstår fra oppgaver, identifiseres som en del av risikovurderinger.

Kontrolltiltak, inkludert opplæring og ressurser, er på plass for å håndtere nødsituasjoner og deles med relevante parter.

Felles øvelser for nødrespons finner sted med andre organisasjoner involvert i en oppgave.

Omfattende prosedyrer for nødrespons finnes, som involverer andre organisasjoner, for eksempel nødtjenester eller lokale myndigheter som aktuelt.

Nivå 4 — Forventet

Nivå 3 pluss at det tas hensyn til tilbakemelding fra øvelsesrapporter når prosedyrer gjennomgås, for å sikre at nødrespons forblir oppdatert og effektiv.

Det er jevnlig samarbeid mellom organisasjonen, nødtjenestene og andre involverte aktører når alvorlige hendelser oppstår, for å sikre at endringer i prosesser/prosedyrer og tekniske saker vurderes nøye og endres gjennom endringshåndteringsprosessen.

Nivå 5 — Utmerket

Nivå 4 pluss at organisasjonen tar i bruk gode praksiser i nødsituasjonshåndtering, spesielt ved kontaktkoordinering, både innenfor og utenfor jernbanebransjen. Jevnlig samarbeid med nødtjenester er proaktivt med hensikt på å utvikle bedre felles respons for alle fremtidige hendelser.

4.6 PE — Ytelsesevaluering

Formål

Hensikten er å sikre at risikokontroller er på plass, fungerer korrekt og oppnår organisasjonens målsettinger.

Innledende notater

Organisasjoner må måle effektiviteten til risikokontroller for å sikre at risikoer identifiseres og håndteres i praksis. Sikkerhetssystemer for arbeid må overvåkes for å sikre at de er passende og at de faktisk følges. Systemer for overvåkings-, revisjons- og gjennomgangsytelse skal være på plass for å sikre at sikkerhetsstyringssystemet fungerer korrekt.

En revisjon sjekker at organisasjonen gjør det den sier den skal gjøre. Den skal støttes av jevnlige gjennomganger for å sikre at organisasjonens forretningsmålsettinger er korrekte. Gjennomgangen skal også sjekke at ordningene som er på plass for å oppfylle forretningsmålsettingene, fungerer som ment.

Overvåking, revisjon og gjennomgang danner en tilbakemeldingssløyfe innenfor det samlede sikkerhetsstyringssystemet, og er en viktig del av programmer for kontinuerlig forbedring og oppnåelse av utmerkethet.

4.6.1 PE1 — Overvåking

Organisasjonen skal kunne demonstrere at den har på plass en prosess for overvåking av bruken og effektiviteten til sikkerhetsstyringssystemet, og at denne prosessen er passende for størrelsen, omfanget og typen drift. Organisasjonen skal demonstrere at prosessen kan identifisere, evaluere og korrigere eventuelle mangler i funksjonen til SMS.

Nivå 1 — Grunnleggende

Det finnes ingen effektiv prosess for å angi sikkerhetsmål og samle inn og analysere data. Det er lite eller ingen forståelse av om eksisterende risikokontroller fungerer effektivt.

Det er ikke noe oppfattet forretningsbehov for å håndtere og måle problemer med menneskelige faktorer. Der de vurderes, skjer det på ad hoc-basis.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Overvåking implementeres, men dette er ofte ad hoc; noen prosesser kontrolleres og noe utstyr inspiseres, dette fører til en inkonsekvent tilnærming til datainnsamling.

Registre er isolerte og analyseres ikke på selskapsnivå. Konsekvensen er en tilnærming til handlingsplaner som ikke er tydelig definert og ikke er koordinert på selskapsnivå.

Det er ingen tydelig forbindelse mellom sikkerhetsretningslinjer, selskapets sikkerhetsmål og handlingsplaner for forbedringer.

Behovet for å overvåke risikokontroller anerkjennes ikke av ledelsen, og det er opp til enkelte avdelinger eller enheter å avgjøre hvilken informasjon som skal samles inn.

