

Making the railway system
work better for society.

Vägledning

Mognadsmodell för säkerhetsstyrningssystem

	<i>Utarbetad av</i>	<i>Validerad av</i>	<i>Godkänd av</i>
<i>Namn</i>	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
<i>Position</i>	Projektansvarig	Projektledare	Enhetschef
<i>Datum</i>	29/06/2018	29/06/2018	29/06/2018
<i>Underskrift</i>			

Dokumenthistoria

<i>Version</i>	<i>Datum</i>	<i>Kommentar</i>
1.0	29/06/2018	Sista version för publicering

Detta dokument utgör en icke rättsligt bindande vägledning från Europeiska unionens järnvägsbyrå. Det har ingen inverkan på de beslutsprocesser som föreskrivs i tillämplig EU-lagstiftning. Europeiska unionens domstol är dessutom ensamt behörig att utfärda en bindande tolkning av unionsrätten.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

1 Inledning

Efter att ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd beviljats måste de nationella säkerhetsmyndigheterna (NSA) försäkra sig om att det säkerhetsstyrningssystem (SMS) som den sökande presenterat implementeras effektivt och fortsätter att uppfylla kraven i EU-rätten och i nationell rätt. Med andra ord måste de nationella säkerhetsmyndigheternas tillsyn av ett järnvägsföretags eller en infrastrukturförvaltares verksamhet säkerställa att det som angavs i ansökan om ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd överensstämmer med verkligheten. Denna modell har utarbetats av Europeiska unionens järnvägsbyrå (nedan kallad byrån) som ett verktyg för att bedöma mognad och förmåga hos en organisations säkerhetsstyrningssystem, och är avsedd att underlätta för nationella säkerhetsmyndigheter när de i sin tillsyn ska bedöma järnvägsföretagens och infrastrukturförvaltarnas säkerhetsstyrningssystem.

Mognadsmodellen kan även fungera som ett "fönster" in till en organisations säkerhetskultur och hjälpa de nationella säkerhetsmyndigheterna och organisationerna som de reglerar att diskutera hur dessa organisationer kan förbättra sina säkerhetsstyrningssystem.

Modellen har införts av byrån som vägledning. Det står de nationella säkerhetsmyndigheterna fritt att använda den eller låta bli. Om en nationell säkerhetsmyndighet har en annan motsvarande metod för att bedöma hur bra ett säkerhetsstyrningssystem fungerar, så kan den metoden användas. Ingenting i detta dokument innebär ett ifrågasättande av giltigheten hos andra modeller som uppnår samma resultat.

Det står också alla järnvägsföretag och infrastrukturförvaltare fritt att använda modellen på sin egen organisation närhelst de vill. Vägledningen är fritt tillgänglig och kan laddas ner från byråns webbplats tillsammans med det verktyg som behövs för att lägga in den insamlade datan i diagram. För att förenkla arbete i fält finns verktyget även i form av en app som kan laddas ner från Apple Store eller Google Play.

Byrån föreslår att ett järnvägsföretag eller en infrastrukturförvaltare använder modellen under hela femårsperioden för att göra sin egen bedömning, baserad på den tillsyn som gjorts, och granska resultaten i samband med ansökan om förnyelse av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd. Vid denna tidpunkt kan modellen användas för att belysa eventuella svaga områden i järnvägsföretagets eller infrastrukturförvaltarens säkerhetsstyrningssystem och ge organisationen tillfälle att åtgärda eventuella brister innan ansökan om ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd lämnas in.

1.1 Vägledningens syfte

De nationella säkerhetsmyndigheterna erbjuder i denna vägledning en enkel modell för att bedöma hur väl järnvägsföretagens och infrastrukturförvaltarnas säkerhetsstyrningssystem fungerar.

Modellen kategoriserar med hjälp av ett enkelt nivåsystem säkerhetsstyrningssystemets prestanda eller kapacitet så att man får den information som behövs för att göra en rimligt korrekt bedömning av en organisations hela säkerhetsstyrningssystem eller delar av det, beroende på vad den nationella säkerhetsmyndigheten beslutar sig för att titta på under tillsynen.

Observera att modellen tillämpas under tillsyn och att tillsyn endast kan utföras efter det att ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd har beviljats. Modellens värderingsskala utgår därför från en punkt där en organisation har underskridit den miniminivå som krävs för att ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd ska beviljas. En nationell säkerhetsmyndighet som i samband med tillsyn bedömer att en organisations mognad ligger på denna nivå (nivå 1 i modellen) förväntas vidta åtgärder för att göra något åt situationen. I de mest extrema fallen kan detta innebära att det gemensamma säkerhetsintyget eller säkerhetstillståndet återkallas eller att ärendet hänvisas till certifieringsorganet för säkerhetsintyg för

övervägande. Detta beror på att en ansökan om förnyelse av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd skulle avslås om en organisation presterar på denna nivå.

1.2 Vem är vägledningen till för?

Detta dokument vänder sig till

- *de nationella säkerhetsmyndigheterna när de bedömer järnvägsföretagens och infrastrukturförvaltarnas säkerhetsstyrningssystem under tillsynen av dessa,*
- *de nationella säkerhetsmyndigheterna när de utarbetar sin tillsynsstrategi och sin(a) tillsynsplan(er),*
- *de nationella säkerhetsmyndigheterna när de, vid gemensam eller samordnad tillsyn, utbyter information sinsemellan om säkerhetsnivån inom deras respektive medlemsstat,*
- *de nationella säkerhetsmyndigheterna när de utbyter information med byrån efter att en ansökan om förnyelse eller uppdatering har mottagits, i de fall byrån ansvarar för utfärdandet av det gemensamma säkerhetsintyget, och*
- *järnvägsföretagen och infrastrukturförvaltarna som ett verktyg för självutvärdering av prestandan hos deras säkerhetsstyrningssystem, i synnerhet innan de lämnar in en ansökan om förnyelse av sitt gemensamma säkerhetsintyg eller säkerhetstillstånd eller som en del av självövervakningen.*

1.3 Syfte och tillämpning

De nationella säkerhetsmyndigheterna behöver ha en metod att mäta kvaliteten på säkerhetsstyrningssystemet i praktiken jämfört med den teoretiska kvaliteten som presenteras under ansökningsstadiet för det gemensamma säkerhetsintyget eller säkerhetstillståndet. Byråns mognadsmodell för säkerhetsstyrningssystem kan fylla detta behov men det står varje enskild nationell säkerhetsmyndighet fritt att utarbeta en egen metod för att tillhandahålla sådan tillsynsinformation till byrån.

Modellen är inte avsedd att vara ett definitivt svar på frågan om hur bra ett enskilt säkerhetsstyrningssystem är, utan snarare ett sätt att ge stringens och struktur till den nationella säkerhetsmyndighetens bedömning i frågan.

1.4 Vägledningens uppbyggnad

Detta dokument ingår i byråns kompendium över vägledning till stöd för järnvägsföretag, infrastrukturförvaltare, nationella säkerhetsmyndigheter och byrån när de fullgör sina uppgifter och utför sina uppdrag i enlighet med direktiv (EU) 2016/798.



Figur 1: Kompendium över byråns vägledning

Byråns mognadsmodell för säkerhetsstyrningssystem har samma struktur som bilagorna I och II till kommissionens delegerade förordning (EU) 2018/762 för att man ska kunna göra en bedömning av kvaliteten hos en organisations säkerhetsstyrningssystem. Tre av kravområdena har i mognadsmodellen fått delvis andra rubriker än motsvarande kravområde för säkerhetsstyrningssystemet, detta för att möjliggöra appversionen av verktyget. Intentionen med respektive kravområde är dock densamma.

Modellen uppfyller också den nationella säkerhetsmyndighetens behov av ett verktyg som kan användas för att uppfylla de krav som anges i artikel 7.1 i kommissionens delegerade förordning (EU) 2018/761 för att utvärdera effektiviteten hos säkerhetsstyrningssystemet och artikel 5.2 i samma förordning för att utvärdera säkerhetsnivån i järnvägsföretagets eller infrastrukturförvaltarens säkerhetsstyrning.

Den strategi, som föreskrivs i artikel 5.2 syftar till att skapa en robust koppling mellan den bedömning som görs i samband med ansökan om gemensamt säkerhetsintyg eller säkerhetstillstånd och därpå följande tillsyn, den underlättar ett bättre informationsutbyte inom och mellan de nationella säkerhetsmyndigheterna och mellan de nationella säkerhetsmyndigheterna och byrån (det vill säga mellan de som utför tillsynen och de som utför bedömningen) och ger avslutningsvis större klarhet för järnvägssektorn när det gäller att förstå hur deras egen säkerhetsnivå påverkar de nationella säkerhetsmyndigheternas tillsyn (till exempel prioritering av tillsyn på de områden som har de största säkerhetsriskerna).

Vägledningens beskrivning av varje avsnitt av modellen inleds med att beskriva syftet med respektive avsnitt. Här förklaras vad avsnittet handlar om. För vissa avsnitt finns även några inledande kommentarer för att ge ytterligare klarhet. För varje avsnitt anges fem nivåer: Otillräcklig – nivå 1, Acceptabel – nivå 2, Konsekvent – nivå 3, Förebyggande – nivå 4 och Utmärkt – nivå 5. Till var och en av dessa nivåer hör en text som förklarar hur prestandan på denna nivå definieras jämfört med kriterierna. Användaren måste utvärdera de bevis som

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

har samlats in från intervjuer, dokumentgenomgångar och så vidare, och göra en bedömning av vilken nivå som bäst motsvaras av bevisen. Nivå 2 är den första nivå som anses uppfylla regelkraven. För nivåer över nivå 2 anges därför i texten att prestandan bör bedömas mot textens beskrivning av föregående nivå samt den aktuella nivån, så att nivå 4 omfattar faktorerna på nivå 3 samt de tillkommande faktorerna för nivå 4.

För att utifrån nivåerna för varje kriterium skapa en framställning av resultaten i diagramform måste användaren fylla i det kalkylblad i Excel som medföljer modellen som är tillgänglig på ERA:s hemsida, eller så kan användaren ladda ner byråns app som har den här funktionen inbyggd. När man fyller i siffrorna på kalkylblad 1 skapas radardiagrammet/spindelnätsdiagrammet i diagram 1. När det är färdigt kan det diagram som blir resultatet kopieras och klistras in i rapporten till järnvägsföretaget/infrastrukturförvaltaren.

Tabell 1, se nedan, visar ett alternativt sätt att presentera samma data genom att visa nivåerna med hjälp av ett trafikljussystem. Även denna kan, efter att den färdigställts, kopieras och klistras in i den slutliga rapporten till järnvägsföretaget/infrastrukturförvaltaren när denna är färdig. Om man ska använda det ena eller det andra eller båda sätten att presentera resultaten är ett val som görs av varje nationell säkerhetsmyndighet (eller järnvägsföretag/infrastrukturförvaltare).

1.5 Fyra saker man behöver veta innan man använder modellen

Det finns fyra saker man måste komma ihåg när man använder en modell av denna typ:

- 1) Modellen ger en ögonblicksbild av de delar av säkerhetsstyrningssystemet som man tittar på.
- 2) Den numeriska nivån är mindre viktig än vad som sägs i bedömningen av hur väl säkerhetsstyrningssystemet fungerar.
- 3) Eftersom resultaten från revisioner/inspektioner av enskilda delar av säkerhetsstyrningssystemet sannolikt varierar *kan resultaten användas som indikatorer som kan påverka den övergripande kapacitetsbedömningen* av ett järnvägsföretags eller en infrastrukturförvaltares genomsnittliga prestanda. När modellen används av utbildad personal ger den en bild av prestandan hos ett enskilt säkerhetsstyrningssystem och skapar därmed ett fokus för förbättringar av de områden där prestandan är mindre bra. På nationell nivå kan modellen även ge den nationella säkerhetsmyndigheten en övergripande bild över var deras resurser bör sättas in för att förbättra säkerheten, eftersom den till exempel kan visa att det finns en systemisk svaghet som är gemensam för hela järnvägsbranschen på ett särskilt säkerhetsstyrningsområde. Om alla järnvägsföretags resultat till exempel tyder på en låg nivå när det gäller riskbedömning kan detta utgöra ett viktigt underlag för den nationella säkerhetsmyndigheten vid utarbetandet av en tillsynsstrategi.
- 4) Det är av avgörande betydelse att både den nationella säkerhetsmyndigheten och den organisation som blir bedömd har en klar bild av insatsens omfattning och nivå när modellen används. Detta är ytterst viktigt eftersom det kommer att återspeglas i den grad av förtroende som man kan hysa för de omdömen som fälls av den nationella säkerhetsmyndigheten.

Innehåll

1	Inledning.....	2
1.1	Vägledningens syfte.....	2
1.2	Vem är vägledningen till för?	3
1.3	Syfte och tillämpning.....	3
1.4	Vägledningens uppbyggnad	3
1.5	Fyra saker man behöver veta innan man använder modellen.....	5
2	Mognadsmodellen och riskhantering.....	8
2.1	Vilken nivå i modellen kan godtas av en nationell säkerhetsmyndighet?	8
2.2	Tillämpning av modellen för nationella säkerhetsmyndigheter med olika rättsliga befogenheter..	8
2.3	Rapporter.....	9
2.4	Förutsättningar för att använda modellen	9
2.5	Hur använder man modellen?.....	9
3	Modellnivåer.....	14
3.1	Definition av uppnådda nivåer	14
3.2	Rapportering av modellens resultat.....	15
4	Mognadsmodellen för säkerhetsstyrningssystem.....	19
4.1	C – Organisationens förutsättningar	19
4.1.1	C1 Organisationen ska	19
4.2	L – Ledarskap	21
4.2.1	L1 – Ledarskap och åtagande	21
4.2.2	L2 – Säkerhetspolicy	24
4.2.3	L3 – Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen	25
4.2.4	L4 – Samråd med personal och andra parter	27
4.3	PL – Planering	29
4.3.1	PL 1 – Åtgärder för att hantera risker	29
4.3.2	PL2 – Säkerhetsmål och planering	31
4.4	S – Stöd	33
4.4.1	S1 – Resurser	33
4.4.2	S2 – Kompetens	34
4.4.3	S3 – Medvetenhet	36
4.4.4	S4 – Information och kommunikation	37
4.4.5	S5 – Dokumenterad information	39
4.4.6	S6 – Integrering av mänskliga och organisatoriska faktorer	41
4.5	OP – Verksamhet.....	43

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

4.5.1	OP1 – Operativ planering och styrning	43
4.5.2	OP2 – Styrning och kontroll av operativa tillgångar	45
4.5.3	OP3 – Entreprenörer, partner och leverantörer	47
4.5.4	OP4 – Hantering av ändringar	50
4.5.5	OP5 – Hantering av nödsituationer	51
4.6	PE – Utvärdering.....	53
4.6.1	PE1 – Övervakning	53
4.6.2	PE2 – Internrevision	55
4.6.3	PE3 – Ledningens genomgång	56
4.7	I – Förbättringar.....	58
4.7.1	I1 – Lärdomar av olyckor och tillbud	58
4.7.2	I2 – Kontinuerlig förbättring.....	60
	Bilaga – Vägledning rörande nivåer.....	62

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

2 Mognadsmodellen och riskhantering

Bedömningen av säkerhetsstyrningssystemet fungerar som ett indirekt mått på organisationens kapacitet att hantera riskerna i dess järnvägsverksamhet. Om säkerhetsstyrningssystemet fungerar väl är det rimligt att anta att riskerna som följer av organisationens verksamhet hanteras väl. Om organisationens säkerhetsstyrningssystem har svaga områden är detta en indikation på att riskerna på dessa områden inte hanteras tillräckligt väl, och som en följd av detta är det mer sannolikt att det på dessa områden finns omständigheter som kan leda till att olyckor eller tillbud inträffar, jämfört med andra områden där säkerhetsstyrningssystemet fungerar väl. Därför gäller att ju högre resultatet är enligt mognadsmodellen, desto bättre är riskhanteringen.

2.1 Vilken nivå i modellen kan godtas av en nationell säkerhetsmyndighet?

När man tittar på modellen nedan kan man anse att en organisation när den har nått nivå 3 vanligtvis fungerar på ett sätt som säkerställer att säkerhetsstyrningssystemet resulterar i en lämplig nivå av riskhantering och styrning. Detta är som synes en nivå högre än den som motsvarar miniminivån för regelefterlevnad (nivå 2). Det finns goda skäl för detta.

På miniminivån för regelefterlevnad finns det en konstant risk för att man halkar ner och hamnar på nivå 1, som underskrider denna miniminivå. En organisation som ligger på nivå 3 har naturligtvis större marginaler innan man hamnar på en oacceptabelt låg prestationsnivå. Det skulle dock vara fel av organisationerna att betrakta nivå 3 som den önskvärda nivån att uppnå. Syftet med modellen är att hjälpa den nationella säkerhetsmyndigheten tillsammans med ett järnvägsföretag eller en infrastrukturförvaltare diskutera svaga områden i deras säkerhetsstyrningssystem och var de kan **göra förbättringar**.

Eftersom de nationella säkerhetsmyndigheterna bör rikta in sina resurser där man ser de största riskerna kan myndigheten besluta att minska tillsynen av ett järnvägsföretag eller en infrastrukturförvaltare under en period om organisationen befinns prestera på modellens högre nivåer jämfört med ett järnvägsföretag eller en infrastrukturförvaltare som presterar på lägre nivåer och har behov av förbättringar. Detta kan utgöra ett incitament för järnvägsföretag och infrastrukturförvaltare att försöka förbättra sina säkerhetsstyrningssystem så att deras resultat når de högre nivåerna på skalan.

Det är också värt att påpeka att en del nationella säkerhetsmyndigheter som använder liknande modeller har gjort erfarenheten att användningen av olika nivåer skapar konkurrens mellan järnvägsföretagen om att bli "bäst i klassen" när det gäller säkerhetsstyrning, vilket kan uppmuntra till säkerhetsförbättringar i en medlemsstat. Detta kan också påverka deras förmåga att vinna nya kontrakt i framtiden, beroende på de affärsmöjligheter som finns att tillgå i de enskilda medlemsstaterna.

2.2 Tillämpning av modellen för nationella säkerhetsmyndigheter med olika rättsliga befogenheter

Modellen syftar till att hjälpa de nationella säkerhetsmyndigheterna att bedöma kapaciteten hos järnvägsföretagens och infrastrukturförvaltarnas säkerhetsstyrningssystem i enlighet med järnvägssäkerhetsdirektivet och de tillhörande förordningarna. Det bör dock noteras att utöver detta lagrum agerar de nationella säkerhetsmyndigheterna även inom ramen för de befogenheter som de har i enlighet med nationell lag. Detta betyder till exempel att vissa nationella säkerhetsmyndigheter ansvarar för att se till att arbetsmiljöfrågor hanteras på lämpligt sätt av järnvägsföretagen och infrastrukturförvaltarna inom deras medlemsstat medan andra inte gör det.