Det anerkjennes at menneskelige faktorer kan spille en rolle i forretningsytelsen, men bruken er ikke konsekvent.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at organisasjonen forsøker å bruke den gjeldende felles sikkerhetsmetoden for å sjekke den korrekte bruken av sikkerhetsstyringssystemet og alle prosessene og prosedyrene innenfor det, og implementerer de nødvendige korrigerende tiltakene som kreves som et resultat av ikke-samsvar identifisert.

Overvåking er prosessdrevet, så kritiske og sårbare systemer blir ikke prioritert over overvåking av mindre kritiske eller sårbare systemer. Måling finner sted for syns skyld, og ikke med et tydelig definert formål.

Koblingen mellom risikovurdering er begrenset til identifikasjon av risikokontroller, som deretter overvåkes på en logisk måte.

En overvåkingsstrategi er definert, og planer er utviklet for å implementere den. Dette fører til en konsekvent tilnærming til innsamling og analysering av data, informasjon brukes av ledelsen til å ta avgjørelser og forbedre organisasjonen.

Tilordningen av ressurser til overvåking er ikke prioritert i henhold til resultatene av risikovurderingen.

Det finnes en godkjent prosess som en del av ytelsesevalueringen for undersøkelse av påvirkningen av problemer med menneskelige faktorer innenfor SMS. Der det er nødvendig, er det tilgang til spesialekspertise for å evaluere dette.

Nivå 4 — Forventet

Nivå 3 pluss en forståelse av overvåkingen av viktige og sårbare systemer.

Den relevante CMS brukes fullt ut og overvåking er fullstendig risikobasert. Kritiske prosesser er prioritert i ressurstilordning.

Ledere og tilsynsførere er godt opplært og har de nødvendige ressursene, og det er bevis på utfordring av eksisterende arbeidssystemer for å identifisere eventuelle svikter i tilnærmingen.

Mellomledere og overordnede ledere overvåker resultater på en risikobasis, og handlingsplaner koordineres og diskuteres på selskapsnivå. Formålet med overvåking er å forutse degraderingen av sikkerhetsytelse og å se etter områder for forbedring og ikke bare måle resultatene til SMS.

Det er spesifikke indikatorer for evaluering av påvirkningen av menneskelige faktorer på bruken av SMS og for å spore forsikringsprosessen.

Nivå 5 — Utmerket

Nivå 4 pluss bruk av avanserte verktøy for overvåking. Organisasjonen har verktøy for å støtte arbeidere i rapportering av forekomster og for å foreslå løsninger som skal diskuteres i handlingsplanene.

Dataanalyser anses som en konkurransefordel, og overvåking av sikkerhetsytelse er en del av en global overvåkingsprosess som inkluderer alle enhetene og avdelingene. Organisasjonen har et omfattende datahåndteringssystem for å kartlegge sine aktiva og vilkårene for bruk.

Selskapet anerkjenner viktigheten av å bruke risikomodeller og dele data og informasjon med andre jernbaneoperatører for å forstørre datasettene sine og forbedre datakvalitet for risikovurdering.

Rapportering er god praksis og det er prosjekter for å støtte en sterk rapporteringskultur i selskapet.

Overvåkingsprosedyrer gjennomgås for å sikre at de forblir relevante til organisasjonens risikoprofil.

Data fra forsikringen av problemer med menneskelige faktorer er en vesentlig del av kontinuerlig forbedring i organisasjonen. Resultatene brukes deretter for å ta forretnings- og sikkerhetsstyringsavgjørelser. Informasjonen som skaffes, deles med partnere, leverandører og entreprenører.

4.6.2 PE2 — Intern revisjon

En intern revisjon er en avgjørende uavhengig og systematisk sjekk av risikokontrollsystemer og håndteringsordninger som tar sikte på å sikre at forretningsmålsettinger oppfylles. Intern revisjon kreves også under CMS for overvåking. Revisjoner er generelt sett designet for å prøve å begrense subjektivitet til fordel for en mer bevisbasert tilnærming. Den systematiske naturen til en revisjon i SMS-konteksten er ment å gi den overordnede ledelsen noe tydelig bevis som de bør basere avgjørelser for å forbedre sikkerhetsytelse på.

Nivå 1 — Grunnleggende

Det finnes lite eller ingen bevis på at revisjoner utføres.

Revisjoner som utføres, er ikke planlagt eller prioritert, og funnene har ingen innvirkning.