I modellen nedan tas därför inte arbetsmiljöfrågor upp i den vägledande texten. Om en nationell säkerhetsmyndighet väljer att tillämpa modellen på både säkerhets- och arbetsmiljöfrågor kan dock de grundläggande principer som kortfattat beskrivs nedan lätt tillämpas även på dessa faktorer.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

2.3 Rapporter

När en bedömning har gjorts kan man skriva en rapport som sammanfattar resultaten. I rapporten bör anges de bevis som leder till en slutsats rörande en viss nivå. Resultaten kan presenteras antingen i ett radardiagram/spindelnätsdiagram eller en trafikljusstabell. Syftet med rapporten är att kartlägga styrkor och svagheter och att ge en grund för diskussion med organisationen kring områden att förbättra under det gemensamma säkerhetsintygets eller säkerhetstillståndets giltighetstid. När man skriver rapporten bör bedömningens omfattning tydligt anges redan från början för att ge en förståelse av hur ingående den nationella säkerhetsmyndigheten har granskat arrangemangen i säkerhetsstyrningssystemets olika områden.

2.4 Förutsättningar för att använda modellen

All den personal hos de nationella säkerhetsmyndigheterna som använder modellen ska ha den kompetens som behövs för att använda den. För att använda modellen krävs att personalen hos de nationella säkerhetsmyndigheterna förstår både säkerhetsstyrningssystemets olika områden så som de beskrivs i bilagorna I och II till den gemensamma säkerhetsmetoden för säkerhetsstyrningssystem, och modellen i sig. Personalen behöver också ha god kunskap om lämpliga intervju- och inspektionstekniker och kunna hämta in en lång rad upplysningar från en mängd olika källor och hänföra dem till de relevanta avsnitten i säkerhetsstyrningssystemet. I praktiken bör man, där så är möjligt, göra dokumentgenomgångar innan man gör intervjuer på plats.

Mognadsmodellen har utarbetats för att kunna användas av en kompetent person, men det är god praxis att använda flera kompetenta personer som kan stödja varandra under tillsynens gång, både på grund av de logistiska svårigheterna med att utföra ett flertal intervjuer och för att ge ytterligare säkerhet vad gäller resultaten.

2.5 Hur använder man modellen?

Mognadsmodellen ersätter inte den bedömning som görs av personen som utför tillsynen. Den är snarare ett hjälpmedel för att göra denna bedömning och den möjliggör ett tydligare fokus och bättre kopplingar mellan bedömningen, de bevis som den bygger på och delarna i ett säkerhetsstyrningssystem. Den hjälper därför både dem som utför tillsynen att lägga fram sina resultat till järnvägsföretag och infrastrukturförvaltare, och järnvägsföretagen och infrastrukturförvaltarna att förstå varför dessa resultat har framkommit.

Om till exempel intervjuer, dokumentgenomgångar och fältarbete visar att en organisation inte har ett robust dokumenthanteringssystem kan detta flaggas som en svaghet i säkerhetsstyrningssystemet av den nationella säkerhetsmyndighet som utför tillsynen, och bevisen för detta kan diskuteras med organisationen och avhjälpande åtgärder kan gemensamt beslutas. Den nationella säkerhetsmyndigheten kan också använda svagheter i en organisations dokumenthanteringssystem för att lyfta fram problem med internrevision och övervakning, eftersom dessa borde ha identifierat sådana problem.

De olika rubrikerna i modellen motsvarar de olika delarna i säkerhetsstyrningssystemet så som detta beskrivs i bilagorna I och II till den gemensamma säkerhetsmetoden för krav på säkerhetsstyrningssystem. Detta betyder att det finns en direkt koppling mellan denna modell så som den används för övervakning, och den bedömning som görs av den nationella säkerhetsmyndigheten eller av byrån (i sin egenskap av certifieringsorgan för säkerhetsintyg) innan ett gemensamt säkerhetsintyg eller säkerhetstillstånd beviljas.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Detta betyder också att en noggrann och planerad användning av denna modell av en nationell säkerhetsmyndighet i samband med tillsyn kan fylla funktionen att bedöma om den organisation som har beviljats ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd har ett säkerhetsstyrningssystem som levererar vad det i ansökningen påstods kunna leverera under det gemensamma säkerhetsintygets eller säkerhetstillståndets giltighetstid.

Resultatet av mognadsmodellen är alltså viktig information för organisationen och för certifieringsorganet för säkerhetsintyg eftersom det är av relevans för ansökningar om förnyelse av gemensamma säkerhetsintyg eller säkerhetstillstånd. Det bör även noteras att säkerhetsstyrningssystemets element så som de beskrivs i denna modell alla har ett samband och utgör en helhet. När den nationella säkerhetsmyndigheten reflekterar över de övergripande resultaten kan den därmed fundera på säkerhetsstyrningssystemets prestanda inom de enskilda delarna, men även överväga vad detta betyder för säkerhetsstyrningssystemets prestanda överlag.

En nationell säkerhetsmyndighet kan använda mognadsmodellen omedelbart efter det att ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd har beviljats för att ge en bild av utgångsvärdet för prestandan hos ett säkerhetsstyrningssystem. Den information som inhämtas kan sedan utgöra grund för planering av tillsyn under återstoden av det gemensamma säkerhetsintygets eller säkerhetstillståndets giltighetstid.

Denna strategi kan vara lämplig om organisationen i fråga tidigare har haft ett gemensamt säkerhetsintyg/säkerhetstillstånd och därför har en viss resultathistoria när det gäller hur väl dess säkerhetsstyrningssystem fungerar. Att för en ny aktör på marknaden på samma vis genomföra tillsyn med hjälp av mognadsmodellen omedelbart efter att ett gemensamt säkerhetsintyg/säkerhetstillstånd beviljats ger inte nödvändigtvis mer information än vad som fanns att tillgå på bedömningsstadiet, eftersom säkerhetsstyrningssystemet är nytt och obeprövat.

Alternativt kan tillsynsmyndigheten, efter det att ett gemensamt säkerhetsintyg eller säkerhetstillstånd har beviljats, planera för användningen av mognadsmodellen under det gemensamma säkerhetsintygets eller säkerhetstillståndets giltighetstid baserat på all den information som har lämnats in av den bedömande myndigheten om områden av intresse för tillsynen, och då ta hänsyn till behovet av att sätta av tid för att pröva organisationens säkerhetsstyrningssystem i praktiken.

Det rekommenderas att den nationella säkerhetsmyndigheten använder resultaten från mognadsmodellen som indata för sin tillsynsstrategi (och därmed för sina tillsynsplaner). I praktiken kan detta betyda att mindre tillsyn ges till organisationer eller delar av organisationer som bedöms ha uppnått höga nivåer i mognadsmodellen än till organisationer som uppnår mer blygsamma nivåer totalt eller på särskilda områden.

Även om denna strategi är ett rimligt sätt att prioritera riskerna utifrån tillgänglig information, bör dessa risker ställas mot den relativa risken för hela verksamheten. Ett järnvägsföretag som specialiserar sig på transport av farligt gods kan till exempel nå nivå 4 och 5 i mognadsmodellen och kan därför anses ha ett mycket välutvecklat säkerhetsstyrningssystem, men det kan ändå vara lämpligt att utföra en omfattande tillsyn av detta på grund av den typ av risker som förknippas med verksamheten.

Det är sällan som bevisen man hittar vid en tillsyn av ett område ger en helt samstämmig bild av hur väl organisationens säkerhetsstyrningssystem fungerar på det aktuella området. Ofta hittar man såväl positiva som negativa sidor. När man tilldelar området en nivå baserat på bevisen måste man därför fatta ett beslut om man ska tilldela en högre eller lägre nivå på skalan. Det står klart att man måste fatta ett beslut genom att väga de bevis som finns mot varandra. Om denna avvägning lutar mot en högre i stället för en lägre nivå bör detta avspeglas i det beslut som fattas. Om bevisen pekar åt olika håll ska antingen den som utför tillsynen försöka hitta fler bevis under pågående och/eller framtida tillsynsaktiviteter (till exempel verklighetskontroller/inspektioner) riktade mot det aktuella området för att utifrån dessa kunna fatta ett mer

korrekt beslut, eller så ska en lägre nivå tilldelas på grund av att det inte finns bevis som stöder bedömningen av en högre nivå.

Vid det avslutande mötet med järnvägsföretaget/infrastrukturförvaltaren kan man alltid ta upp svårigheten med att fatta ett beslut och ge järnvägsföretaget/infrastrukturförvaltaren möjlighet att lämna in ytterligare bevis. Man bör dock vara försiktig när man gör detta. Det bör vara undantag snarare än regel, eftersom följden av att tillåta ytterligare bevis kan vara att järnvägsföretaget/infrastrukturförvaltaren åtgärdar saker på detta stadium hellre än att åtgärda dem inom ramen för den handlingsplan som följer på tillsynen.

Frågan om hur mycket bevis det krävs för att fatta ett korrekt beslut är svår att besvara. Bevisen utgörs i de flesta fall av en kombination av intervjuer, skriftlig bevisning, fältobservationer och resultat från utredningar av tillbud/olyckor för givna tider, datum och platser. Beslutet måste vara baserat på de bevis som har hittats, så att om järnvägsföretaget/infrastrukturförvaltaren hävdar att det som har hittats inte är representativt ändrar detta inte resultatet eftersom det som har hittats de facto har hittats. Att det var möjligt att hitta en situation som järnvägsföretaget/infrastrukturförvaltaren inte känner igen är i sig ett tecken på att det finns problem med hur säkerhetsstyrningssystemet fungerar. Att järnvägsföretaget/infrastrukturförvaltaren bestrider detta är också ett tecken på att saker och ting inte står rätt till.

Om ett antal bevis pekar på att ett område som undersöks är välkött är detta ett välgrundat skäl för att sluta söka efter ytterligare bevis. Om däremot bevisen inte ger denna försäkran men det är omöjligt att avgöra varför bör man försöka hitta ytterligare bevis. Det är inte nödvändigt att undersöka allt, från processer och förfaranden på en hög nivå till detaljerade arbetsanvisningar, för att dra slutsatser rörande huruvida systemet fungerar på ett effektivt sätt. Tillräckligt mycket information från dokumentgenomgångar och intervjuer måste inhämtas för att dra rimligt säkra slutsatser om hur verkligheten ser ut i praktiken.

Man bör komma ihåg att en rapport som baseras på mognadsmodellen till syvende och sist har utarbetats av en kompetent person som använder modellen som stöd för sitt professionella omdöme, och eftersom den bygger på ett urval av dokument, intervjuer och annan information är det osannolikt att den någonsin kan ge en fullständig bild av en organisations prestanda eftersom detta skulle kräva att man granskar varje uppgift som rör organisationen och intervjuar varje person som arbetar för den och alla organisationer som samverkar med den.

Vad man i allmänhet försöker hitta är bevis för att det område som undersöks

- a) styrs på ett säkert sätt och
- b) att denna styrning är konsekvent och överensstämmer med det sätt på vilket säkerhetsstyrningssystemet är avsett att fungera enligt vad organisationen uppgivit vid sin ansökan om ett gemensamt säkerhetsintyg eller säkerhetstillstånd, och
- c) att organisationen är medveten om hur dess verksamhet styrs och fungerar.

Om a) förekommer utan b) eller c) kan det sägas att säkerheten styrs av ren tur snarare än av en konsekvent plan, något som klart tyder på ett bristfälligt säkerhetsstyrningssystem.

Det är ytterst viktigt att man, när man lägger fram resultaten för den organisation som har bedömts, klagör hur ingående bedömningen har varit. De bevis som har undersökts och de personer som har intervjuats bör anges i rapporten. Om man har hittat exempel på bristfälligt dokumentation bör dessa också bifogas rapporten.

Om modellen används för att bedöma särskilda områden av säkerhetsstyrningssystemet bör de områden som inte bedöms tydligt anges i avsnittet om studiens omfattning och bör inte tilldelas en nivå i slutrapporten, såvida inte tillräckliga bevis framkommer från de områden som omfattas av studien för att lämna synpunkter på de områden som inte bedöms. När man studerar förvaltning av tillgångar kan det till exempel framkomma att det finns ett svagt kompetensstyrningssystem. I en revision som använder

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

mognadsmodellen skulle det i ett sådant fall vara befogat att bedöma en nivå till detta område även om det inte utgjorde huvudfokus för revisionen.

Den eller de som utför tillsynen bör göra tillräckligt många intervjuer/dokumentgenomgångar och tillräckligt mycket fältarbete för att försäkra sig om att de har god överblick över verksamheten. Bilden behöver inte vara komplett men man behöver samla in tillräckligt med bevis för att motivera järnvägsföretagets/infrastrukturförvaltarens placering i modellen. För ett litet järnvägsföretag eller en liten infrastrukturförvaltare kan det räcka med intervjuer med den högsta ledningen samt ett mindre antal ur övrig personal för att fastställa organisationens placering, till exempel med avseende på ledarskap. För ett stort järnvägsföretag eller en stor infrastrukturförvaltare med verksamhet på flera olika platser och en ledningsstruktur med flera olika nivåer kan det vara svårare att skapa sig en komplett bild, och fler val måste göras när det gäller vem som ska intervjuas på hög nivå. Under dessa omständigheter skulle det kunna vara befogat att titta på organisationen i genomsärning uppifrån och ned, kanske på årlig basis, och då titta på olika områden varje gång och intervju ett lämpligt antal personer på varje ledningsnivå för att kunna bilda sig en väl övervägd uppfattning om ämnesområdet.

För stora och komplexa organisationer är det lämpligt att använda modellen för att skapa en övergripande bild av hur organisationen sköts, till exempel genom att titta på dokumentationen på hög nivå och intervju högre chefer, innan man använder modellen för att titta på skilda aspekter av verksamheten, till exempel fordonsunderhåll vid ett antal olika anläggningar. Om det gäller en välskött organisation med ett bra säkerhetsstyrningssystem så bör det vara möjligt att se att uppfattningen/dokumentationen på hög nivå avspeglas på samma sätt i var och en av de underhållsverkstäder som man tittar på. Detta innebär inte att det inte kan finnas skillnader mellan de olika verkstäderna, bara att den övergripande strukturen i sina nyckelaspekter är likadan och drivs på samma sätt. På samma sätt skulle man för en lågpresterande organisation förvänta sig att se skillnader mellan den uppfattning som den övergripande ledningen har om hur organisationen sköts på central nivå för underhållsverkstäderna och uppfattningen vid själva verkstäderna, såväl som betydande skillnader mellan de olika verkstäderna som kan omvandlas till säkerhetsrisker, till exempel skillnader i besiktningens frekvensen för liknande fordon utan någon förklaring till varför, samtidigt som ledningen endast är medveten om en enda sådan underhållsstruktur.

Numreringssystemet i modellen finns till för att underlätta kategoriseringen av organisationens mognad. Att erhålla en viss poäng ska inte ses som ett självändamål. När man presenterar resultaten för ett järnvägsföretag/en infrastrukturförvaltare är det mycket viktigt att man klargör detta och betonar att resultaten utgör uppfattningen hos den person som utför tillsynen och baseras på de bevis som hittats vid en särskild tidpunkt och på en särskild plats.

Man kan förvänta sig ett visst motstånd från järnvägsföretag eller infrastrukturförvaltare och att de antingen ifrågasätter "nivån" – och det är då viktigt att betona att detta är den nationella säkerhetsmyndighetens uppfattning baserad på de bevis man kunnat iaktta, och att företagen och förvaltarna har rätt till en annan uppfattning baserad på deras egen kunskap om organisationen – eller att de försöker hantera saken genom att tillhandahålla ytterligare bevis – och man måste då välja om man ska godta detta, som nämndes ovan, och modifiera resultaten som en följd av detta, eller om man ska påpeka att resultaten är de som framkom vid en särskild tidpunkt. Eventuella bevis som lämnas in efter tillsynen och som ger en mer positiv uppfattning bör i allmänhet lämnas in som en del av bevismaterialet för att fullborda den handlingsplan som har avtalats mellan organisationen och den nationella säkerhetsmyndigheten.

Vid det avslutande mötet bör man framhålla att syftet med övningen är att hjälpa järnvägsföretaget/infrastrukturförvaltaren att förbättra sitt säkerhetsstyrningssystem. Handlingsplaner bör fastställas för att åtgärda eventuella brister i uppfyllandet av lagstiftningen, det vill säga på nivå 1, och förslag till förbättringar bör fastställas för nivå 2 och däröver. Dessa bör överenskommas med järnvägsföretaget/infrastrukturförvaltaren, och järnvägsföretaget/infrastrukturförvaltaren bör förbinda sig

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

att utarbeta en tidssatt handlingsplan för genomförandet av dessa punkter, inklusive detaljer om vem som ansvarar för vad och när ändringarna senast bör genomföras, så att den nationella säkerhetsmyndigheten i tillämpliga fall kan göra uppföljningar.

Modellen finns till för att hjälpa till med utförandet av tillsynen, inte för att ersätta någons professionella omdöme. Den gör inte anspråk på att ge det exakta svaret på vad som upptäcks under tillsynen, och inte heller visar den vad som ska göras åt det. Det är den nationella säkerhetsmyndighetens sak att utifrån sina rättsliga befogenheter besluta om eventuella åtgärder som kan vidtas efter att tillsyn utförts med hjälp av modellen, men dessa åtgärder ska klart och tydligt utgå från de bevis som har uppdagats under revisionen. Byrån har utarbetat en vägledning till en modell för åtgärder vid tillsyn för att hjälpa de nationella säkerhetsmyndigheterna att räkna ut vilka åtgärder som kan vara lämpliga.

Modellen kan också användas för att titta på resultat från olycksutredningar eller från ett företags interna revisionsrapporter. I detta fall bör resultaten i rapporten analyseras för att se vad de säger om säkerhetsstyrningssystemet. Utifrån den tillämpliga kravbilden kan en bedömning av organisationens mognad göras med hjälp av modellen baserat på resultaten i revisions- eller olycksrapporten. En enda rapport säger kanske inte så mycket om kapaciteten hos organisationens säkerhetsstyrningssystem, men om denna övning genomförs en gång per år eller vartannat år och man kan undersöka flera rapporter kan detta vara en effektiv metod för att identifiera områden i organisationens säkerhetsstyrningssystem där problem hela tiden uppstår.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

3 Modellnivåer

Den struktur som används är en skala mellan 1 och 5 där 1 står för svag prestanda hos styrningssystemet och 5 står för en utmärkt styrningsprestanda.

3.1 Definition av uppnådda nivåer

Nivå 1 – Otillräcklig

På denna nivå har den bedömda organisationen ett säkerhetsstyrningssystem, men det står klart att det finns brister som drar ner prestandanivån till under vad som krävs för beviljandet av ett gemensamt säkerhetsintyg eller säkerhetstillstånd. Det finns förfaranden och anvisningar för styrning av verksamhetens säkerhet, men under tillsynen står det klart att det finns allvarliga problem i hur sammanhängande dessa är som helhet. Enskilda risker hanteras, men de övergripande processerna som styr detta är bristfälliga. Organisationen fungerar i praktiken på ett sätt som förefaller att ha stora brister i överensstämmelsen med vad som beskrivs i säkerhetsstyrningssystemet.

Policyer, förfaranden och anvisningar tycks tillämpas på sätt som inte stämmer överens med vad som anges i säkerhetsstyrningssystemet, och därför hanteras inte nödvändigtvis de risker som följer av organisationens och dess entreprenörers verksamhet på lämpligt sätt. På denna nivå bör den nationella säkerhetsmyndigheten överväga att vidta åtgärder för att få organisationen att åter uppnå regelefterlevnad (se byråns vägledning till en modell för åtgärder vid tillsyn för mer information om hur denna process kan fungera).

Nivå 2 – acceptabel

På denna nivå presterar organisationen på miniminivån för regelefterlevnad, det vill säga säkerhetsstyrningssystemet fungerar på en nivå tillräcklig för att ett gemensamt säkerhetsintyg eller säkerhetstillstånd skulle beviljas på bedömningsstadiet. Det finns ett skriftligt säkerhetsstyrningssystem som används för att styra säkerhetsrisker, men det har brister när det gäller struktur och samordning. Systemet är sammanhängande i det stora hela, men det finns luckor och en del bristande överensstämmelse vad gäller strategin på olika områden.

Organisationen klarar i huvudsak av att uppfylla sina skyldigheter när det gäller säkerhet, men med knapp nöd. Det skulle inte behövas mycket för att betydande problem skulle skapas och organisationen skulle falla tillbaka till nivå 1 på grund av att bristen på integrering mellan förfaranden och riskhantering kan bli ett stort problem när det gäller tekniska, mänskliga och organisatoriska risker. En del områden inom verksamheten klarar sig bättre när det gäller säkerhetsstyrning än andra. Riskerna begränsas mer genom organisationens anställdas handlingar än genom säkerhetsstyrningssystemets utformning. En brandsläckningsstrategi för riskhantering är mer regel än undantag, vilket gör att företaget agerar reaktivt när det gäller olyckor och tillbud i stället för att proaktivt vidta åtgärder för att förhindra att de inträffar.

Nivå 3 – konsekvent

Säkerhetsstyrningssystemet har utarbetats för att skapa en systematisk och konsekvent strategi för riskhantering. Alla delar är på plats och fungerar, och alla säkerhetsaspekter har beaktats. Man har tagit viss hänsyn till förbättringar av säkerhetskulturen inom organisationen genom att utarbeta en förbättringsstrategi för säkerhetskultur. Samtidigt som organisationen har ett konsekvent arbetssätt försöker man inte förebygga risker i förväg och inte heller är kulturen inom organisationen tillräckligt utvecklad för att riskhanteringsprocessen ska vara självgående. Brandsläckningsstrategin har ersatts av en mer väl övervägd strategi för riskhantering, men det skulle inte behövas mycket (till exempel brister i styrningen av centrala processer eller förfaranden över tid) för att organisationen skulle falla tillbaka till nivån acceptabel.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Nivå 4 – förebyggande

Som nivå 3 samt att säkerhetsstyrningssystemet kontinuerligt hanterar risker på ett proaktivt sätt. Här övervakar organisationen förebud till risker och vidtar där det är möjligt åtgärder i förväg för att förhindra att farliga incidenter uppkommer. Organisationen har bestämt sig för att utveckla en säkerhetskultur, och de anställda är delaktiga i organisationens arbete med att styra säkerheten på ett konsekvent och framåtsyftande sätt. På denna nivå förekommer det verkligt ledarskap från organisationens ledning och personalen tror på och respekterar ledningens strategier. Mycket arbete läggs ner på regelbundna genomgångar av verksamhetens prestationer och på att förstå de risker som organisationen möter och vad som kan göras åt dem.

Nivå 5 – utmärkt

Som nivå 4 samt att det skriftliga säkerhetsstyrningssystemet har utformats på ett sätt som möjliggör kontinuerliga förbättringar. Organisationen söker aktivt efter möjligheter att förbättra säkerheten och utvecklar sin säkerhetskultur på ett positivt sätt med hjälp av information både inifrån järnvägsbranschen och utifrån. Organisationen jämför sin egen prestanda med andra organisationers, både inom och utanför järnvägssektorn. Det finns bevis för att man i organisationen är medveten om de problem som organisationen har eller kan komma att ha i framtiden och aktivt försöker hantera dem genom säkerhetsstyrningssystemet. På denna nivå är organisationen trygg i sin förmåga att hantera de risker som uppkommer och vänder sig utåt för att utbilda dem som organisationen samverkar med, och man försöker dessutom att förbättra säkerheten genom att lära sig av andra verksamhetsområden. Säkerhet är en integrerad del av organisationens verksamhet.

3.2 Rapportering av modellens resultat

Modellens resultat kan presenteras i ett radardiagram eller som ett trafikljussystem, som i exemplen i

Figur 2 och Tabell 1 nedan. I båda fallen visualiseras organisationens mognad uttryckt genom de fem mognadsnivåerna för vart och ett av områdena i kommissionens delegerade förordning (EU) 2018/762. Härigenom får man en klar och tydlig bild av organisationens säkerhetsnivå.



Figur 2: Exempel på presentation av modellens resultat i ett radardiagram/spindelnätsdiagram.

Radardiagrammet kan fyllas i med hjälp av byråns app ERA SMS som finns tillgänglig på Apple Store och Google Play eller via en länk på byråns webbplats. Alternativt finns ett Excel-kalkylblad också tillgängligt på byråns webbplats.

Tabell 1: Trafikljussystem indelat per nivå.

Inslag av PDCA-modellen (Planera–Göra–Studera– Agera) i säkerhetsstyrningssystemet	Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5
Organisationens förutsättningar					
Organisationen ska					
Ledarskap					
Ledarskap och åtagande					
Säkerhetspolicy					
Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen					
Samråd med personal och andra parter					
Planering					
Åtgärder för att hantera risker					
Säkerhetsmål och planering					
Stöd					
Resurser					
Kompetens					
Medvetenhet					
Information och kommunikation					
Dokumenterad information					
Integrering av mänskliga och organisatoriska faktorer					
Verksamhet					
Operativ planering och styrning					
Styrning och kontroll av operativa tillgångar					
Entreprenörer, partner och leverantörer					
Hantering av ändringar					
Hantering av nödsituationer					
Utvärdering					
Övervakning					
Internrevision					
Ledningens genomgång					
Förbättring					
Lärdomar av olyckor och tillbud					

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Tabell 1: Trafikljussystem indelat per nivå.

Inslag av PDCA-modellen (Planera–Göra–Studera– Agera) i säkerhetsstyrningssystemet	Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5
Kontinuerlig förbättring					

Man bör dock vara medveten om att gränserna mellan de olika nivåerna är tydliga när det gäller övergången från nivå 1 till nivå 2 eftersom nivå 1, till skillnad från nivå 2, inte uppfyller minimikraven för regelefterlevnad. Övergången från gult till grönt när man rör sig från 2 till 3 är dock en mer oklar gräns eftersom organisationen i båda fallen efterlever regelkraven samtidigt som förändringen innebär att man förbättrar kvalitet och prestanda hos sitt säkerhetsstyrningssystem.

För att kunna använda denna modell måste den organisation som tillsynas ha ett gemensamt säkerhetsintyg eller säkerhetstillstånd eftersom tillsyn endast kan ske efter det att ett sådant har beviljats. Syftet med modellen är att hjälpa den person som utför tillsynen att bedöma hur bra säkerhetsstyrningssystemet är i praktiken. Nivå 1 anses vara en nivå som understiger miniminivån för regelefterlevnad och på denna nivå är det därför nödvändigt med förbättringar för att undvika att den nationella säkerhetsmyndigheten utdömer påföljder på grund av att de villkor för vilka det gemensamma säkerhetsintyget eller säkerhetstillståndet beviljades inte uppfylls.

Från och med nivå 2 (miniminivån för regelefterlevnad) och uppåt representerar varje nivå en högre grad av utveckling. Av detta skäl ska man inte i avsnittet nedan se nivå 2 som kumulativ men det ska man för nivåerna 3–5, dvs. när man når nivå 2 uppfyller man de grundläggande regelkraven. På nivå 3 har man nått en rimlig och konsekvent standard för sitt säkerhetsstyrningssystem och kan vidmakthålla denna standard över tid så att man kan bygga vidare på sitt säkerhetsstyrningssystem för att nå högre nivåer. Med hjälp av trafikljussystemet kan man lätt se i grova drag att nivå 1 (rött) motsvarar otillräcklig prestanda, nivå 2 (gult) är acceptabel, och när man övergår till nivåerna 3, 4 och 5 (grönt) är prestandan konsekvent, förebyggande respektive utmärkt.

I bilagan kan man för tydlighetens skull se trafikljusfärgerna inlagda i femnivåsystemet, med allmänna beskrivningar som visar hur varje nivå ser ut i praktiken. Pilen under tabellen är en påminnelse om att gränserna mellan nivåerna inte är fasta:

- **Grönt** när bedömningen motsvarar nivåerna 3, 4 och 5 och prestandan anses vara konsekvent, förebyggande eller utmärkt,
- **Gult** för nivå 2, där prestandan anses vara acceptabel,
- **Rött** för nivå 1, där prestandan anses vara otillräcklig.

4 Mognadsmodellen för säkerhetsstyrningssystem

4.1 C – Organisationens förutsättningar

Syfte

För att få ett gemensamt säkerhetsintyg eller säkerhetstillstånd måste sökanden beskriva typ av verksamhet, omfattningen av och området för sin verksamhet, visa hur man identifierar de allvarliga risker man står inför, identifierar berörda parter, beskriva hur man uppfyller sina rättsliga säkerhetsförpliktelser och vilka de är, samt förklara omfattningen av sitt säkerhetsstyrningssystem. Syftet med detta är att klargöra verksamhetens omfattning och storlek för bedömaren. Från ett tillsynsperspektiv är det viktigt att kontrollera att den information som den sökande angav i samband med ansökan om gemensamt säkerhetsintyg eller säkerhetstillstånd, till exempel förståelsen av risker och uppgifter om hur de hanteras i organisationens säkerhetsstyrningssystem, faktiskt avspeglas i den dagliga driften av företaget.

Inledande kommentarer

Det är av avgörande betydelse att en organisation kan ge certifieringsorganet för säkerhetsintyg korrekt information om typ av verksamhet, omfattningen, och området för verksamheten eftersom dessa faktorer fastställer gränserna för verksamheten, vilket bör återspeglas i organisationens säkerhetsstyrningssystem. Denna faktor utgör det första bland beslutskriterierna, eftersom den utgör grunden för de övriga kriterierna. Från ett tillsynsperspektiv är det därför mycket viktigt att den faktiska verksamheten återspeglar vad som angivits vid tiden för bedömningen, eftersom man annars måste dra slutsatsen att bedömningen gjordes på grundval av ett ofullständigt underlag. Beskrivningen av organisationens förutsättningar kan också indikera hur mänskliga och organisatoriska faktorer hanteras.

Att identifiera allvarliga risker betyder i detta fall att sökanden ska kunna visa att dennes organisation baserat på den egna analysen är medveten om vilka risker som är viktigast av de risker den står inför. Detta bidrar till att fastställa det sammanhang som organisationen verkar inom och visar den bedömande myndigheten att organisationen förstår miljön i vilken den är verksam. Aktiviteter hos parter som står utanför järnvägssystemet kan också påverka verksamhetens säkerhet, och måste därmed också övervägas i riskbedömningen.

4.1.1 C1 Organisationen ska

Nivå 1 - otillräcklig

På denna nivå har organisationen beskrivit typ av verksamhet, omfattning, område för verksamheten och/eller beskaffenhet tämligen tydligt. I praktiken tycks det dock finnas skillnader mellan verksamhetens faktiska omfattning och vad som angivits i samband med ansökan, och det är oklart om alla allvarliga risker har registrerats på lämpligt sätt. Det är oklart om organisationen på ett effektivt sätt efterlever alla de rättsliga bestämmelser som den påstår sig efterleva. Det verkar inte som om säkerhetsstyrningssystemet avspeglar alla berörda parter på lämpligt sätt.

Nivå 2 - acceptabel

På denna nivå finns alla grundläggande beskrivningar på plats, men det finns farhågor om att verksamhetens omfattning och skala inte har beskrivits korrekt. En kartläggning av rättsliga och andra krav som påverkar de berörda parterna har gjorts, men det finns problem med den. Det finns en del berörda parter som inte omfattas av det ursprungliga underlaget för säkerhetsstyrningssystemet och det finns bevis på att allvarliga risker ibland inte styrs i tillräckligt hög grad, med påföljande konsekvenser för säkerhetsstyrningssystemets effektivitet.

Nivå 3 - konsekvent

Som nivå 2 samt att på denna nivå stämmer beskrivningen av verksamheten, säkerhetsstyrningssystemet och de allvarliga risker som förekommer överens med vad som kan ses i praktiken. Det står klart att organisationen är medveten om vad den gör och den riktning den rör sig i. Det finns en tydlig uppfattning om vilken lagstiftning som gäller och vilka de berörda parterna är.

Nivå 4 - förebyggande

Som nivå 3 samt att organisationen strävar efter att utvecklas och lära sig att beskriva sig själv på ett bättre sätt till berörda parter och samarbeta med dem för att utarbeta säkrare förfaranden och processer inom ramen för sitt säkerhetsstyrningssystem. Hellre än att bara räkna upp den lagstiftning som den måste efterleva försöker organisationen aktivt samarbeta med de relevanta regleringsmyndigheterna för att utarbeta strategier för att uppfylla regelkraven. Man har en klar uppfattning om gränserna till andra delar av verksamheten och hanterar dessa på ett tydligt sätt.

Nivå 5 - utmärkt

Som nivå 4 samt att organisationen framstår som ett gott föredöme för andra organisationer. Den har insikt om sina egna egenskaper och sina rättsliga förpliktelser och försöker utvecklas genom att bygga vidare på sina starka sidor och dra nytta av erfarenheter både inom järnvägsbranschen och utanför denna.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

4.2 L – Ledarskap

Syfte

Att se till att organisationen styrs och leds på ett effektivt sätt.

Att se till att säkerhetspolicyn tydligt uttrycker den högsta ledningens förväntningar, korrekt fastställer vad organisationen vill åstadkomma, hur den vill åstadkomma det (genom de beteenden som uppvisas med avseende på ledarskap) och hur ledningen ska kunna veta när dessa förväntningar uppnås. Effektivt ledarskap kan uppfattas som att tillhandahålla vägledning, organisation och resurser, och som förmågan att ingjuta rätt kultur i verksamheten för att uppnå de önskade målen. Ledningen bör sköta verksamheten effektivt så att säkerhetsmålen inte äventyras på grund av rivaliserande affärsprioriteringar. Ledningen bör göra klart för personalen vilka säkerhetsmålen är och hur de ska uppnås.

Att se till att organisationen (i synnerhet styrelsen) på ett effektivt sätt ifrågasätter om en säkerhetspolicy och den verksamhet som är knuten till den är korrekt, att den har införts och är verkningfull. Att se till att budskapen är konsekventa, tydliga och utformade för att skapa den bästa miljön för säkerhetsstyrning.

Inledande kommentarer

Dåligt ledarskap har varit orsak till många uppmärksammade misslyckanden på säkerhetsområdet. En organisations förhållning till säkerhet återspeglar ofta inställningen hos dem som tar affärsbesluten och den påverkar åsikterna och inställningen hos organisationens personal.

Den övergripande policyn, den verksamhet som är knuten till denna och det säkerhetsklimat som följer därav och som har införts av den högsta ledningen är av yttersta betydelse för att skapa och vidmakthålla organisationens förhållningssätt till säkerhet. Denna policy bör ge en tydlig förståelse av hur organisationen avser att hantera säkerheten. Den högsta ledningen och annan ledningspersonal bör även föregå med gott exempel och agera på sätt som förstärker de budskap som policyn innehåller. Järnvägssäkerheten bör vara integrerad i verksamheten.

4.2.1 L1 – Ledarskap och åtagande

Ledarskap och åtagande handlar om att organisationens ledning pekar ut riktningen och utarbetar en positiv och framåtsyftande agenda för den personal som arbetar för dem som ett led i styrningen av risker i alla organisationens affärsprocesser. Ledningen skapar organisationens kultur och anger tonen för hur organisationen beter sig, både internt och gentemot dem den samverkar med. De som sitter i ledningspositioner är de som har det största inflytandet på organisationens kultur och struktur och på att organisationen sköts på ett effektivt sätt, och det är därför av avgörande betydelse att de kan förmedla sitt budskap till sin personal. När personal från den nationella säkerhetsmyndigheten bedömer detta område under tillsyn bör de där så är möjligt överväga om det finns motstridiga prioriteringar mellan säkerhetsstyrning och andra affärsprocesser.

Nivå 1 – Otillräcklig

Förfaranden och säkerhetsmål är föråldrade och har inte förmedlats inom organisationen, och det finns få bevis för att det finns en förståelse för dem.

Det finns inga bevis på att personalen rådfrågas om säkerhetsfrågor och avståndet är stort mellan personalen och ledningen.

Säkerhetsstyrningssystemet finns på en mycket förenklad nivå (även om hänsyn tas till mänskliga faktorer är till exempel det system som har införts för att göra detta bristfälligt) och är inte kopplat till organisationens löpande verksamhet.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Det finns få bevis för att ledningen på olika nivåer har något intresse av säkerhetsfrågor. Produktionen är viktigare för dem. Det är svårt att få resurser till att ta itu med riskhanteringsfrågor, eftersom organisationen inte sätter något värde på vikten av att använda resurser på detta sätt.

Det finns brister i förståelsen för människornas betydelse för säkerheten, effektiviteten och kvaliteten i verksamheten.

Ledningen engagerar sig inte i säkerhetskulturen och det finns brister i organisationens kunskaper i fråga om säkerhetskultur som begrepp eller om skälen till varför säkerhetskulturen är viktig för att åstadkomma en säker och effektiv organisation. Säkerheten uppfattas som skild från organisationens affärs mål och definieras som efterlevnad av föreskrifter och som tekniska och förfarandemässiga lösningar. Säkerheten hanteras och styrs av en fristående säkerhetsavdelning som uppfattas som primärt ansvarig för organisationens säkerhetskultur. Ledningens engagemang för och förmedling av säkerhetsmål och prioriteringar är begränsade till den grad att dessa är okända i organisationen. Säkerheten uppfattas som något som måste göras, hellre än något som organisationen har nytta av. Strävan efter en positiv säkerhetskultur saknas till stor del i organisationens ledarskap.

Incidenter och olyckor "kommer alltid att hända" – en fatalistisk kultur dominerar. Den mänskliga faktorn och fel som begåtts av personer som är direkt inblandade fastställs alltid som orsak och det görs inga försök att driva utredningarna vidare. Det finns ingen rättvisekultur och de personer som är inblandade i incidenter och olyckor görs ofta till syndabockar. Ledningen och personalen är i allmänhet ointresserade av säkerhet och använder eventuellt säkerhet endast som grund för andra argument, såsom lön, arbetstid, osv.

Prestationsnivån understiger miniminivån för regelefterlevnad och den nationella säkerhetsmyndigheten bör därför överväga hur organisationens prestanda kan höjas till den miniminivå som krävs.

Nivå 2 – acceptabel

Det finns en brist på samband mellan säkerhetsrelaterade processer och affärsprocesser.

Ledningen tillhandahåller otillräckliga resurser för att skapa ett engagemang för att bidra positivt till organisationens säkerhet och kultur.

Ledarskap uppfattas som viktigt för säkerhetsstyrningen, men det avspeglas i säkerhetsstyrningssystemet på ett något inkonsekvent och rörigt sätt.

Säkerhet uppfattas som en affärsrisk som kan ha negativa konsekvenser för organisationens finansiella mål. Även på denna nivå definieras säkerhet som efterlevnad av föreskrifter och som tekniska och förfarandemässiga lösningar. Det allmänna förhållningssättet till säkerhet är reaktivt, från högsta ledningen ner till verkstadsgolvet. Ledningens engagemang ses som halvhjärtat – de reagerar när något har gått fel snarare än att vidta proaktiva åtgärder för att förbättra förhållandena.