Revisorer får ikke konsekvent opplæring, og koblingene til CMS-prosessen er ufullstendige.

Revisjonsprosesser er ikke strukturerte, det er ingen virkelig forskjell mellom revisjoner og inspeksjoner.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Det skjer noe revisjon, men teknikkene som brukes og områdene som dekkes, tar ikke hensyn til karakteren eller viktigheten til det bestemte risikokontrollsystemet.

Det er planer for revisjoner, men disse er ikke koordinert.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at det er bevis på en koordinert, effektiv og planlagt tilnærming til revisjoner. Revisjonsaktiviteter har fokus på å oppnå samsvar med lovgivning og å oppfylle forretningsmålsettinger.

Revisjoner er systematisk dokumentert og resultatene registrert. Organisasjonens styre er klar over resultatene og diskuterer disse på regelmessige styremøter.

Kompetansestyringssystemet inkluderer bestemmelser for opplæring av revisorene. Et register av kompetente revisorer opprettholdes.

Nivå 4 — Forventet

Nivå 3 pluss at revisjonsaktiviteter er planlagt og prioritert, og tar hensyn til resultatene av tidligere revisjoner og resultatene av overvåking.

En passende kombinasjon av revisjonsteknikker brukes for å gi informasjon om ytelse mot forretningsmålsettinger.

Toppledelsen informeres om resultatet av revisjonene, slik at de er i en posisjon til å gjennomgå sikkerhetsstyringssystemet. På dette nivået er kontinuerlig forbedring som er påkrevd av SMS, underlagt analyse for å teste om forbedringene faktisk leverer de forventede fordelene eller må endres for å forbedre resultatene.

Nivå 5 — Utmerket

Nivå 4 pluss tillegget at forretningsmålsettingene som revisjonen utføres mot, er mer utfordrende og det er en sammenligning med beste praksis.

Peer-to-peer-revisjonsmålsettinger er inkludert.

4.6.3 PE3 — Ledelsesgjennomgang

Sterk sikkerhetsledelse fra ledelsen er viktig for at et organisasjons sikkerhetsstyringssystem skal fungere effektivt, og for systemets kontinuerlige utvikling over tid. Organisasjonen skal demonstrere at ledelsen er aktivt involvert i gjennomgangen av ytelsen til sikkerhetsstyringssystemet og utviklingen av det for fremtiden. Gjennomgang av ledelsen kan anses som en del av overvåkingen som en organisasjon utfører for å sikre at dens prosesser og prosedyrer leverer det tiltenkte resultatet.

Nivå 1 — Grunnleggende

Det er lite analyse av funnene til overvåking og revisjoner av toppledelsen. Dette gjøres mer på enhets-/avdelingsnivå.

Forretnings- og sikkerhetsmålsettinger gjennomgås ikke regelmessig.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Gjennomgangene som utføres, er ikke en del av en organisert tilnærming til forbedring. De er ofte reaktive, og er ikke ofte planlagt som en del av ledelsessyklusen.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at ledelsen automatisk bruker funnene fra overvåking og revisjoner til å gjennomgå organisasjonens ytelse og foreta endringer der det er nødvendig.

Anbefalinger fra gjennomganger tilordnes, spores og viser tydelig at de bredere implikasjonene vurderes.

Nivå 4 — Forventet

Nivå 3 pluss at man tar lærdom av hendelser i andre organisasjoner og andre bransjer.

Ledelsen spør etter forslag fra ansatte angående forbedringer i forretningsprosesser, og går gjennom disse for å se om de vil utgjøre en forskjell for virksomheten.

Nivå 5 — Utmerket

Nivå 4 pluss at ledelsen iverksetter vilkårlige gjennomganger av praksiser i bestemte områder av virksomheten for å teste om prosesser og prosedyrer fortsatt passer for formålet.

Ledelsen engasjerer seg i «analyse av fremtiden» med det formålet å identifisere nye teknologier eller ideer, som kan forbedre virksomheten. For eksempel anses bruk av stordata for å forbedre virksomhetseffektivitet og sikkerhetsytelse.