Strategin för mänskliga och organisatoriska faktorer i säkerhetsstyrningen stöds av ledningen och genomgångar av den förekommer. Detta görs dock mera för att uppfylla regelkrav än för att man har någon verklig förståelse för betydelsen av mänskliga och organisatoriska faktorer för organisationens förmåga att uppfylla sina mål. Som konsekvens av detta saknas ofta nödvändiga resurser och nödvändigt stöd för detta arbete.

På denna nivå uppfyller organisationen den miniminivå som kan förväntas för beviljandet av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att de anställda tar aktiv del i att se över och revidera säkerhetspolicy och säkerhetsmålen och tillämpningen av dessa.

Man kan se tecken på att en positiv organisationskultur börjar utvecklas. Man börjar ta hänsyn till kunskap och metoder kring mänskliga och organisatoriska faktorer på ett systematiskt sätt vid utvecklingen av organisationens affärsprocesser. Ledningen har ett konsekvent och mestadels positivt förhållningssätt till att diskutera mänskliga och organisatoriska faktorer, och till att tillhandahålla resurser för arbete med dessa faktorer.

Ledningen ser säkerhet som något viktigt men produktionen prioriteras ibland. Den grundläggande säkerheten finns på plats och organisationen är på väg mot ett proaktivt perspektiv snarare än ett som enbart bygger på efterlevnad av regler och föreskrifter. Organisationen vet att det är viktigt att all personal deltar för att man ska kunna göra ytterligare förbättringar och de flesta är villiga att bidra på ett positivt sätt. De flesta anställda tar personligt ansvar för sin egen säkerhet. Säkerheten drivs på genom kampanjer och tillsyn, huvudsakligen uppifrån och ned men med visst deltagande från personalens sida.

Säkerhetsstyrningssystemet är konsekvent när det gäller att kontrollera de flesta risker som organisationen utsätts för.

Nivå 4 – förebyggande

Som nivå 4 samt att säkerhetsmålen underbyggs genom beteendet hos alla som agerar i ledningskedjan.

Det finns ett förverkligat engagemang för att kontinuerligt förbättra riskhanteringens effektivitet och verkningsfullhet. Det finns bevis för ett utbrett samarbete genom hela ledningskedjan. Det finns bevis för att säkerhetsrisker övervägs när man tittar på affärsrisker.

Policyer på ledningsnivån

- *ses över och revideras för att driva fram förbättringar på ett förutsebart sätt, och*
- *tolkas på samma sätt i alla de delar av organisationen som tillämpar dem,*
- *är utåtriktade och inriktade på förbättring.*

Organisationens kultur är överlag positiv och det finns möjligheter för personalen att bidra proaktivt till utvecklingen av säkerhetsstyrningssystemet på vissa områden.

Resurser görs tillgängliga för säkerhetsstyrning men det finns fortfarande vissa begränsningar.

Ledningen förstår att säkerhet och produktivitet är sammankopplade och att säkerheten ska prioriteras högst i oklara fall. Ledningen är engagerad i säkerheten och avsätter betydande resurser till proaktiva säkerhetsåtgärder såsom riskbedömningar, utredningar av incidenter och olyckor samt processer för hantering av förändringar. Vikten av säkerhet accepteras genom hela organisationen och personalen är engagerad på ett positivt sätt i säkerhetsinitiativ. Säkerhetsprestandan är inriktad på både ledande och eftersläpande indikatorer som använder all data som finns att tillgå.

Ett medvetet arbete med mänskliga och organisatoriska faktorer genomsyrar organisationens hela verksamhet och stöds av högsta ledningen.

Nivå 5 – utmärkt

Nivå 4 samt att säkerhetspolicyen omfattar säkerhetsmål som bryts ner till relevanta nivåer genom hela organisationen. Det finns förfaranden för att avsätta tillräckliga mänskliga, ekonomiska och tekniska resurser till stöd för att dessa mål ska kunna uppnås, och ledningen övervakar införandet av de nödvändiga säkerhetskraven. Säkerhetspolicyens effektivitet utvärderas och resultaten beaktas i följande revision. Säkerhetsmålen används för att sporra organisationen till att uppnå ett affärsresultat och hantera affärsrisker på ett sätt som ligger i linje med prestandan hos de organisationer som har bäst prestanda inom och utanför järnvägssektorn.

Det finns en medvetenhet om att hantering av säkerhetsrisker inte är en separat funktion utan en integrerad del i en produktiv, konkurrenskraftig och lönsam organisation.

Säkerhetsrisker ses som en risk för hela affärsresultatet och säkerhetsstyrningssystemet är effektivt när det gäller att hantera befintliga risker och förutse nya.

Säker produktion är högsta prioritet och man inser att säkerheten hänger ihop med affärsresultatet. Ledningens engagemang för säkerheten är stort och i organisationen vidtar man alla åtgärder för att hitta kraftfullare och mer hållbara lösningar på säkerhetsproblem. De lärdomar som dras tillämpas varje dag. Personalen förstår och stöder säkerhetsinitiativen och att säkerhet är en livsstil. Organisationen främjar säkerhet på arbetet och hemma och avsätter tillräckliga resurser för att göra detta.

Organisationens ledning betraktas som ledare av utvecklingen gällande mänskliga och organisatoriska faktorer som berör verksamheten och i ett vidare perspektiv.

4.2.2 L2 – Säkerhetspolicy

En effektiv säkerhetspolicy stakar ut en tydlig riktning för organisationen att följa. Den bidrar till alla aspekter av ett företags resultat som en del av en förpliktelse att åstadkomma kontinuerliga förbättringar. Säkerhetspolicyn är ett viktigt dokument för att visa hur organisationen hanterar sina säkerhetsförpliktelser och sitt ledarskap och engagemang för en lämplig hantering av säkerheten.

Nivå 1 – Otillräcklig

Policyn är inaktuell eller har inte vidarebefordrats inom organisationen.

Det finns inga tecken på att personalen rådfrågas.

Den roll som människor spelar för organisationens förmåga att uppnå en säker och effektiv verksamhetsnivå erkänns endast i liten omfattning.

Säkerhetspolicyn innehåller inget åtagande om att uppfylla regelkrav.

Denna prestationsnivå ligger under den minimistandard som man kan förvänta sig.

Nivå 2 – acceptabel

Säkerhetspolicyn är aktuell och kommuniceras inom organisationen, men lokala chefer och arbetsledare har oförenliga strategier eller tolkningar. Detta leder till att policyn tillämpas på olika sätt i olika delar av organisationen.

Policyn ses inte som avgörande för att upprätthålla säkerheten.

Det finns en viss insikt i det värde som en förbättrad förståelse för människans roll kan innebära för verksamheten, men den är ojämnt fördelad i organisationen.

Säkerhetspolicyn innehåller ett åtagande om att uppfylla regelkrav.

Prestationsnivån uppfyller miniminivån för kraven för att beviljas ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att säkerhetspolicyn och andra policyer som hänger samman med den används som fokus för cheferna, vilket leder till att de tolkas på samma sätt av all personal.

Personalen engageras aktivt i att se över och revidera säkerhetspolicyn och dess tillämpning.

Det finns ett tydligt fokus på frågor som rör mänskliga faktorer inom organisationen och en förståelse för den viktiga roll som människor spelar för att åstadkomma en säker och effektiv organisation och att uppnå affärsmålen.

Nivå 4 – förebyggande

Säkerhetspolicyen stämmer överens med beteendet hos alla som agerar i ledningskedjan.

Säkerhetspolicyen omfattar ett förverkligat engagemang för att kontinuerligt förbättra riskhanterings effektivitet och verkningsfullhet. Det finns bevis för ett utbrett samarbete i hela ledningskedjan byggt på en förståelse av människans betydelse för att förbättra verksamhetens förmåga att uppnå sina mål.

Organisations förmåga att hantera mänskliga faktorer mäts, anpassas och görs proportionerlig till organisationens mognad och komplexitet med ett fokus på kontinuerlig förbättring.

Säkerhetspolicyen och alla policyer som hänger samman med den

- *stämmer överens med varandra,*
- *ses över och revideras för att driva fram förbättringar på ett förutsebart sätt, och*
- *tolkas på samma sätt i alla de delar av organisationen som tillämpar dem.*

Nivå 5 – utmärkt

Säkerhetspolicyen används för att sporra organisationen att uppnå en affärsprestanda som ligger i linje med prestandan hos de organisationer som presterar bäst.

Det finns en medvetenhet i säkerhetspolicyen om att hantering av säkerhetsrisker inte är en separat funktion utan en integrerad del i en produktiv, konkurrenskraftig och lönsam organisation.

Det finns en insikt i att säkerhetsrisker innebär en risk för affärsprestandan.

Det finns en förståelse för människans betydelse för organisationens framgång och detta beaktas vid varje översyn av den operationella utvecklingen och affärsutvecklingen.

Organisationen är utåtblickande och söker efter externa möjligheter att utveckla sin effektivitet och verkningsfullhet och tar hänsyn till frågor rörande mänskliga faktorer när den gör detta.

4.2.3 L3 – Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen

Syftet med detta krav är att den organisation som står under tillsyn ska visa vilken struktur den har och hur ansvarsområden fördelas för att uppfylla organisationens företagsmål och säkerhetspolicy. Det kan finnas arbetsnivåer som stöder detta ur policysynvinkel och ur ett strategiskt perspektiv.

Riskhanteringen bör passa in på ett lämpligt sätt i ledningsstrukturerna så att det står klart var ansvaret ligger. Organisationens riskhantering bör också omfatta att identifiera och effektivt hantera de risker som uppkommer på grund av samverkan med entreprenörer, partner och leverantörer.

Dessa faktorer är centrala för förståelsen av hur väl organisationens säkerhetsstyrningssystem hanterar risker. Organisationen bör visa hur kompetent personal tillhandahålls för verksamheter, hur det säkerställs att denna personal har en klar förståelse av sina roller och ansvarsområden, och hur människor hålls ansvariga för sina prestationer. Den organisatoriska strukturen och de enskilda personernas roller och ansvarsområden förutsätter en balans mellan efterlevnad och säkerhetskultur – en tänkande kultur snarare än säkerhet som motiveras endast av efterlevnad för dess egen skull.

Nivå 1 – Otillräcklig

Organisationens ledningsstrukturer har inget samband med dess säkerhetsmål, så personalens ansvarsområden och ansvarsskyldighet blandas lätt ihop.

Vid tilldelningen av ansvarsområden ges personalen inte de befogenheter eller de resurser som behövs för att utföra dem. En del personal som tilldelas ansvarsområden kanske inte är medvetna om dem eller har den kompetens som behövs för att utföra dem. Arbetsbeskrivningarna speglar inte på ett korrekt sätt hur människor faktiskt hanterar sina roller eller ansvarsområden.

Fördelningen av roller och ansvarsområden över hela organisationen är slumpartad och saknar samband med organisationens operativa mål.

Prestationsnivån understiger den som kan förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Det finns en beskrivning av organisationens struktur inklusive fördelningen av roller och skyldigheter inom ramen för säkerhetsstyrningssystemet. Det finns planer för hur man fastställer hur arbete verkligen utförs inom organisationen.

Organisationens struktur innebär att de flesta risker hanteras av de människor eller grupper som utför arbetet, men en del risker är uppdelade så att det förekommer, eller det kan förekomma, konflikter mellan säkerhet och andra mål.

Det tycks finnas brist på samstämmighet mellan de enskilda affärsenheternas verksamhet och de bredare målsättningarna i organisationens verksamhetsmål.

Det tycks finnas brist på samstämmighet i organisationens strukturer, fördelningen av ansvarsområden och den därmed förknippade kultur som krävs för att kunna genomföra dem på ett effektivt sätt.

Organisationen uppfyller miniminivån för efterlevnad för att beviljas ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att den organisatoriska strukturen på olika områden på ett tydligt sätt stämmer överens med de ansvarsområden som fördelats mellan olika affärsenheter.

Övergripande policyer och förfaranden som rör roller och ansvarsområden stämmer överens med policyer och förfaranden för berörda affärsenheter.

Det finns kriterier för att fördela och tilldela ansvarsområden och uppgifter till personer som har den nödvändiga kompetensen och de nödvändiga kunskaperna. Dessa kriterier tillämpas och säkerhetsuppgifterna tilldelas därför på ett tydligt sätt till personal som har lämplig kompetens samt de befogenheter och resurser som krävs för att utföra dessa arbetsuppgifter.

När ansvarsområden fördelas finns det en systematisk strategi för hur detta ska göras. Personalen är kompetent och ges tillräckligt med resurser och maktbefogenheter för att hantera dessa ansvarsområden.

När man överväger nya eller förändrade roller och ansvarsområden analyseras frågor som rör mänskliga faktorer i relation till förändringen och till det sätt på vilket arbetsuppgifter faktiskt utförs inom organisationen.

Nivå 4 – förebyggande

Samma som för nivå 3, men med tydliga kopplingar mellan delarna i den organisatoriska strukturen genom hela organisationen, inte endast på arbetsnivåerna.

Övergripande policyer och förfaranden har utformats för att komplettera varandra över alla affärsenheter för att främja organisationens strategiska mål.

Personal med säkerhetsansvar hålls ansvarig för sina prestationer på ett rättvist och konsekvent sätt. Organisationens kultur gör det möjligt för personal med säkerhetsansvar att påverka hur uppgifterna utförs och hur förbättringar görs.

Som en följd av att man förstår hur arbetet faktiskt utförs ligger de individuella och kollektiva insatserna i linje med de operationella prestandamålen.

Nivå 5 – utmärkt

Samma som för nivå 4, med tillägg av effektiva genomgångar av organisationens struktur, roller och ansvarsområden på alla nivåer, i relation till strategiska och affärsrelaterade mål.

En formell granskningsprocess har införts för att se till att roller och ansvarsområden fortsatt är giltiga, aktuella och integrerade med den föränderliga organisationen, strategin och miljön. Organisationen tar på ett konsekvent sätt, och som ett standardsinslag i granskningsprocessen, hänsyn till människan i systemet.

4.2.4 L4 – Samråd med personal och andra parter

Framgångsrika organisationer låter personalen delta aktivt för att uppmuntra dem att använda sin kunskap och sina erfarenheter och för att skapa engagemang för de gemensamma målen. Sådana organisationer stöder aktivt och uppmuntrar till engagemang och samråd på olika sätt.

En undersökning av denna aspekt ger även tillsynsmyndigheten en indikation på hur säkerhetskulturen ser ut inom organisationen och hur aktivt organisationen låter eventuella tredjeparter delta i säkerhetsstyrningen på områden med delade risker.

Nivå 1 – Otillräcklig

Det förekommer få eller inga samråd.

Personalen förstår inte hur de bidrar till sin egen säkerhet och till sina medarbetares säkerhet.

Organisationen uppfyller inte den standard som kan förväntas på miniminivån för rättslig efterlevnad.

Nivå 2 – acceptabel

Personalen förstår att de ansvarar för sin egen säkerhet och för sina medarbetares säkerhet, men detta är inte konsekvent i hela organisationen.

Det förekommer en del samråd rörande hälsa och säkerhet, men samrådsarbetet tycks inte utföras på ett systematiskt sätt och alla anställda deltar inte.

Organisationen uppfyller de rättsliga miniminormer som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att organisationen har förfaranden som ser till att personalen rådfrågas om säkerhetsfrågor.

Personalen förstår hur de bidrar till sin egen och järnvägens säkerhet och de får återkoppling om sina bidrag.

Personer i liknande roller tillämpar standarder på samma sätt.

Nivå 4 – förebyggande

Organisationens policy omfattar att försöka engagera personalen på organisationens alla nivåer, och det finns en tydlig struktur för att kommunicera denna policy. Arbetstagare och personal rådfrågas när beslut ska tas om åtgärder för riskhantering.

Organisationen rådfrågar regelbundet sin personal på en rad olika sätt, som enkäter, workshoppar, möten med chefer och säkerhetsronder.

Personalen är motiverad till att uppnå verksamhetsmålen och uppvisar en konsekvent förståelse för hur detta ska åstadkommas.

Personalen känner att de kan fatta beslut inom en ram med fastställda mål.

Personer i liknande roller tillämpar standarder på ett konsekvent sätt.

Personalen förstår behovet av förändring och bekräftar att de rådfrågas om hur förändringar ska införas.

Nivå 5 – utmärkt

Organisationen använder sina arbetstagares och andra berörda parter potential fullt ut och låter dem aktivt delta i att utarbeta gemensamma värderingar och en kultur som bygger på tillit, öppenhet och medbestämmande.

Organisationen använder sig av personalens deltagande för att samla in idéer om förbättring och omvandlar dem till praxis.

Personalen visar att de förstår hur de bidrar till att organisationens mål uppnås. Denna förståelse stämmer överens med organisationens tillämpliga policyer och ledningens vision.

Personalen engagerar sig i att överträffa dessa mål genom att följa befintliga processer och visa var dessa processer kan förbättras.

4.3 PL – Planering

Syfte

Att se till att organisationen kan definiera och tillämpa riskhantering som gör det möjligt för verksamheten att bedrivas på ett säkert sätt. Att planera verksamheten på ett säkert sätt med vederbörlig hänsyn till den egna personalens välfärd och välfärden för andra som påverkas av verksamheten.

Inledande kommentarer

Bra planering är utgångspunkten för riskhantering. Organisationen bör ha infört lämpliga förfaranden för att kunna uppfylla sina rättsliga förpliktelser och uppfylla sina mål på ett effektivt och verkningsfullt sätt. Bra planering förbättrar organisationens sätt att hantera säkerheten genom att se till att de rätta resurserna finns tillgängliga, inklusive kompetent personal som kan utföra uppgifterna. Detta leder till en verkningsfull riskkontroll och effektivt arbete.

4.3.1 PL 1 – Åtgärder för att hantera risker

Denna faktor har att göra med säkerhetsstyrningssystemets kärna, och syftar till att låta organisationen visa hur deras system identifierar och hanterar de risker som organisationens verksamhet medför. Tillsyn visar hur man använder resultaten från riskbedömningen i praktiken för att förbättra riskhanteringen och hur man övervakar detta över tid. Det är viktigt att komma ihåg att denna faktor inte direkt handlar om hantering av risker i samband med förändringar (vilket är en annan faktor), men den står i nära samband med denna. Man bör även notera att det är ett särskilt krav att man riskhanterar frågor som rör mänskliga prestationer, såsom utformningen av arbetsuppgifter och trötthetsriskhantering. Från ett tillsynsperspektiv bör man därför försöka hitta bevis för att dessa frågor hanteras inom ramen för organisationens riskbedömningsprocess.

De system som används för planering och införande av riskhantering bör samordnas för att säkerställa att de följer tillämpliga lagar och gör det möjligt för organisationen att uppfylla sina mål på ett effektivt och verkningsfullt sätt.

Nivå 1 – Otillräcklig

Företaget har en riskbedömningsprocess men den har inte införts på ett konsekvent sätt och uppdateras inte heller på ett konsekvent sätt, vilket leder till att gamla operativa regler eller gammal verksamhetspraxis används för att styra risker när risken har förändrats.

Riskbedömningar genomförs inte eller granskas inte för alla tillämpliga aktiviteter i verksamheten.

Riskbedömningarna är olämpliga för sin avsedda användning. Det förekommer tydliga exempel på missförstånd av riskbedömningarnas syfte och hur de ska utföras.

Riskhantering används på ett bristfälligt sätt och det förekommer inte mycket uppföljning av verkningsfullheten av den styrning som har införts.

Risker relaterade till mänskliga faktorer tycks inte beaktas under riskbedömningen. Det finns inget medvetet affärsbehov av att hantera sådana frågor.

Det finns få bevis inom riskbedömningsprocessen på att man tar tillräcklig hänsyn till säkerhetsrisker relaterade till mänskliga eller organisatoriska faktorer när man hanterar förändringar.

Organisationen presterar på en nivå som understiger den som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Riskbedömningar genomförs, men den övergripande samordningen är otillräcklig.

Åtgärder för styrning av en aktivitet omfattar inte alltid de åtgärder som har identifierats i samband med riskbedömning av aktiviteten.

Riskbedömningar används ofta bara för att visa att redan befintlig riskhantering är tillräcklig.

Riskbedömningar används endast för att fastställa var riskhantering behövs, men denna styrning införs inte på ett lämpligt sätt av organisationen.

Utbildning om riskbedömning har erbjudits till alla medlemmar av personalen som behöver detta på den nivå som är lämplig för olika ansvarsnivåer.

Det finns bevis för att riskhantering används och övervakas.

Det finns en medvetenhet om att frågor som rör mänskliga faktorer bör beaktas under riskbedömningen men tillämpningen av detta kan vara bristfällig. Som en följd av detta styrs inte sådana problem i så hög grad som de borde genom säkerhetsstyrningssystemet.

Det finns bevis för att säkerhetsrisker, inklusive mänskliga och organisatoriska faktorer, övervägs inom ramen för processen för hantering av förändringar.

Organisationen presterar på miniminivån för efterlevnad för en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att organisationen har en tydlig policy för användningen av riskbedömningar och för vilka risker som tolereras och varför.

Riskhanteringen används på ett konsekvent sätt i olika delar av organisationen, inklusive inom ramen för processen för hantering av förändringar. Cheferna förstår sin roll i processen.

Man gör effektivt bruk av riskhantering och riskeliminering.

Samordningen av riskbedömningar är konsekvent och bedömningarna granskas regelbundet.

Risker och tillhörande åtgärder för att styra dem kommuniceras på ett tydligt sätt till personalen.

Riskbedömningsförfaranden är en del av processen för hantering av förändringar.

Det finns ett enkelt system på plats för att kontrollera verkningfullheten hos den riskhantering som införts som ett resultat av regelbundna riskbedömningar.

Det har införts konsekventa processer för att identifiera risker förknippade med mänskliga och organisatoriska faktorer under riskbedömningens gång. Verksamheten kan vid behov dra nytta av specialiserad expertkunskap för att underlätta detta.

Nivå 4 – förebyggande

Som nivå 3 samt att riskbedömningarna har byggts in i andra aspekter av verksamheten för att säkerställa att det finns en systematisk strategi för riskhantering.

Alla nivåer av arbetsstyrkan såväl som externa organisationer kan bidra till riskbedömningarna.

Riskbedömningar, inklusive riskeliminering, är en del av förändringsprocessen och organisationens kultur.

Genomgångar utgör en del av riskbedömningsprocessen.

Riskhanteringsprinciper tillämpas på ett intelligent sätt på alla nivåer.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Det finns ett mer komplext system på plats för att kontrollera verkningsfullheten hos den riskhantering som införts som ett resultat av regelbundna riskbedömningar.

Frågor som rör den mänskliga och organisatoriska faktorn har helt integrerats i säkerhetsstyrningssystemets processer för riskbedömning och ändringshantering. De som ansvarar för utförandet av riskbedömningar ges återkoppling om hur väl de presterar.

Nivå 5 – utmärkt

Som nivå 4 samt att riskbedömningarna används som en drivkraft för kontinuerliga förbättringar av organisationens riskprofil.

Strategin för riskhantering är integrerad i och konsekvent tillämpad i hela organisationen. Riskerna bedöms noggrant och övervägs långt i förväg innan några förändringar genomförs.

Riskeliminering är en del av en konsekvent strategi vilket avspeglas i organisationens policyer.

Det finns proaktiva förfaranden på plats för att utarbeta åtgärder för riskhantering i samverkan med andra enheter med ansvar för riskhantering där det förekommer gemensamma problem.

Informationen från riskbedömningar av mänskliga och organisatoriska faktorer används i hela verksamheten som en drivkraft för kontinuerlig förbättring av säkerheten. Resultaten av bedömningarna kommuniceras i tillämpliga fall med entreprenörer, partner och leverantörer som en del i att förbättra effektiviteten i organisationens verksamhet.

4.3.2 PL2 – Säkerhetsmål och planering

För att säkerställa att organisationen uppfyller tillämpliga regelkrav, att säkerheten kontinuerligt förbättras, att personalen känner till och att ledningen står bakom organisationens mål är det nödvändigt att man har säkerhetsmål som uppfyller de så kallade SMART-kraven.

Organisationen måste visa att den har meningsfulla mål och en process för att uppnå dessa samt för att övervaka hur väl dessa uppfylls under sin giltighetstid. Säkerhetsmålen måste vara "Specifika, Mätbara, uppnåeliga (eng. Achievable), Realistiska och Tidssatta" (SMART). Både kortsiktiga och långsiktiga mål bör fastställas och prioriteras utöver mera omfattande affärs mål. Prioriteringar som står i konflikt med varandra bör hanteras så att säkerhetsmålen prioriteras ned till förmån för andra affärsbehov. Mål som har fastställts på olika nivåer eller för olika delar av en organisation bör anpassas till varandra så att de stöder de övergripande målen i organisationens policy. Personliga mål kan också avtalas med enskilda personer för att se till att målen uppnås.

Nivå 1 – Otillräcklig

Det finns få eller inga säkerhetsmål.

De säkerhetsmål som finns är inte SMARTa eller prioriteras inte.

Att misslyckas med att uppnå säkerhetsmålen tolereras och inga åtgärder vidtas för att ta itu med brister i uppnåendet av målen.

De personliga målen står inte i samband med målen i organisationens övergripande policyer.

Organisationen presterar på en nivå som understiger den som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Det finns säkerhetsmål. En del kan vara SMARTa och prioriteras, men målen inom olika delar av organisationen är inte tydligt anpassade till varandra och kan stå i konflikt med varandra, och som en följd av detta stöder de inte alltid de övergripande målen i organisationens policy.

De personliga målen sammanfaller i huvudsak med målen i organisationens övergripande policy.

Det finns uppföljning av framstegen rörande uppnåendet av säkerhetsmålen.

Organisationen uppfyller den minimistandard som kan förväntas för regelefterlevnad.

Nivå 3 – konsekvent

Som nivå 2 samt att säkerhetsmålen har fastställts och det finns en säkerhetsplan som visar hur organisationen ska uppnå sina mål.

De fastställda säkerhetsmålen tar hänsyn till tillämpliga regelkrav och andra krav.

Man försöker att fastställa SMARTa mål och att prioritera mål och riktmärken och anpassa dem till varandra.

Det finns system på plats för uppföljning av uppnåendet av målen.

Uppnåendet av målen är inte väl anpassat till processen för genomgångar, det vill säga vid genomgångarna tas inte hänsyn till de fastställda målen.

Personalen är medveten om relevansen och vikten av sin verksamhet och om hur de bidrar till uppnåendet av säkerhetsmålen och till planeringen för hanteringen av säkerhetsrisker.

Nivå 4 – förebyggande

Som nivå 3 samt att målen är SMARTa, prioriteras och ligger i linje med varandra för att stödja den övergripande policyn.

Säkerhetsstyrningssystemet säkerställer att säkerhetsmålen fastställs och resultatet mäts.

Uppnående eller brist på uppnående dokumenteras och används för att bidra till den kontinuerliga förbättringen.

Det finns system på plats för uppföljning av potentiella och faktiska misslyckanden med att uppnå säkerhetsmålen.

Nivå 5 – utmärkt

Som nivå 4 samt att organisationen jämför sina resultat med andra organisationers, inom och utanför järnvägsbranschen, för att se till att målen representerar högsta kvalitet.

4.4 S – Stöd

Syfte

Syftet med detta krav är att se till att organisationen bidrar med tillräckligt med resurser inklusive kompetent personal för att säkerhetsstyrningssystemet ska kunna styra riskerna i enlighet med målen:

Att fastställa roller och ansvarsområden för uppnåendet av organisationens säkerhetsmål.

Att se till att viktig information finns att tillgå för de personer som fattar beslut.

Att se till att organisationens arrangemang och åtgärder främjar en kultur som möjliggör högsta kvalitet när det gäller riskhantering.

Inledande kommentarer

Dokumentationen för säkerhetsstyrningssystemet måste styras noggrant och regelbundet ses över så att endast den senaste versionen av varje enskilt dokument som krävs för säkerhetsstyrning är i omlopp. Alla ändringar av dokumentationen som följer av processen för kontinuerlig förbättring av riskhantering måste genomföras i god tid.

Det är av avgörande betydelse att säkerhetsstyrningssystemet innehåller ett övergripande och tillämpat kompetensstyrningssystem och att lämpliga arbetssätt för kommunikation har införts både från ledningen till personalen och vice versa, och till andra parter som är beroende av kommunikation med organisationen för att hantera säkerheten inom sina egna organisationer. Detta beror på att dessa faktorer stöder säkerhetsstyrningssystemets effektivitet och verkningsfullhet. Att ha kompetent personal i tjänst som utför de uppgifter som krävs av dem minimerar risken för felbedömningar som undergräver säkerhetsstyrningssystemets funktion. Att samtidigt se till att kommunikationssystemet fungerar både uppifrån och ned och nedifrån och upp genom hela organisationen säkerställer att de centrala meddelandena uppfattas i god tid av rätt personer.

4.4.1 S1 – Resurser

En effektiv användning av resurser är en central faktor i alla säkerhetsstyrningssystem. Det räcker inte att ha infört processer, de måste också fungera, och det kräver att tillräckligt med resurser tilldelas för att detta ska hända på ett effektivt och verkningsfullt sätt.

Nivå 1 – Otillräcklig

Organisationen tillhandahåller resurser som gör det möjligt för säkerhetsstyrningssystemet att fungera, men detta görs inte på ett systematiskt sätt utan enligt en lappverksstrategi. Följden av detta är att fördelningen av resurser inom organisationen blir ojämn, så att några områden får tillräckligt med resurser medan andra områden inte får det.

Organisationen underskrider den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

På denna nivå är organisationen bättre på att hantera resurser för att möjliggöra genomförandet av uppgifter. Tilldelningen av resurser anses vara en viktig del av säkerhetsstyrningssystemet. Organisationens ledning granskar regelbundet resurserna.

Organisationen presterar på den grundläggande nivå som kan förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Nivå 3 – konsekvent

Som nivå 2 samt att på denna nivå kan organisationen visa att det finns tillräckligt med resurser och att fördelningen av dem är konsekvent över alla delar av verksamheten. Frånvaron av en del personal utgör inte ett viktigt problem eftersom detta åtgärdas inom ramen för säkerhetsstyrningssystemets processer. Man börjar inom organisationen tänka på hur man kan använda sig av resurserna på ett mer effektivt sätt.

Nivå 4 – förebyggande

Samma som för nivå 3, men här förutser organisationen sina framtida behov så att den är förberedd för kommande förändringar och har resurser på plats för att hantera detta.

Nivå 5 – utmärkt

Som nivå 4 samt att här hanterar organisationen sina resurser på ett mycket proaktivt sätt och använder dem på ett flexibelt sätt över hela organisationen för att uppnå större säkerhet och effektivitet.

4.4.2 S2 – Kompetens

För att över tid säkerställa styrning av personal med säkerhetsansvar är det av avgörande betydelse att en organisation har ett kompetensstyrningssystem som utgör en del av säkerhetsstyrningssystemet. Det är genom denna mekanism som personalens kompetens utvärderas, utvecklas, bibehålls och övervakas så att säkerheten inte undermineras.

Organisationer behöver ha ett effektivt system för kompetensstyrning för att säkerställa att personalen har lämplig kompetens. En avgörande del av alla kompetensstyrningsprocesser är bibehållandet av kompetens. Detta omfattar ett övergripande kontinuerligt yrkesmässigt program för kompetensutveckling där mer erfaren personal får kunskap om ny utveckling på säkerhetsområdet.

Hur kompetensstyrningssystemet fungerar kan säga en hel del om en organisations säkerhetskultur. Ett väl uttänkt kompetensstyrningssystem är inkluderande och låter personal som faktiskt utför arbetet och som därför bäst förstår uppgiften lämna synpunkter om utformningen av kompetensstyrningssystemet, vilket därmed hjälper både enskilda personer och organisationen att prestera bättre. Ett fungerande kompetensstyrningssystem är en nyckelindikator för en organisations säkerhetskultur.

Nivå 1 – Otillräcklig

Kompetensstyrningssystemet har dokumenterats men har inte genomförts på ett tydligt sätt och är inte kopplat till utformningen av arbetsuppgifter. Strategin för att hantera personalens kompetens är rörig.

Personalen är kanske kompetent (eller inte), men det finns ingen konsekvent process för att identifiera detta.

Utbildningsbehoven hanteras slumpmässigt, och omedelbara behov prioriteras framför långsiktig utveckling.

Lite eller ingen uppmärksamhet har fästs vid de kompetenser som är nödvändiga för göra människor effektiva i att hantera mänskliga och organisatoriska faktorer eller säkerhetskulturförändringar inom organisationen.

Organisationen presterar på en nivå som understiger den som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Utbildning sker i enskilda verksamhetsenheter och huvudsakligen genom praktikutbildning inom ramen för ett kompetensstyrningssystem. Det finns en miniminivå för efterlevnad av lagkraven för rekrytering, antagning och utbildning. Det finns en antagningsprocess för säkerhetsroller av avgörande betydelse.

Rekryterings-, antagnings- och utbildningspolicyerna ingår inte i ett konsekvent system och är inte kopplade till organisationens strategiska mål, och går inte mycket längre än att uppfylla lagkraven.

Det förekommer ett visst fastställande av utbildningsbehov, inklusive utbildning inom mänskliga och organisatoriska faktorer samt säkerhetskultur, men tilldelningen av utbildningen är ofta slumpartad och styrs av tillgången både på utbildningen och den relevanta personalen i stället för att utgöra en del av en strukturerad strategi.

Organisationen uppfyller den miniminivå för efterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att organisationen har infört ett effektivt dokumenterat kompetensstyrningssystem. Detta omfattar den kompetens som behövs för att uppfylla organisationens strategiska mål och hantera risker. Organisationens kan fullt ut utnyttja personalens kompetens när den känner till vad denna är.

Organisationen kan organisera och utarbeta utbildningsprogram för den del av personalen som utför säkerhetsuppgifter av avgörande betydelse, vilket säkerställer att de relevanta behoven uppfylls och att personalens kompetens bibehålls.

Tillbaka-till-arbetet-strategier finns att tillgå för personal efter olyckor/incidenter eller lång bortavaro från arbetet, däribland strategier som identifierar behovet av ytterligare utbildning där så krävs.

Rekryterings- och antagningsprocesserna är omfattande (till exempel psykometriska och uppgiftsbaserade) och i stort konsekventa, och de resulterar vanligen i att lämpliga personer väljs ut för de olika roller som krävs.

Utbildningssystemet tillhandahålls av kompetenta personer inom ramen för ett fastställt program som bygger på behoven hos en viss roll. Utbildningen inbegriper reaktioner på normala och dåliga arbetsätt.

Det finns en förståelse för behovet av att koppla kompetensstyrningssystemet till uppgiftens utformning.

Det finns en förståelse för vilken kompetens som behövs för att hantera mänskliga och organisatoriska faktorer samt för säkerhetskultur, och relevant personal rekryteras med rätt kompetens.

Nivå 4 – förebyggande

Som nivå 3 samt att rekryterings-, antagnings- och utbildningspolicyerna har tydliga kopplingar till organisationens strategiska mål, som i sig bryts ner till målen för enskilda arbetstagare. De bygger på en korrekt bedömning av uppgifter (uppgiftsanalys), som bidrar till ett tydligt och konsekvent kompetensstyrningssystem.Handledning används och förändringar av roller är väl genomtänkta.

Utbildningssystemet är omfattande och kopplat till den kompetens som krävs och behövs för att man ska kunna fungera effektivt i särskilda roller.

Rekryteringsprocesserna är omfattande och inriktade på den optimala uppsättningen färdigheter för en särskild roll. De stöds av regelbunden granskning (såväl som granskningar när personal lämnar organisationen) för att se till att rätt personer rekryteras allteftersom organisationen förändras och utvecklas.

Organisationen är tydlig om vilka behov av kompetens som finns på områdena mänskliga och organisatoriska faktorer och säkerhetskultur och det finns arbetsätt för att säkerställa att den har personal med rätt kompetens och att den vidmakthålls över tid.

Nivå 5 – utmärkt

Som nivå 4 samt att organisationen förstår personalens kompetens och utnyttjar deras potential till fullo. Organisationens låter dem aktivt delta genom delade värderingar och en kultur som bygger på tillit, öppenhet och medbestämmande.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Organisationen låter personalen vara delaktig i att ta fram och implementera förbättringsförslag. Personalplanering görs för att säkerställa verksamhetens kontinuitet.

Det finns en framåt- och utåtriktad vision som syftar till att säkerställa att rätt personer rekryteras och ges lämplig utbildning och utvecklingsmöjligheter för att se till att färdigheter bibehålls på en nivå som låter organisationen växa och utvecklas samtidigt som säkerhetsprestandan upprätthålls och förbättras.

Organisationen är ledande i att utveckla sin personal inom relevanta kompetensområden för att kunna upprätthålla en högklassig prestationsnivå vad gäller hanteringen av mänskliga och organisatoriska faktorer samt organisationskultur.

4.4.3 S3 – Medvetenhet

Medvetenhet betyder att göra personalen medveten om organisationens säkerhetspolicy och om hur de bidrar till säkerheten inom organisationen, de faror och risker som de behöver känna till och resultaten från olycks- och incidentutredningar. Det omfattar även att göra personalen medveten om följderna av att inte bidra till tillämpningen av säkerhetsstyrningssystemet, både från deras eget och från organisationens perspektiv. Denna faktor tillhandahåller därför viktig information om organisationens säkerhetskultur.

Nivå 1 – Otillräcklig

Här har organisationen gjort säkerhetspolicy tillgänglig för personalen och kommunicerar viss grundläggande information om risker och faror. Resultaten av incidentutredningar meddelas inte systematiskt till all personal och det finns inga samordnade försök att verifiera att personalen förstår vilka deras egna och organisationens ansvarsområden är. Som ett resultat av detta är säkerhetskulturen bristfällig.

Organisationens prestanda understiger den som kan förväntas för rättslig efterlevnad.

Nivå 2 – acceptabel

På denna nivå lämnas mer information till personalen men denna information verkar inte ha ett fast format och de meddelanden som sänds ut är inte tydliga över hela organisationen. Organisationen försöker se till att personalen förstår sin roll i att utveckla säkerheten inom ramen för säkerhetsstyrningssystemet.

Organisationens prestanda motsvarar den miniminivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Utifrån insamlad information är det uppenbart att organisationen har en svag säkerhetskultur som varierar mellan olika delar av organisationen.