4.7 I — Forbedring

Formål

Organisasjoner må utvikle seg over tid, for hvis de ikke gjør det, vil de stagnere og bli tilfredse. Dette vil eventuelt ha konsekvenser for styringen av sikkerhet. Organisasjonen bør slutte seg til en filosofi der de lærer fra sine egne og andres feil for å forbedre sine sikkerhetsstyringskontroller. Filosofien bak forbedring er å fokusere organisasjonen på å tenke fremover, prøve å forutse endringer i fremtiden og sikre at når endringen oppstår, resulterer den i at SMS utvikles på en positiv måte.

Innledende notater

En organisasjon kan forbedre seg gjennom å lære fra sine egne undersøkelser av ulykker og hendelser (inkludert hendelser og farlige forekomster) i tillegg til å lære fra andre hendelser som oppstår i jernbanesektoren eller andre industrielle sektorer. Organisasjoner skal også undersøke mulige hendelser med den samme grundighet som de vil undersøke en ulykke, slik at de kan lære hva som nesten skjedde, hvordan situasjonen oppstod og hvordan lignende forekomster kan unngås. Oppsummeringer av undersøkelser og resultatene av disse skal deles på tvers av organisasjonen og med andre lignende organisasjoner så langt som mulig. Organisasjoner skal være proaktive når de prøver å lære å forbedre seg, ikke bare gjennom å lære fra ulykker og hendelser, men gjennom andre relevante tilgjengelige informasjonskilder, for eksempel overvåking og revisjon eller erfaringen til andre som kan hjelpe organisasjonen med å forbedre seg.

4.7.1 I1 — Lære av ulykker og hendelser

Undersøkelsen av ulykker og hendelser skal gå gjennom ytelsen til sikkerhetsstyringssystemet før hendelsen fant sted, og finne ut hvilke deler av systemet som fungerte bra og hvilke områder som krever forbedring, inkludert all lærdom om menneskelig ytelse. Organisasjonen skal også prøve å lære fra resultatene til undersøkelser av det nasjonale etterforskningsorganet (NIB), andre NIB-er i EU og fra undersøkelser av hendelser og ulykker over hele verden.

Nivå 1 — Grunnleggende

Det finnes lite bevis på effektive undersøkelser, og kulturen til organisasjon er å finne noen å legge skylden på. Det tas ingen lærdom av undersøkelse av hendelser som oppstår utenfor organisasjonen eller i andre bransjer. Kompetansen til personer som utfører undersøkelser, kan betviles.

Det er lite eller ingen indikasjon på at rollen til mennesket i en ulykke eller hendelse vurderes korrekt.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 2 — Mestring

Hendelser undersøkes, men det er liten veiledning for hvordan eller hva som skal undersøkes.

Direkte årsaker undersøkes.

Spekteret av hendelser som undersøkes, er stort sett begrenset til ulykker, og anbefalinger som oppstår fra undersøkelser, er begrenset til å forhindre at det samme skjer igjen. De identifiserer ikke områder for bredere forbedring.

Det er noen forsøk på å lære fra andre ulykker i andre deler av bransjen.

Ansatte som utfører undersøkelsen, har fått noe opplæring, men de er ikke en del av et effektivt kompetansestyringssystem.

Det anerkjennes at menneskelige faktorer spiller en rolle i ulykker og hendelser, og noen forsøk gjøres for å utforske dette i undersøkelsen, men dette går ofte tapt når rapporten signeres på ledelsesnivå.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Nivå 3 — Konsekvent

Nivå 2 pluss at det finnes standardordninger for når og hvordan undersøkelser utføres.

Den underliggende årsaken til en hendelse undersøkes, og undersøkelser utføres også etter en hendelse.

Ansatte har fått omfattende opplæring i undersøkelse av ulykker og hendelser, og er en del av et kompetansestyringssystem.

Aspektene med menneskelige faktorer ved ulykker og hendelser er et standardaspekt av undersøkelsesprosessen. Ledelsen anser disse som like viktige som andre årsaker til en hendelse, og jobber for å korrigere problemer når de oppstår.

Nivå 4 — Forventet

Nivå 3 pluss at undersøkelsen er av slik kvalitet at den gir anbefalinger som kan brukes både innenfor og utenfor organisasjonen.