Nivå 3 – konsekvent

Som nivå 2 samt att arbetssättet för att kommunicera säkerhetspolicy till personalen samt kommunikationen till personalen om deras roller är konsekventa och meddelandena förstås av personalen. Viss övervakning utförs för att se till att personalen har tagit till sig informationen och att de förstår vikten av sina roller när det gäller att se till att säkerhetsstyrningssystemet fungerar på ett effektivt sätt.

Organisations säkerhetskultur förefaller att vara konsekvent men det finns luckor i den och den verkar inte utvecklas.

Nivå 4 – förebyggande

Samma som för nivå 3 samt att organisationen proaktivt försöker att främja medvetenheten om organisationens och personalens roller och ansvarsområden. Organisationen försöker aktivt främja fördelarna för personalen själva med en förbättrad säkerhetsprestanda.

Organisationen arbetar aktivt med att övervaka och förbättra sin säkerhetskultur för att säkerställa att säkerhetsstyrningssystemet bidrar till önskvärda resultat.

Nivå 5 – utmärkt

Samma som för nivå 4 samt att organisationen försöker förbättra medvetenheten om organisationen och dess ansvarsområden inte bara hos sin egen personal utan också kommunicera detta till sina entreprenörer, leverantörer och andra som den samverkar med.

Organisationen ses som ledande ifråga om positiv och existerande säkerhetskultur. Personalen är engagerad och förstår sina ansvarsområden och roller, och stöttar proaktivt verksamheten i att uppnå de uppsatta målen.

4.4.4 S4 – Information och kommunikation

Syftet med detta område är att säkerställa att organisationen har infört lämpliga sätt att hitta säkerhetsrelaterad information på olika nivåer och att kommunicera denna i rätt tid och till rätt personer. Att de använder sig av situationsanalys och framtidsspaning för att se till att den befintliga riskhanteringen fortsatt är relevant och aktuell och kan identifiera nya hot och möjligheter i inflytandet utifrån (det politiska, sociala, miljömässiga, tekniska, ekonomiska och rättsliga). Att de kan se till att informationen når rätt personal (särskilt personal som är avgörande för säkerheten) inom organisationen som behöver reagera på den. Detta inbegriper hur man tillhandahåller relevant säkerhetsrelaterad information till andra berörda parter som man samverkar med.

Strategierna behöver säkerställa att all personal som fattar ett beslut eller utför en uppgift har rätt information, i form av

- företagsmeddelanden om vikten av säkerhet,
- förfaranden för utbyte av information med de berörda intressenterna,
- förfaranden och standarder som rör säkerhet,
- faktauppgifter och underrättelser, och
- anvisningar och rapporter.

Nivå 1 – Otillräcklig

Det görs knappt några försök att förmedla lämplig säkerhetsinformation. Om förfaranden har införts fattar personalen beslut baserade på deras eget omdöme.

Information om säkerhet samlas in och delas med andra endast i liten omfattning.

Cheferna pratar inte med sina underlydande, eller gör det på ett ineffektivt sätt.

Informationsutbytet och kommunikationen inom organisationen är slumpartade och ej spårbara.

Det finns liten medvetenhet om den viktiga roll som effektiv kommunikation spelar när det gäller att påverka mänskliga beteenden och därmed säkerhetsprestandan.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Personalen har tillgång till förfaranden och standarder för riskhantering.

En del information som erhålls från personalen används för att påverka beslut.

Chefer ger anvisningar och tar emot rapporter med avseende på riskhantering, men det verkar finnas viss brist på konsekvens.

Det finns ett visst erkännande av vikten av kommunikationer som avgörande för säkerheten för att uppnå säker operativ prestanda. Det finns bevis på att kvalitetssäkringsplaner utarbetas för att kontrollera detta.

Organisationen presterar på den miniminivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 3 samt att skriftliga verksamhetsmål, standarder och förfaranden för att kontrollera och förmedla betydande risker förekommer i format som är lämpliga för användarna.

Faktauppgifter används för att utbyta erfarenheter och fungera som vägledning för framtida prestationer och beslut.

Cheferna ger anvisningar som förstärker förfaranden som bidrar till att uppnå säkerhetsmålen.

Personalen rapporterar om sina prestationer och erfarenheter eftersom organisationen uppmanar dem att göra detta.

Kommunikationen inom organisationen är regelbunden och utförs enligt ett fastställt förfarande både uppåt och nedåt i ledningskedjan.

Roller och ansvarsområden för personer vars uppgift är att vidarebefordra information över hela organisationen bör tydligt definieras.

Övervakning och bedömning av kommunikationerna utförs regelbundet.

Nivå 4 – förebyggande

Som nivå 3 samt att allt ligger i linje med de huvudsakliga riskhanteringssystemen.

Rätt information finns att tillgå för att fatta beslut.

Effektiva förfaranden för insamling av återkoppling har införts där så är lämpligt för att se till att kommunikationerna förstås och att man förstår personalens reaktion på kommunikationerna. Berörd personal ges återkoppling om sina prestationer på ett positivt och icke-diskriminerande sätt.

Kommunikationerna övervakas och resultaten används för att påverka ett organisationsomfattande kommunikationsprogram.

Nivå 5 – utmärkt

Som nivå 4 samt att kvaliteten på kommunikationerna och arbetsätten för kommunikation granskas regelbundet och jämförs med god praxis i andra sektorer. Informationen delas på ett proaktivt sätt med organisationer med vilka företaget samverkar, såväl som med entreprenörer.

Informationsutbyten dokumenteras.

Det finns en utåtriktad vision för kommunikationen som delas både internt och externt med berörda partner, leverantörer och entreprenörer.

Den roll som spelas av mänskliga faktorer inom ramen för kommunikationsverksamheten förstås tydligt och organisationen har ett tydligt mål att hela tiden förbättra kommunikationsprestandan.

4.4.5 S5 – Dokumenterad information

Högkvalitativa organisationer tillhandahåller en tillförlitlig dokumentation över viktiga beslut och information som har insamlats över åren, för att visa att de styr risker på alla nivåer.

För att se till att information om riskkontroll, arbetsprocesser och lärdomar från revisioner och incidenter kommuniceras till berörd personal i god tid och på ett effektivt sätt måste organisationen ha ett system för styrning och hantering av dokumentation som åstadkommer detta.

I denna faktor ingår dokumentering av säkerhetsstyrningssystemet, skapande och uppdatering av dokument samt styrning av dokumenterad information.

Nivå 1 – Otillräcklig

Dokumentationen för säkerhetsstyrningssystemet utarbetas. Den täcker inte företagets hela verksamhet och uppdateras inte regelbundet efter alla typer av förändringar som innebär att det behöver göras.

Dokumentationen sprids eller delas inte på lämpligt sätt. Organisationen använder inte säkerhetsstyrningssystemet som anvisningar för arbetet utan den operativa praxisen är annorlunda och ofta kopplad till personalens och arbetstagarnas personliga minnen och till historisk praxis utan beaktande av tidens gång och av de förändringar som kan vara nödvändiga på grund av detta.

Dokumentationen används endast av intygs-/tillståndsskäl.

Dokumentstyrningssystemen är bristfälliga, vilket leder till att olika delar av verksamheten använder olika versioner av samma dokument.

Organisationen når inte upp till den prestandanivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Järnvägsföretaget/infrastrukturförvaltaren arbetar vanligtvis i enlighet med de förfaranden och anvisningar som anges i säkerhetsstyrningssystemet. Vissa avvikelser är möjliga. Det finns en del dokumentation av information om viktig riskhantering, men dokumentationen är inte konsekvent.

Det finns en årlig säkerhetsrapport som lämnas in till den nationella säkerhetsmyndigheten och som innehåller den organisatoriska strukturen, säkerhetsmålen för det kommande året och varför dessa har valts ut. Den innehåller också information om interna olycks- och incidentutredningar, detaljer om de säkerhetsindikatorer som har valts ut för att övervaka verksamhetens prestanda jämfört med målen och huruvida det finns några öppna rekommendationer från det nationella utredningsorganet.

Dokumentstyrningssystemet är i allmänhet tillförlitligt men det förekommer fortfarande problem med versionsnumrering och uppdatering av dokument på ett systematiskt sätt.

Organisationen presterar på den miniminivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att det finns dokumentation över processer och standarder för de huvudsakliga riskerna.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Det förs register över viktig information och beslut som sannolikt kommer att vara värdefulla i framtiden.

Säkerhetsstyrningssystemet innehåller en beskrivning av aktiviteter som ingår i processerna för säkerhetsstyrning och samspelet mellan dessa processer. Personalen tillämpar säkerhetsprocesserna på ett konsekvent sätt.

Det finns en översikt över avtalsstyrda processer och andra affärsavtal inklusive detaljerad information om hur säkerhetsriskerna styrs. Det finns en aktuell förteckning över entreprenörer, partner och leverantörer med en beskrivning av typ av verksamhet och omfattningen av den tjänst som erbjuds, som uppdateras kontinuerligt.

Dokumentstyrningssystemet är tillförlitligt och kan säkerställa att endast den aktuella versionen av ett dokument är i omlopp.

Nivå 4 – förebyggande

Som nivå 3 samt att det finns omfattande förteckningar över säkerhetsrelaterade processer och de risker som är förknippade med dem samt standarder, beslut och information att tillgå för användare och beslutsfattare.

Dokumentstyrningen är tillräckligt avancerad för att flagga dokument som behöver uppdateras och den person som är ansvarig för detta.

Nivå 5 – utmärkt

Som nivå 4 samt att den process som är drivkraften bakom effektiviteten och verkningsfullheten hos styrningssystemet används i högre grad. Säkerhetsstyrningssystemet speglar järnvägsföretagets/infrastrukturförvaltarens faktiska operativa praxis. Säkerhetsstyrningssystemet är ett levande dokument som hela tiden utvecklas för att förbättra säkerheten och är inte en administrativ börda.

Dokumentstyrningssystemet verkar för att förbättra och utveckla säkerhetsstyrningssystemet och ses som ett användbart verktyg för att se till att säkerhetsstyrningssystemet har ett konsekvent syfte.

4.4.6 S6 – Integrering av mänskliga och organisatoriska faktorer

Nivå 1 – Otillräcklig

Ledningens engagemang i mänskliga och organisatoriska faktorer är bristfällig och det finns dåliga kunskaper i organisationen om mänskliga och organisatoriska faktorer som begrepp och om skälen till varför begreppet mänskliga och organisatoriska faktorer bör användas för att åstadkomma en säker och effektiv organisation. Det finns en strategi för mänskliga och organisatoriska faktorer, men det finns många luckor och den omfattar inte alla de berörda processerna.

Strategin för mänskliga och organisatoriska faktorer har inte anpassats till den organisatoriska strukturen och till de organisatoriska processerna. Det finns dokumenterade processer för mänskliga och organisatoriska faktorer på vissa områden men inte på alla. Till exempel finns det inga metoder för integrering av mänskliga och organisatoriska faktorer i riskanalyserna. Det finns inga beskrivningar av roller och ansvarsområden med avseende på mänskliga och organisatoriska faktorer, kompetensen rörande mänskliga och organisatoriska faktorer saknas och det tilldelas inga resurser till arbetet med mänskliga och organisatoriska faktorer.

De strategier och processer rörande mänskliga och organisatoriska faktorer som har införts tillämpas inte fullt ut i praktiken. Utformningen av utrustning, arbetsplatser, system och verktyg görs med begränsad hänsyn till användarens behov. Man litar på kommersiellt tillgänglig användarinformation från tillverkare, och gör minimal eller ingen anpassning till den egna verksamheten. Förfaranden utformas av icke-användare utan att användare involveras. Inte mycket hänsyn tas till användarens behov i utformningen av arbetsmiljön.

Nivå 2 – acceptabel

Det finns en insikt att risker som uppstår från mänskligt beteende behöver identifieras men det görs inte konsekvent i verksamheten. Strategin för mänskliga och organisatoriska faktorer täcker alla relevanta processer inom organisationen, men strukturen är otydlig och processerna på en del områden rörande mänskliga och organisatoriska faktorer är mer fullständigt beskrivna än andra. Det står inte klart när och hur de mänskliga och organisatoriska faktorerna bör tillämpas. Det finns beskrivningar av de roller och ansvarsområden som har tilldelats inom ramen för mänskliga och organisatoriska faktorer, men det har inte avsatts tillräckligt med resurser.

Det finns en brist på förståelse för begreppet mänskliga och organisatoriska faktorer och för när och hur metoder avseende mänskliga och organisatoriska faktorer bör tillämpas. Strategier och processer rörande mänskliga och organisatoriska faktorer tillämpas vid behov, men det framförs synpunkter på att de inte behövs. Perspektivet kring mänskliga och organisatoriska faktorer anses inte vara viktigt för att uppnå säkerhet och effektivitet i organisationen.

Nivå 3 – konsekvent

Som nivå 2 samt att det finns en insikt om värdet av kunskap kring mänskliga och organisatoriska faktorer. Mänskliga och organisatoriska faktorer är ett begrepp som är känt av alla i organisationen och alla förstår vikten av att ha ett systematiskt arbetssätt för mänskliga och organisatoriska faktorer för att uppnå ett effektivt säkerhetsarbete i organisationen.

En systematisk strategi för mänskliga och organisatoriska faktorer tillämpas i organisationens alla delar. Strategier, processer och metoder som rör mänskliga och organisatoriska faktorer tillämpas för det mesta

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

men inte alltid, och resurser tilldelas mänskliga och organisatoriska faktorer. Krav på kompetens rörande mänskliga och organisatoriska faktorer med avseende på olika roller beskrivs och uppfylls.

Man tar hänsyn till mänskliga och organisatoriska faktorer inom hanteringen av förändringar. Mänskliga och organisatoriska faktorer är ett välkänt begrepp för alla i organisationen och alla förstår vikten av att använda en systematisk strategi för mänskliga och organisatoriska faktorer för att uppnå säkerhet och effektivitet i organisationen.

Nivå 4 – förebyggande

Som nivå 3 samt att en systematisk strategi för mänskliga och organisatoriska faktorer tillämpas konsekvent i organisationens alla delar. Strategin rörande mänskliga och organisatoriska faktorer utgör en naturlig del i alla processer. Fokus ligger inte på att uppfylla lagkraven som gäller mänskliga och organisatoriska faktorer utan i stället på att tillämpa arbetssätt för mänskliga och organisatoriska faktorer på ett sätt som uppfyller företagets mål.

Alla i organisationen inser fördelarna för säkerheten, effektiviteten och kvaliteten med att tillämpa arbetssätt för mänskliga och organisatoriska faktorer. Kapaciteten rörande mänskliga och organisatoriska faktorer är anpassad, skräddarsydd och proportionerlig till organisationens mognad och komplexitet, och är inriktad på förbättring över tid.

Åtgärder kring mänskliga och organisatoriska faktorer används i utformningen av processen för att validera nya gränssnitt och verktyg samt förändringar för att automatisera. Nya automatiserade funktioner granskas i särskilda studier om mänskliga faktorer. Metoder för mänskliga faktorer till exempel uppgiftsanalyser och användbarhetsanalyser används som indata för utformning, struktur och innehåll i förfaranden och fullskalesimuleringar involverar befintlig driftspersonal för att optimera förfaranden. Kapaciteten för att hantera mänskliga och organisatoriska faktorer mäts, skräddarsys och är proportionerlig till organisationens mognad och komplexitet samt är fokuserad på förbättring över tid.

Nivå 5 – utmärkt

Som nivå 4 samt att organisationen fungerar som ett föredöme för andra organisationer i sin framtoning. Den är tydlig med sina egna egenskaper och sina rättsliga förpliktelser och försöker utveckla detta genom att bygga vidare på sina starka sidor och dra nytta av erfarenheter både inom järnvägsbranschen och utanför denna. Organisationen är en aktiv främjare av vikten av att diskutera frågor rörande mänskliga faktorer i säkerhetsstyrningen.

Det finns en förståelse för att människan spelar en viktig roll för organisationens framgång och hänsyn till detta tas alltid när man utvärderar verksamhetens utveckling. Användaren står i centrum för all utveckling. Organisationen är utåtblickande, lär sig av intressenter och andra industrier, och söker utåt efter möjligheter för att utveckla sin effektivitet och sin säkerhet, hela tiden med hänsyn till mänskliga och organisatoriska faktorer.

4.5 OP – Verksamhet

Syfte

En korrekt styrning av den operativa verksamheten, av samverkan och av förändringar gör det möjligt för en organisation att uppfylla sina rättsliga förpliktelser, att reagera på ett flexibelt sätt på ändrade förhållanden och att skapa positiva beteenden hos sina anställda. Detta kommer i sin tur att göra det möjligt för organisationen att uppfylla sina affärsmål och affärsbehov.

Inledande kommentarer

Detta avsnitt innehåller de delar av säkerhetsstyrningssystemet som har att göra med samverkan (till exempel med entreprenörer, leverantörer och larmtjänster), förvaltning av tillgångar över tid och hantering av förändringar. Det är av avgörande betydelse för alla organisationer att hantera dessa områden på ett effektivt och verkningsfullt sätt till fördel för branschen som helhet. Det är den del av säkerhetsstyrningssystemet som tar upp de praktiska aspekterna av driften av ett järnvägsföretag eller en infrastrukturförvaltare. Det finns tydliga kopplingar i detta avsnitt till den övergripande tillsynen av säkerhetsstyrningssystemets effektivitet.

I detta område ingår även de delar av verksamheten som har den största förmågan att skada anseendet genom otillräcklig hantering av entreprenörer, leverantörer och samverkan. Detta avsnitt har starka kopplingar till den tekniska specifikation för driftskompatibilitet – Drift och trafikledning (TSD Drift och trafikledning) som fastställer grundläggande driftsförfaranden som ska följas på alla funktionella verksamhetsområden. Eftersom de nationella säkerhetsmyndigheterna måste verifiera efterlevnaden av TSD Drift och trafikledning är det nödvändigt att kontrollera dessa faktorer under tillsynens gång.

4.5.1 OP1 – Operativ planering och styrning

Syfte

Organisationen måste se till att de tekniska krav och verksamhetskrav som framkommer efter riskbedömningar tar hänsyn till de relevanta tekniska specifikationerna för driftskompatibilitet som avser delsystemen för drift och trafikledning. När nationella regler är tillämpliga uppfylls dessa genom planering, genomförande och granskning av de lämpliga verksamhetsprocesserna.

En högpresterande organisation har infört kraftfulla system för att uppnå efterlevnad med tekniska och operativa föreskrifter och har en kultur som stöder detta, och försöker alltid förbättra sig genom att ta hänsyn till innovationer inom järnvägssektorn och i andra branscher.

Nivå 1 – Otillräcklig

Operativa aktiviteter utförs utan hänvisning till mer långsiktiga strategier och andra affärsbehov. När operativa aktiviteter omfattar personalens kompetens och ledningen av personalen hanteras detta på ett slumpmässigt sätt.

Riskbedömningsprocesserna tillämpas inte på lämpligt sätt på den operativa verksamheten. Det förekommer liten eller ingen anpassning av styrningen av den operativa verksamheten till den faktiska verkligheten. I stället speglar styrningens utformning en idealiserad version av verkligheten. Ett resultat av detta är att mänskliga och organisatoriska faktorer inte beaktas för det operativa arbetet.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Det förekommer begränsad eller ingen efterlevnad av de grundläggande operativa principer som fastställs i TSD Drift och trafikledning.