Spekteret av undersøkte hendelser inkluderer, der aktuelt, forstyrrelser i arbeid og der forventede resultater ikke oppnås.

Toppledelsen informeres om resultatet av undersøkelsene og anbefalingene, og sørger for at de blir implementert som aktuelt.

Anbefalinger fra hendelsesundersøkelser i andre jernbanebyråer eller -virksomheter utenfor organisasjonen studeres for å se om det er relevante resultater for virksomheten.

Organisasjonen prøver å ta lærdom av menneskelige faktorer fra andre undersøkelser innenfor jernbanebransjen og utenfor den, og å håndtere disse i SMS.

Nivå 5 — Utmerket

Nivå 4 pluss en forståelse av implikasjonene til funnene fra andre organisasjoners undersøkelser.

Det er en villighet til å lære fra hendelser gjennom endring i atferd på tvers av virksomheten.

Toppledelsen er involvert i spredningen av egne erfaringer til andre virksomheter i jernbanesektoren og utenfor den, og handler på lærdom fra andre jernbanebyråer eller andre bransjer.

Organisasjonen prøver å formidle lærdom om menneskelige faktorer fra ulykker og hendelser til sine partnere, leverandører og entreprenører og andre.

4.7.2 I2 — Kontinuerlig forbedring

Organisasjonen må vise at den prøver å forbedre seg hele tiden gjennom å lære fra hendelser, kontakt med reguleringsorgan og andre ruter. Under kontroll forventes det at organisasjoner demonstrerer at den har en prosess for å identifisere og implementere positive endringer til sitt SMS, inkludert gjennom strategien for kontinuerlig forbedring for sikkerhetskultur. Korrigerende tiltak handler om definisjon, tilordning og fullføring av tiltak identifisert som obligatoriske etter overvåking, undersøkelse, revisjon og gjennomgang.

Nivå 1 — Grunnleggende

Til tross for prosesser og prosedyrer i SMS resulterer overvåking, revisjoner og gjennomganger i lite eller ingen endring, enten fordi ingen utføres eller de følges ikke opp.

Organisasjonen faller under nivået som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Hendelser og ulykker «kommer til å skje» — en fatalistisk kultur dominerer. Det finnes ingen virkelig strategi for kontinuerlig forbedring av sikkerhetskulturen. Menneskelige feil i det problematiske området identifiseres alltid som årsaken uten at det gjøres forsøk på å undersøke videre. Det er ingen rettferdig kultur, og personale som er involvert i hendelser og ulykker, blir ofte gjort til syndebukker. Ledelsen og ansatte er generelt sett uinteressert i sikkerhet, og bruker muligens sikkerhet kun som grunnlaget for andre diskusjoner, for eksempel lønn, arbeidstimer osv.

Nivå 2 — Mestring

Enkle funn fra overvåking, undersøkelse, revisjon og gjennomgang fremkaller enkle tiltak og endringer til lave nivåer av sikkerhetsstyringssystemet. Det er noen få forsøk på å se etter underliggende årsaker i hele organisasjonen fra en systematisk gjennomgang av informasjon fått fra overvåking, undersøkelse og revisjon.

Organisasjonen oppfyller akkurat minimumsforholdene for juridisk samsvar som forventes av en innehaver av et felles sikkerhetssertifikat eller sikkerhetsfullmakt.

Sikkerhetsavdelingen anses å være ansvarlig for sikkerheten, men ledelsen legger tid og innsats i forhindring av hendelser og ulykker, siden disse betraktes som noe som kan forhindres. En kontinuerlig forbedringsstrategi for sikkerhetskultur finnes, og den dekker de riktige generelle områdene, men korrigerende tiltak håndterer hovedsakelig menneskelige feil av ansatte i det problematiske området gjennom straff eller andre måter, for å redusere utrygg atferd siden dette ses på som årsakene til hendelser og ulykker. Sikkerhetsytelse måles i hemmende indikatorer, for eksempel skader med tapt tid, medisinske skader, avsporinger, kjøring på rødt lys osv. Organisasjonen har flere alvorlige hendelser og ulykker enn konkurrentene.