Nivå 2 – acceptabel

Organisationen tar hänsyn till de relevanta tekniska specifikationerna för driftskompatibilitet och till nationella regler där så är tillämpligt, men detta sker inte på ett systematiskt sätt och tilläggsåtgärderna bygger inte tydligt på resultaten av riskbedömningar.

Personalen är medveten om de lokala rollerna och ansvarsområdena för den operativa verksamhet som påverkar dem men deltar inte i planeringen eller organiseringen av dem.

Viss utformning görs av operativa arbetsförfaranden, i synnerhet sådana som är av avgörande betydelse för säkerheten, men inte på ett systematiskt sätt. Mänskliga och organisatoriska faktorer beaktas bara i viss mån.

Organisationen uppfyller nätt och jämnt de minimivillkor för rättslig efterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Man efterlever TSD Drift och trafikledning men på minsta godtagbara nivå.

Nivå 3 – konsekvent

Som nivå 3 samt att när riskbedömningsprocessen tillämpas på den operativa verksamheten på ett konsekvent sätt tar den hänsyn till hanteringen av processer och förfaranden som utformats för att se till att exempelvis tåglägen planeras på lämpligt sätt och att de risker som är förbundna med den personal som sköter dem omfattas på lämpligt sätt.

Kompetensstyrningen samt informations- och kommunikationsprocesser tillämpas på ett konsekvent sätt på de operativa processerna.

Det finns en konsekvent process för att säkerställa att förfarandena som beskrivs återspeglar verkligheten bakom uppgiften. Mänskliga och organisatoriska faktorer beaktas på ett konsekvent sätt i organisationen.

Man efterlever TSD Drift och trafikledning på ett konsekvent sätt i organisationens hela verksamhet.

Nivå 4 – förebyggande

Som nivå 3 samt att det har införts system för styrning av den operativa verksamheten som bygger på riskbedömning i hela organisationen. Dessa system tar hänsyn till de dynamiska effekter som den operativa verksamheten på ett verksamhetsområde har på ett annat (signalkraven påverkar till exempel hur man tillhandahåller nödvändigt underhåll av spåren) och försöker förutse dessa för att avlägsna risker.

Personal i hela organisationen anammar en kultur som gör det möjligt för dem att bidra på ett positivt sätt till den operativa verksamheten och till eventuella förändringar av den.

Kommunikationen och informationsutbytet om den operativa verksamheten är robusta och processens effektivitet övervakas av den högsta ledningen.

Operativa förfaranden inbegriper samverkansarrangemang mellan olika uppgifter, däribland upphandlade arbetsuppgifter. Viss uppgiftsinsamling utförs som används för att fastställa mänskliga prestationer. Organisationens har ett proaktivt arbetssätt för att identifiera och styra mänskliga och organisatoriska faktorer i hela organisationen

De grundläggande operativa principer som fastställs i TSD Drift och trafikledning börjar användas som ett sätt att driva på en dynamisk verksamhetsfaktor i säkerhetsstyrningssystemet.

Nivå 5 – utmärkt

Som nivå 4 samt att organisationen hela tiden söker efter nya sätt att förbättra sin operativa verksamhet genom att använda sig av situationsanalys och framtidsspaning inom och utanför järnvägsbranschen. Personal på alla nivåer deltar i denna process och kan bidra till den.

Organisationen är proaktiv när det gäller att bedöma landvinningar i förståelsen mellan förfaranden och verkligheten bakom uppgifterna och försöker använda dessa landvinningar till att förbättra verksamhetens säkerhet och effektivitet. Som ett resultat har organisationen en god styrning av mänskliga och organisatoriska faktorer och ses som ledande inom området.

De grundläggande operativa principer som fastställs i TSD Drift och trafikledning utgör en integrerad del av en säker tågdrift och förespråkas aktivt av organisationen som god praxis i kontakterna med andra organisationer.

4.5.2 OP2 – Styrning och kontroll av operativa tillgångar

En framgångsrik styrning av tillgångar innebär att identifiera de tillgångar en organisation äger och förvaltar. Det innebär också att ha system på plats för att se till att tillgångarna fortsatt är i gott skick under sin livscykel och endast används inom sina avsedda verksamhetsområden, så att organisationen kan uppfylla sina affärsmål på ett säkert, effektivt och verkningsfullt sätt. I detta avsnitt hänvisas särskilt till alla tillgångar som är av avgörande betydelse för säkerheten. Hänvisningar till styrning av tillgångar betyder i detta sammanhang en styrning av tillgångens livscykel från utformning till bortskaffande. Avslutningsvis bör organisationen visa att den har tillämpat ett människocentrerat synsätt på varje stadium i tillgångens livscykel.

Nivå 1 – Otillräcklig

Aktivt och reaktivt schemalagt underhåll utförs men det finns ingen övergripande dokumentation över tillgångar, så organisationen kan inte vara säker på att alla tillgångar bibehålls i ett säkert skick.

Tillgångarna är utformade med begränsad hänsyn till framtida underhållsbehov, mänskliga faktorer eller möjligheten att bortskaffa tillgången på ett säkert sätt i slutet av dess livscykel.

Det finns få eller inga kriterier för utformning av ny utrustning.

Planen för underhåll av tillgångarna har luckor så att det inte är möjligt att vara säker på att tillgången har underhållits på ett korrekt sätt under sin livscykel.

Det utbyts information om tillgångarnas skick men den är ofullständig.

Det system som har införts för underhåll av tillgångar åtgärdar efterlevnaden av de viktigaste kraven för driftskompatibilitet där så är lämpligt.

Även om människor utbildas finns det få bevis för att det finns ett övergripande kompetenshanteringssystem.

Styrningen av dokumentation över tillgångar är inte aktuell.

Det finns inget system för att registrera användningsbegränsningar, och systemet för att ta artiklar ur drift och åter ta dem i drift är ofullständigt.

Utformningen av tillgångar inriktas på kommersiell tillgänglighet snarare än på att spegla användarens behov.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Det finns scheman för inspektion och underhåll av de flesta, men inte alla, tillgångar.

Inspektionsfrekvensen anges, men den vilar inte alltid på riskbasis.

Underlåtenhet att uppfylla inspektionsfrekvensen hanteras inte på ett tydligt sätt och eftersläpningar i arbetet uppstår på grund av detta.

Den övergripande policyn om förvaltning av tillgångar syftar inte på ett tydligt sätt till att förbättra säkerheten. En del tillgångar har utformats med avseende på säkerhetsfördelarna inklusive diskussion av frågor rörande mänskliga faktorer, men dessa är enstaka exempel som inte ingår i någon övergripande plan.

Inspektionsprocessen för tillgångar är drivkraften bakom förvaltningen av tillgångar, inte tillgångarnas skick. Informationsutbyte förekommer men ger inte en fullständig bild av tillgången från utformningen och framåt. Informationen om hur och när en tillgång ska bortskaffas är begränsad.

Det finns en bättre förteckning över tillgångar där tillämpningen av begränsningar av användningen anges för utrustning som åter tas i drift.

Utformningen bygger på en blandning av sunt förnuft, operativ erfarenhet och personliga preferenser snarare än ett strukturerat synsätt.

Organisationen uppfyller nått och jämnt de minimivillkor för rättslig efterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att förteckningen över tillgångar är aktuell, och inspektions- och underhållsschemana baseras på risk och följs.

Det kan förekomma en del eftersläpning av inspektionerna, men man är medveten om detta och hanterar det genom förmildrande åtgärder som införts för att minska risken.

Det förekommer viss granskning av inspektionsfrekvensen, och man har viss förmåga att anpassa sig till förändringar av tillgångens skick.

Tillgångarna används för det avsedda syftet samtidigt som deras avsedda driftsskick bibehålls och driftsproblem i normalt och försämrade skick åtgärdas. Det finns dokumentation av utformningen för de flesta tillgångar som inbegriper beaktande av mänskliga faktorer, och informationen i denna utgör en del av det referensskick jämfört med vilket inspektionerna utförs. De finns bortskaffningsplaner för de flesta tillgångar med en tydlig väg till ett styrt avlägsnande från tillgångsbasen.

Man använder sig av tillgängliga designstandarder för mänskliga faktorer och bästa praxis. Det finns ett testsystem för utformning som inbegriper frågor rörande mänskliga faktorer. Slut användarna har del i fastställandet av krav och i testprocessen. Processer för hantering av förändringar (se avsnitt 4.5.4 OP4 Hantering av ändringar) inbegriper frågor rörande mänskliga faktorer som en del av övervägandet av utformningen.

Nivå 4 – förebyggande

Som nivå 3 samt att inspektionsfrekvensen granskas systematiskt och är riskbaserad. Systemet medger flexibilitet för att kunna anpassa sig till förändringar i tillgångarnas skick både kort- och långsiktigt.

Det finns dokumentation av utformningen för alla tillgångar och alla tillgångar har en tydlig väg till ett styrt bortskaffande. Det finns en tydlig mekanism för att införliva information om förändringar av tillgångarnas skick inom ramen för processen för hantering av tillgångarna och bortskaffande av dem i slutet av deras livscykel.

Snarare än att reagera på förändringar i tillgångarnas skick försöker organisationen i förväg vara medveten om tillgångarnas föränderliga skick, till exempel genom användning av fjärrövervakning av tillgångar, och kan tilldela de nödvändiga resurser som krävs för att hantera detta.

Organisationen har en tydlig plan för utformning och förvaltning av framtida tillgångar som förbättrar säkerheten.

Återkoppling från slutanvändare om befintlig utformning används för att planera nya tillgångar. Att ta hänsyn till mänskliga faktorer är en integrerad del av utformningsprocessen.

Nivå 5 – utmärkt

Som nivå 4 samt att granskningar av inspektionsfrekvenser och inspektionsscheman inbegriper information som har sitt ursprung utanför organisationen eller järnvägsbranschen.

Organisationen försöker utveckla sin förvaltningspolicy för tillgångar genom att följa bästa praxis på området, både inom branschen och globalt.

Organisationen har ett övergripande förvaltningssystem för tillgångar som följer dessa från utformningen genom driften till bortskaffandet. Organisationen tillämpar det senaste tankesättet rörande tillgångsförvaltning för att se till att säkerheten förbättras och utvecklas över tid.

Fjärrförvaltningssystem för tillgångar ger detaljerad information om alla tillgångars skick och detta påverkar organisationens riskhanteringspolicy så att tillgången kan bibehållas i lämpligt skick.

Det finns ett övergripande kompetenshanteringssystem som hjälper personal som ansvarar för förvaltning av tillgångar att utvecklas och ser till att de utbildas på lämpligt sätt och har den nödvändiga kunskapen och kompetensen för att kunna utföra det arbete som de är ansvariga för.

Utformningar bygger på en ingående kunskap om vad tillgången är avsedd för och hur den används. Organisationen försöker använda sig av bästa praxis när det gäller mänskliga faktorer för att införskaffa, introducera, underhålla och bortskaffa tillgångar.

4.5.3 OP3 – Entreprenörer, partner och leverantörer

Organisationer behöver hantera säkerheten hos sina entreprenörer, partner och leverantörer på ett effektivt sätt, såväl som hos dem som påverkas av deras verksamhet, oberoende av var denna verksamhet utförs.

Detta är inte endast en fråga om riskbedömning och inte heller krävs det en förteckning över alla risker eller kategorier av relevanta risker, men det kräver att sökanden visar hur dennes system och förfaranden som helhet är utformade och organiserade för att underlätta fastställandet, bedömningen och kontrollen av dessa risker. Att använda sig av välskrivna avtal är ett allmänt accepterat sätt att hantera risker. Det främsta ansvaret för att hantera entreprenörer och kontrollera deras tillhandahållande av tjänster gentemot de fastställda specifikationerna ligger dock hos järnvägsföretaget/infrastrukturförvaltaren. Användningen av entreprenörer eller underentreprenörer betyder inte att järnvägsföretaget/infrastrukturförvaltaren delegerar något av sina ansvarsområden rörande att se till att de upphandlade tjänsterna utförs i enlighet med de standarder som fastställts före det att verksamheten inletts.

Sökanden bör visa att denne har processer på plats för att fastställa entreprenörers och andra leverantörers kompetens och bedöma deras säkerhetsprestanda som en del av sin upphandlingsprocess.

Huvudfaktorerna i entreprenörskontroll inbegriper

- en tydlig definition av avtalsvillkoren,
- att tydligt specificera arbetet,

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

- att välja entreprenören,
- att låta entreprenören bekanta sig med arbetsplatsen (i förekommande fall),
- att kontrollera produktsäkerheten och produktkvaliteten,
- arbetstillstånd (i förekommande fall),
- överlåtelse i slutet av arbetet, och
- övervakning och granskning av prestationen.

Frånvaron av eller en ofullständighet när det gäller någon eller alla faktorerna ovan är ett viktigt underlag för beslut i fråga om organisationens mognadsnivå.

Nivå 1 – otillräcklig

Den potentiella inverkan på säkerhetsprestandan hos det företag som använder en entreprenör bedöms inte och de därpå följande organisatoriska förändringarna hanteras inte på lämpligt sätt. Organisationen gör bristfälliga försök att identifiera eller samarbeta om arbete med andra organisationer med avseende på gemensam riskhantering. Avtalsvillkoren tar i förekommande fall inte hänsyn till säkerhetsrestriktioner och entreprenören är inte medveten om sitt säkerhetsansvar. Förfarandena för att åstadkomma detta är bristfälliga eller obefintliga. Ur kultursynpunkt finns det en tendens att inte utbyta information som är lämplig för riskhantering.

Ingen information samlas in eller utbyts och det finns inga krav på detta i avtalsvillkoren.

Entreprenörer utses när de behövs. När entreprenörerna väljs ut tar man dock inte hänsyn till mycket annat än kostnaden. Tidigare entreprenörers säkerhetsprestanda är till exempel inte ett urvalskriterium under upphandlingsprocessen. Det förekommer knapphändig planering av arbetet och det tas liten hänsyn till ansvaret för riskhanteringen när man bestämmer hur arbetet ska utföras.

Övervakning av entreprenörer och utvärdering av hur avtal uppfyllts görs bara i liten utsträckning. Arbetsätt för att hantera mänskliga och organisatoriska faktorer saknas i hög grad, och de arbetsätt som finns på området hanterar inte entreprenörer, partner och leverantörer.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Förfarandena identifierar verkligen samverkan mellan verksamhetsenheter på arbetsnivå. Det förekommer kontakter med andra organisationer rörande förfaranden och standarder som ska tillämpas, men detta görs inte på ett systematiskt sätt. Kontakterna används av personalen för en del gemensamma riskhantering som har fastställts på denna nivå.

Vissa faktorer i ett riskhanteringssystem har införts för styrning av entreprenörerna, men det tycks inte finnas någon systematisk process från urvalet fram till och med eftergranskningen av avtalet.

Arbetsätt för att hantera mänskliga och organisatoriska faktorer hanterar inte på ett tillräckligt sätt entreprenörer, partner och leverantörer.

Organisationen uppfyller nätt och jämnt de minimivillkor för rättslig efterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att organisatorisk samverkan med entreprenörer, partner och leverantörer fastställs på ett systematiskt sätt.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Förfaranden och standarder har införts för att hantera gemensamma risker med ett tydligt fastställande av vilken part som har ansvar för vad.

Det finns skriftliga mål för systemsäkerhet och man tar hänsyn till dessa mål när man utarbetar avtalsvillkor.

Regelbundna diskussioner förs med andra organisationer med vilka man samverkar för att komma överens om mål, normer, processer och arrangemang.

Det finns sätt att utbyta information på arbetsnivå.

Kommunikationerna utanför organisationen är tillräckligt goda för att se till att de personer som fattar beslut avseende riskhantering som korsar de organisatoriska gränserna innehar rätt information (i form av förfaranden och standarder), faktauppgifter och underrättelser samt anvisningar och rapporter.

Man är medveten om vikten av styrning av entreprenörerna och detta avspeglas i organisationens relevanta policyer.

Entreprenörerna väljs ut på grundval av sin förmåga att slutföra arbetet på ett säkert sätt och till en tillfredsställande standard.

Entreprenörens prestationer övervakas under avtalets löptid och lämpliga prestationsmått används för att spåra utförandet på ett effektivt sätt.

Arbetsätt för att hantera mänskliga och organisatoriska faktorer omfattar relevanta frågor som rör entreprenörer, partner och leverantörer, vilket ger dessa förståelse för sina roller och för sitt ansvar i fråga om styrningen av sin personal.

Nivå 4 – förebyggande

Beslut och åtgärder är förenliga med all den information som anges på nivå 3.

Det finns ett system för informationsutbyte genom hela organisationen för att främja effektiva granskningar och kontinuerlig förbättring.

Det finns ett systematiskt tillvägagångssätt när det gäller styrning av entreprenörerna.

Effektiva förhandskvalificeringsåtgärder gör att man har ett väl avvägt tillvägagångssätt som inbegriper att man tar hänsyn till de potentiella entreprenörernas säkerhetsprestanda.

Det finns en klar förståelse av ansvarsskyldighet på alla stadier av entreprenadarbetet. Goda arbetsförhållanden mellan kunden och alla entreprenörer skapas genom effektiva samverkansarrangemang, inklusive arbetsätt för att hantera mänskliga och organisatoriska faktorer som fungerar som fokus för organisationens relationer med entreprenörer, partner och leverantörer.

Prestationsmått och eftergranskning av avtalet fungerar som vägledning för beslut om valet av entreprenörer för ytterligare arbeten.

Det finns ett system som ser till att de relevanta besluten, kommunikationerna, osv. är spårbara.

Nivå 5 – utmärkt

Som nivå 4 samt att organisationen tittar på andra sektorer och länder för att kartlägga säkerhetsproblem på systemnivå och utvecklingsmöjligheter som kan ha en inverkan på deras hanteringssystem för entreprenörer, partner och leverantörer där så är lämpligt.

Samarbete mellan det upphandlande företaget och deras entreprenörer, partner och leverantörer används för att uppnå bästa möjliga resultat när det gäller gemensamma mål.

Man utbyter god praxis med andra organisationer, inklusive entreprenörer, partner och leverantörer.

Försörjningskedjan för entreprenörer gör att organisationens mål uppnås på ett friktionsfritt sätt.

Entreprenörens huvudsakliga och säkerhetsrelaterade verksamhet ligger i linje med organisationens egen.

Det görs ingen skillnad på behandlingen av entreprenörens anställda och företagets egna – alla får samma utbildning och information för att garantera deras säkerhet. Arbetsätt för att hantera mänskliga och organisatoriska faktorer är strukturerade så att alla parter omfattas på ett likvärdigt sätt.

4.5.4 OP4 – Hantering av ändringar

Syftet med förändringshantering är att se till att förändringar inom en organisation planeras på lämpligt sätt, genomförs i enlighet med krav på EU-nivå och följs upp för att hjälpa organisationen uppnå sina verksamhetsmål. En effektiv förändringshantering hanterar de risker som skapas av förändringen och hjälper organisationen att fatta rätt beslut för att förbättra sin verksamhet utan att kompromissa med säkerheten.

Processen för att hantera förändringar bör göra det möjligt att bedöma risker på ett proportionerligt och tillförlitligt sätt, inklusive frågor som rör mänskliga faktorer där så är lämpligt och att införa rimliga åtgärder för styrning.

Nivå 1 – otillräcklig

Man är medveten om vissa typer av förändringar och aspekter av dem hanteras.