Nivå 3 — Konsekvent

Nivå 2 pluss at det finnes en prosess for å sikre at de nødvendige tiltakene som identifiseres ved overvåking, revisjon og gjennomganger, implementeres, og identifiserer hvem som er ansvarlig for tiltakene og tidsrammene for å utføre dem.

Det finnes prosedyrer for overvåking av egnetheten, tilstrekkeligheten og effektiviteten til sikkerhetsstyringssystemet som tar hensyn til rammeverket angitt i den gjeldende felles sikkerhetsmetoden, og disse gir konsekvente resultater.

Korrigerende tiltak vil være på ethvert nivå av sikkerhetsstyringssystemet.

Ledelsen anerkjenner at hendelser og ulykker forårsakes av flere faktorer, hvor noen kommer fra avgjørelser fra ledelsen. Alvorlige hendelser og ulykker undersøkes, og en systematisk prosess for lærdommer har blitt startet. Det finnes en konsekvent strategi for kontinuerlig forbedring av sikkerhetskulturen, som er godt utarbeidet og i stand til å vurderes korrekt for suksess.

Nivå 4 — Forventet

Nivå 3 pluss mekanismer for å spore fremgang og avslutning for korrigerende tiltak.

Korrigerende tiltak er koblet til målsettinger angitt i sikkerhetsstyringssystemet.

Resultatene av sikkerhetsmål og planlegging, risikovurdering, involvering av ansatte og andre parter, informasjon og kommunikasjon, overvåking, revisjon, ledelsesgjennomgang og lærdom fra ulykker og hendelser brukes som et grunnlag for å utvikle strategier og planer for kontinuerlig forbedring.

Årsaksanalyse utføres for alle hendelser og ulykker, og det aksepteres at de fleste kommer fra avgjørelser fra ledelsen. Det er en forståelse av at alle er ansvarlige for ikke bare sin egen sikkerhet, men også sikkerheten til kollegene. Ledelsen og ansatte behandler hverandre med respekt, og en systematisk tilnærming for å sikre

rettferdighet er på plass. En sunn livsstil fremmes, og ikke-arbeidsulykker overvåkes. Strategien for kontinuerlig forbedring av sikkerhetskulturen følger beste praksis med realistiske og målbare målsettinger.

Nivå 5 — Utmerket

Nivå 4 pluss at de korrigerende tiltakene fører til ledelsesgjennomgang av lignende prosesser utenfor det umiddelbare området der hendelsen oppstod, for å identifisere lignende mangler som finnes og eventuelle endringer som bør gjøres.

Forhindring av hendelser og ulykker som fører til fysisk og psykologisk skade for ansatte eller tredjeparter, er en prioritet i organisasjonen. Organisasjonen har ikke opplevd noen registrerbar hendelse eller ulykke på mange år, men det er ingen følelse av tilfredshet. Atferds- eller organisasjonsdrifting overvåkes kontinuerlig og tiltak iverksettes for å hindre at dette skjer. Organisasjonen bruker en rekke ledende indikatorer til å overvåke ytelse. Strategien for kontinuerlig forbedring av sikkerhetskulturen anses av likestilte som en leder i feltet etter beste praksis fra innenfor og utenfor jernbanesektoren.

Vedlegg — Veiledning til nivåer

Modenhetsnivåer	Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5
Tittel	Grunnleggende	Mestring	Konsekvent	Forventet	Utmerket
Kort definisjon	På dette nivået har organisasjonen som vurderes, et sikkerhetsstyringssystem, men det er tydelig at det er mangler som bringer ytelsesnivået under det som var påkrevd for bevilgning av et felles sikkerhetssertifikat eller sikkerhetsfullmakt. Prosedyrer og instruksjoner for å håndtere sikkerhetsaktiviteter eksisterer, men i løpet av kontrollen er det åpenbart at det er alvorlige problemer angående hvor logiske disse er som en helhet. Individuelle risikoer kontrolleres, men den samlede prosessen som håndterer dette, er svak. Organisasjonen drives i praksis på en måte der det ser ut til å være større uforenligheter med det som er beskrevet i sikkerhetsstyringssystemet (SMS). Retningslinjer, prosedyrer og instruksjoner ser ut til å brukes på måter som ikke tilsvarer de angitt i SMS, og derfor blir ikke risikoene fra virksomheter levert av organisasjonen eller dens	På dette nivået yter organisasjonen på nivået for minimum juridisk samsvar, dvs. SMS fungerer på et nivå som var tilstrekkelig til at et felles sikkerhetssertifikat eller sikkerhetsfullmakt ble bevilget ved vurderingstrinnet. Det skriftlige sikkerhetsstyringssystemet eksisterer og blir brukt til å kontrollere sikkerhetsrisikoer, men det mangler struktur og koordinering. Systemet er logisk generelt sett, men det finnes mangler og noen tilnærmingsuforenligheter i forskjellige områder. Organisasjonen mestrer hovedsakelig sikkerhetsansvaret sitt, men det er så vidt. Det vil ikke kreve mye å skape et betydelig problem og falle tilbake til nivå 1, fordi mangelen på integrasjon mellom prosedyrer og risikohåndtering kan bli et betydelig problem når det kommer til tekniske, driftsmessige og organisatoriske risikoer. Noen områder innenfor virksomheten	Sikkerhetsstyringssystemet er utviklet for å skape en systematisk og konsekvent tilnærming til håndteringen av risiko. Alle elementene er på plass og fungerer, og alle sikkerhetsaspekter vurderes. Sikkerhetskulturen tas i en viss grad til vurdering innenfor organisasjonen. Selv om organisasjonen er konsekvent, prøver den ikke å forutse risikoer på forhånd, og kulturen innenfor organisasjonen er heller ikke utviklet nok til å selvstendig opprettholde prosessen for risikohåndtering. Brannslokking har gitt etter for en mer veloverveid tilnærming til risikohåndtering, men det vil ikke ta veldig mye (f.eks. det å ikke håndtere viktige prosesser eller prosedyrer over tid) før organisasjonen faller tilbake til mestringsmodus.	Som for nivå 3, og i tillegg håndterer sikkerhetsstyringssystemet konstant risiko proaktivt. Her overvåker organisasjonen forløpere for risiko og iverksetter tiltak på forhånd for å forhindre at farlige hendelser oppstår. Organisasjonen er forpliktet til å utvikle en sikkerhetskultur, arbeidsstyrken er engasjert med virksomheten i å håndtere sikkerhet på en logisk og fremtidsrettet måte. På dette nivået er det virkelig ledelse fra toppen av organisasjonen, og de ansatte i organisasjonen har tro på og respekterer ledelsens tilnærming. Det går mye innsats i jevnlige gjennomganger av ytelse og å forstå naturen til risikoene organisasjonen står overfor, og hva som kan gjøres med det.	Som for nivå 4, og i tillegg er sikkerhetsstyringssystemet konstruert på en måte som muliggjør kontinuerlig forbedring. Organisasjonen søker aktivt ut muligheter til å forbedre sikkerhet, og utvikler positivt dens sikkerhetskultur ved å bruke informasjon fra både innenfor jernbanesektoren og utenfor den. Organisasjonen måler sin egen ytelse mot andres, både innenfor jernbanesektoren og utenfor. Det finnes bevis for at organisasjonen er klar over problemer den har eller kan ha i fremtiden, og prøver aktivt å håndtere dem gjennom SMS. På dette nivået er organisasjonen sikker på sin evne til å håndtere risikoene den møter, og ser utover for å lære opp de som den har kontakt med, og den prøver å ta lærdom fra andre felt som kan inkorporeres i virksomheten. Sikkerhet er en vesentlig del av organisasjonens virksomhet.

	entreprenører nødvendigvis tilstrekkelig kontrollert. På dette nivået skal NSA vurdere tiltak for å bringe organisasjonen tilbake til juridisk samsvar (se byråets veiledning for iverksettelse for mer informasjon om hvordan denne prosessen kan fungere).	yter bedre på sikkerhetsstyring enn andre. Risikoer kontrolleres mer av handlingene til personer som arbeider for organisasjonen, enn gjennom utformingen av SMS. En brannslokkingstilnærming til risikohåndtering er den normale situasjonen, noe som gjør at selskapet drives reaktivt til ulykker eller hendelser heller enn å proaktivt iverksette tiltak for å forhindre dem.