Man identifierar inte alla risker förknippade med en förändring och tar därför inte hänsyn till dem.

Man överväger inte den effekt förändringen har på organisationens kultur.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Vikten av en bra förändringshantering förstås och det finns viss styrning av alla typer av förändringar.

Förändringar planeras men är inte alltid lämpliga.

Systemet för planering av förändringar är inte tydligt, vilket leder till att risker identifieras eller hanteras efter en förändring snarare än innan den genomförs.

Man tar inte mycket hänsyn till den effekt förändringen har på organisationens kultur.

Roller och ansvarsområden för hantering av förändringar och de därmed förknippade säkerhetsriskerna har inte tydligt fastställts.

Organisationen uppfyller nätt och jämnt de minimivillkor för rättslig efterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att det finns ett effektivt tillvägagångssätt för styrning av processrelaterade, organisatoriska och tekniska förändringar.

Förändringar kan hanteras genom en strukturerad strategi som omfattar ett antal steg i hanteringssystemet för förändringar.

Det finns en konsekvent strategi för riskbedömningar och riskhantering före och efter det att en förändring genomförs. Riskhantering är en avgörande del av förändringshanteringsprocessen.

Nivå 4 – förebyggande

Som nivå 3 samt att en genomgång görs efter att en förändring har genomförts för att hantera förändringens eventuella inverkan på organisationens kultur.

Det finns ett system för dokumentation av förändring där förändringen kan följas under hela förändringsprocessen.

Man är medveten om de fördelar som kommer av att låta personalen delta i förändringsprocessen.

Arbetsstättet för förändringshantering omfattar kontinuerlig planering, genomförande och styrning av förändringar av tillämpliga delar av organisationens säkerhetsstyrningssystem.

Förändringshanteringsprocessen inkluderar effekter av föreslagna förändringar på partner, leverantörer och andra som organisationen samverkar med.

Nivå 5 – utmärkt

Som nivå 4 samt att det också finns en förståelse för att förändringar påverkar andra aspekter av verksamheten. Detta leder till att man ser kopplingar mellan affärsrisker och säkerhetsrisker i samband med och som resultat av förändring.

De antaganden som görs om en förändring, initialt och under förändringens gång, utvärderas och lämpliga åtgärder införs ifall det visar sig att antagandena inte stämmer.

4.5.5 OP5 – Hantering av nödsituationer

Robusta system för krisplanering är viktiga för alla ansvariga och måste omfatta den information som ska kommuniceras till räddningstjänsten så att de kan utarbeta sina beredskapsplaner för större olyckor.

Krisplanering inkluderar

- att identifiera förutsebara kriser som kan inträffa,
- att utarbeta beredskapsstrategier för dessa kriser,
- att tillhandahålla lämplig utbildning och se till att de nödvändiga resurserna finns tillgängliga, och
- att testa planerna, tillsammans med andra personer och organisationer där så krävs.

Nivå 1 – otillräcklig

Identifiering av möjliga kriser och hur man ska agera om de inträffar sker bara i begränsad omfattning i organisationen.

Organisationen förlitar sig på att räddningstjänsten hanterar alla aspekter av en kris och har inte infört några strategier tillsammans med andra aktörer som kan vara inblandade i hanteringen av större olyckor annat än att ringa upp dem och låta dem hantera händelsen.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Organisationen följer de regler och den praxis som krävs av externa organ/organisationer såsom infrastrukturförvaltaren eller andra järnvägsföretag och har infört ett system för krishantering.

Större kriser som kan uppstå identifieras och det har till viss del införts planer för att hantera dem.

Personalen får utbildning i krisåtgärder endast när det är strikt nödvändigt.

Det finns krisinsatsrutiner som ofta har utarbetats av andra organ/organisationer och införts internt.

Organisationen uppfyller nätt och jämnt de minimivillkor för regelefterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att potentiella kriser som uppstår på grund av arbetsuppgifter identifieras i samband med riskbedömningarna.

Åtgärder för styrning, inklusive utbildning och resurser, har införts för att hantera kriser och kommuniceras med relevanta parter.

Gemensamma krishanteringsövningar genomförs med andra organisationer som deltar i en arbetsuppgift.

Det finns övergripande krishanteringsförfaranden som inbegriper andra organisationer, såsom räddningstjänsten eller de lokala myndigheterna där så är lämpligt.

Nivå 4 – förebyggande

Som nivå 3 samt att man använder sig av återkoppling från genomförda övningar när man gör genomgångar av organisationens arbetssätt för att säkerställa att krishanteringen fortsatt är aktuell och effektiv.

Det förekommer regelbundna kontakter mellan organisationen, räddningstjänsten och andra inblandade aktörer när större kriser inträffar för att säkerställa att man tar lämplig hänsyn till förändringar av processer/förfaranden och tekniska frågor och anpassar dem genom hela förändringshanteringsprocessen.

Nivå 5 – utmärkt

Som nivå 4 samt att organisationen använder god praxis vid krishantering, i synnerhet vad gäller samordning av gränssnitt mellan olika organisationer, både inom och utanför järnvägsbranschen. Man har regelbundna kontakter med räddningstjänsten proaktivt i syfte att utarbeta bättre gemensamma insatser för eventuella framtida kriser.

4.6 PE – Utvärdering

Syfte

Avsikten är att säkerställa att det finns riskhantering, att den fungerar som avsett och att den bidrar till att organisationens mål uppnås.

Inledande kommentarer

Organisationer måste mäta riskhanteringsverkningsfullhet för att se till att risker identifieras och hanteras i praktiken. Säkra arbetssätt måste följas upp för att säkerställa att de är lämpliga och att de faktiskt följs. Arbetssätt för övervakning och revision av riskhanteringen samt utvärdering av riskhanteringsprestanda bör införas för att säkerställa att säkerhetsstyrningssystemet fungerar på ett korrekt sätt.

Genom revision kontrolleras att organisationen gör vad den har sagt att den ska göra. Revisionen bör understödjas av regelbundna genomgångar för att säkerställa att organisationens verksamhetsmål är korrekta. Genomgångarna bör också undersöka om de strategier som har införts för att uppnå verksamhetsmålen fungerar som planerat.

Övervakning, revision och genomgång utgör ett återkopplande kretslopp inom det övergripande säkerhetsstyrningssystemet och utgör en viktig del av programmen för ständig förbättring och för att uppnå en utmärkt standard.

4.6.1 PE1 – Övervakning

Organisationen bör kunna visa att den har en process för övervakning av säkerhetsstyrningssystemets tillämpning och dess verkningsfullhet, och att denna process är lämplig för verksamhetens storlek, omfattning och typ. Organisationens bör kunna visa att processen kan identifiera, utvärdera och korrigera eventuella brister i säkerhetsstyrningssystemets funktionssätt.

Nivå 1 – otillräcklig

Det finns ingen effektiv process för att fastställa säkerhetsmål och samla in och analysera data. Det finns liten eller ingen förståelse av huruvida den riskhantering som införts fungerar på ett effektivt sätt.

Det finns inget medvetet affärsbehov av styrning och mätning inom områdena mänskliga och organisatoriska faktorer. Om de alls tas i beaktande så sker detta från fall till fall.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Organisationen ser inget behov av att ha uppsikt över sin säkerhetskultur.

Nivå 2 – acceptabel

Övervakning genomförs men ofta bara från fall till fall: en del processer ställs under tillsyn och en del utrustning inspekteras, vilket medför att arbetssätten för datainsamling inte är konsekventa.

Dokumentation av den övervakning som görs sammanställs och analyseras inte på företagsnivå. Följden är en strategi för handlingsplaner som inte är tydligt definierad och inte samordnad på företagsnivå.

Det finns ingen tydlig koppling mellan säkerhetspolicy, företagets säkerhetsmål och handlingsplaner för förbättringar. Övervakning av organisationens säkerhetskultur sker bara i begränsad omfattning.

Det finns ingen medvetenhet hos ledningen om behovet av att övervaka riskhanteringen, och man låter enskilda avdelningar och enheter bestämma vilken information som ska samlas in.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.

Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

Det finns en förståelse för att mänskliga och organisatoriska faktorer kan spela en roll i affärsprestandan men det saknas konsekventhet i tillämpningen av denna insikt.

Organisationen uppfyller nätt och jämnt de minimivillkor för regelefterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 3 samt att organisationen försöker använda tillämpliga delar av den gemensamma säkerhetsmetoden för att kontrollera den korrekta tillämpningen av säkerhetsstyrningssystemet och alla de processer och förfaranden som det omfattar, och genomför korrigerande åtgärder baserat på de exempel på bristande efterlevnad som har identifierats.

Övervakningen är processtyrd, så viktiga och sårbara system prioriteras inte över övervakningen av mindre viktiga eller sårbara system. Mätningar utförs för sin egen skull och utan ett tydligt fastställt syfte.

Kopplingen till riskbedömning begränsas till att identifiera riskhantering, som sedan övervakas på ett logiskt sätt.

En övervakningsstrategi fastställs och planer utarbetas för att tillämpa den. Detta leder till ett konsekvent tillvägagångssätt för att samla in och analysera data, och informationen används av ledningen för att fatta beslut och förbättra organisationen.

Resursfördelningen när det gäller övervakning prioriteras inte i enlighet med resultaten från riskbedömningen.

Säkerhetsstyrningssystemet innehåller en accepterad process för att, som en del av prestandautvärderingen, undersöka mänskliga och organisatoriska faktorer inverkan. Där så är nödvändigt finns tillgång till specialiserad expertkunskap för utvärdering av detta.

Organisationen har implementerat ett konsekvent arbetssätt för att övervaka sin säkerhetskultur.

Nivå 4 – förebyggande

Som nivå 3 samt att det finns förståelse för behovet av övervakning av viktiga och sårbara system.

Tillämpliga delar av den gemensamma säkerhetsmetoden är helt implementerade och övervakningen är helt igenom riskbaserad. Kritiska processer prioriteras vid resurstilldelningen.

Chefer och arbetsledare är välutbildade och har de resurser som krävs, och det finns bevis för att befintliga arbetssätt ifrågasätts för att identifiera deras eventuella brister.

Chefer på medel- och toppnivå övervakar resultaten på riskbasis och handlingsplaner samordnas och diskuteras på företagsnivå. Syftet med övervakningen är att förutsäga försämringen i säkerhetsprestandan och att hitta områden som kan förbättras, inte bara att mäta utfallet av organisationens säkerhetsstyrningssystem.

Det finns särskilda indikatorer för utvärdering av mänskliga och organisatoriska faktorer inverkan på tillämpningen av säkerhetsstyrningssystemet samt för att följa upp det arbete som görs för att säkerställa att man arbetar på ett effektivt sätt med dessa faktorer.

Övervakning av säkerhetskulturen sker på regelbunden basis och den information man får genom denna övervakning används för att förbättra strategin för kontinuerlig förbättring av säkerhetskulturen.

Nivå 5 – utmärkt

Som nivå 4 samt att avancerade verktyg används för övervakning. Organisationens har verktyg för att hjälpa anställda rapportera händelser och för att föreslå lösningar att diskutera i handlingsplanerna.

Dataanalyser ses som en konkurrensfördel och övervakningen av säkerhetsprestandan ingår i en global övervakningsprocess som omfattar alla enheter och avdelningar. Organisationen har ett övergripande datahanteringssystem för att kartlägga sina tillgångar och deras användningsvillkor.

Företaget är medvetet om vikten av att använda riskmodeller och utbyta uppgifter och information med andra järnvägsföretag för att utöka sina datamängder och förbättra kvaliteten på data som används för riskbedömning.

Rapportering sker enligt god praxis och det finns innovativa projekt, stödda av organisationens arbete för att förbättra säkerhetskulturen, för att främja en stark säkerhets- och rapporteringskultur inom organisationen.

Organisationen gör genomgångar av förfaranden för övervakning för att säkerställa att de hela tiden är relevanta för organisationens riskprofil.

Data från övervakning av organisationens arbete med att styra mänskliga och organisatoriska faktorer inverkan är väsentlig för arbetet med kontinuerliga förbättringar inom organisationen. Resultaten används när man fattar beslut i affärsfrågor och frågor som rör säkerhetsstyrningen. Den information som erhålls delas med partner, leverantörer och entreprenörer.

Organisationens arbetssätt för att övervaka sin säkerhetskultur är ett gott exempel på hur sådant arbete bör bedrivas i och utanför organisationen.

4.6.2 PE2 – Internrevision

En internrevision är en oberoende och systematisk undersökning av organisationens system för riskhantering och ledningens metoder för att säkerställa att verksamhetsmålen uppfylls. Internrevision krävs också enligt den gemensamma säkerhetsmetoden för övervakning. Revisioner är vanligen utformade för att begränsa subjektiviteten hos den/de som genomför revisionen till förmån för ett mer evidensbaserat tillvägagångssätt. Den systematiska naturen hos en revision av säkerhetsstyrningssystemet avser att ge organisationens högsta ledning tydliga bevis som kan användas som grund för beslut om att förbättra säkerhetsnivån.

Nivå 1 – otillräcklig

Det finns få eller inga bevis för att revisioner genomförs.

De revisioner som utförs är inte planerade eller prioriterade, och man agerar inte utifrån revisionsfynden.

Revisorer utbildas inte på ett konsekvent sätt och kopplingen till organisationens kompetensstyrning är ofullständig.

Revisionsprocessen är inte strukturerad, och det finns ingen reell skillnad mellan revisioner och inspektioner.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Det förekommer en del revisioner, men de metoder som används och de områden som omfattas tar inte hänsyn till det särskilda riskhanteringssystemets natur.

Det finns planer för revisioner men dessa är inte samordnade.

Organisationen uppfyller nått och jämnt de minimivillkor för regelefterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att det finns bevis på ett samordnat, effektivt och planerat tillvägagångssätt för revisioner. Revisionsverksamheten är inriktad på att uppnå regelefterlevnad och på att uppnå verksamhetsmålen.

Revisionerna och deras resultat dokumenteras på ett systematiskt sätt. Organisationens styrelse känner till resultaten och diskuterar dessa på regelbundna styrelsesammanträden.

Kompetensstyrningssystemet innehåller bestämmelser om utbildning av revisorer och man upprätthåller ett register över kompetenta revisorer.

Nivå 4 – förebyggande

Som nivå 3 samt att revisionsverksamheten planeras och prioriteras med hänsyn till resultat från tidigare revisioner och resultat från övervakningen.

En lämplig kombination av revisionsmetoder används för att inhämta information om organisationens prestanda jämfört med verksamhetsmålen.

Den högsta ledningen informeras om resultatet av revision, vilket ger dem förutsättningar för genomgång av säkerhetsstyrningssystemet. På denna nivå analyseras den kontinuerliga förbättring som görs utifrån säkerhetsstyrningssystemets krav för att undersöka om förbättringarna faktiskt leder till de förväntade fördelarna eller om de måste modifieras för att förbättra resultaten.

Nivå 5 – utmärkt

Samma som för nivå 4 med tillägg av att organisationens verksamhet vid revisionen genomförs mot mer krävande verksamhetsmål och mot bästa praxis.

Mål för kollegiala revisioner ingår.

4.6.3 PE3 – Ledningens genomgång

Ett kraftfullt ledarskap är av avgörande betydelse för att en organisations säkerhetsstyrning ska fungera på ett effektivt och verkningsfullt sätt samt fortsätta utvecklas över tid. Organisationen bör visa att ledningen aktivt deltar i genomgångar av säkerhetsstyrningssystemets prestanda och i att utveckla detta för framtiden. Ledningens genomgång kan ses som en del av en organisations arbete med att säkerställa att dess processer och förfaranden leder till de önskade resultaten.

Nivå 1 – otillräcklig

Det förekommer ringa analys från högsta ledningens sida av resultaten från övervakning och revisioner. Detta görs snarare på enhets-/avdelningsnivå.

Det görs inte regelbundna genomgångar av verksamhets- och säkerhetsmålen.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

De genomgångar som utförs ingår inte i en ordnad strategi för förbättring. De är ofta reaktiva och planeras oftast inte som en del av ledningscykeln.

Organisationen uppfyller nätt och jämnt de minimivillkor för regelefterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt att ledningen automatiskt använder resultaten från övervakning och revisioner för genomgångar av organisationens prestanda och gör ändringar där så behövs.

Rekommendationerna från genomgångarna fördelas på ett tydligt sätt i organisationen och följs upp. Rekommendationerna visar att man tar hänsyn till ett större sammanhang.

Nivå 4 – förebyggande

Som nivå 3 samt att man drar lärdom av incidenter i andra organisationer och andra branscher.

Ledningen ber personalen om förslag på förbättringar i affärsprocesserna och vid genomgång av dessa förslag tittar man på förslagens eventuella inverkan på affärsverksamheten.

Nivå 5 – utmärkt

Som nivå 4 samt att ledningen genomför slumpvisa genomgångar av praxis på särskilda områden i företaget för att undersöka om processer och förfaranden fortfarande är ändamålsenliga.

Ledningen använder sig av situationsanalys och framtidsspaning i syfte att identifiera ny teknik eller nya idéer som kan förbättra verksamheten. Man överväger till exempel användning av stordata för att förbättra verksamhetens effektivitet och säkerhetsprestanda.

4.7 I – Förbättringar

Syfte

Organisationer måste utvecklas över tid, eftersom de annars kommer att stagnera och bli självbelåtna. Detta får förr eller senare följder för säkerhetsstyrningen. Organisationen bör omfatta en filosofi av att använda lärdomar från egna och andras misstag för att förbättra sin säkerhetsstyrning. Filosofin bakom förbättring är att organisationen ska inriktas på att tänka framåt, att försöka förutse kommande förändringar och se till att dessa förändringar, när de inträffar, leder till att säkerhetsstyrningssystemet utvecklas på ett positivt sätt.

Inledande kommentarer

En organisation kan förbättra sig genom att dra lärdom av sina egna utredningar av olyckor och incidenter (inklusive tillbud och farliga händelser) samt av andra händelser som inträffar inom järnvägssektorn eller andra industrisektorer. Organisationer bör även utreda tillbud lika noggrant som de skulle utreda en olycka för att förstå vad som var på väg att hända, hur situationen uppstod och hur liknande händelser kan undvikas. Sammanfattningar av utredningar och deras resultat bör kommuniceras i hela organisationen och med andra liknande organisationer så långt som det är möjligt. Organisationer bör vara proaktiva i sin strävan att försöka lära sig att förbättras och dra lärdomar av olyckor och incidenter men också utifrån andra tillgängliga informationskällor som finns att tillgå, såsom övervakning, revisioner och andras erfarenheter som kan hjälpa organisationen att förbättras.

4.7.1 I1 – Lärdomar av olyckor och tillbud

Utredning av olyckor och incidenter bör inkludera genomgång av säkerhetsstyrningssystemets prestanda under upptakten till händelsen och undersöka vilka delar av systemet som fungerade väl och vilka områden som kräver förbättring, inklusive eventuella lärdomar som man har dragit om mänskliga prestationer. Organisationen bör också försöka dra lärdom av resultaten av de utredningar som har gjorts av det nationella utredningsorganet, andra nationella utredningsorgan inom EU och av incident- och olycksutredningar från hela världen.

Nivå 1 – otillräcklig

Det finns få bevis för att effektiva utredningar utförs, och organisationens kultur går ut på att hitta någon att skylla på. Man drar inga lärdomar av incidentutredningar som genomförs utanför organisationen eller i andra branscher. Kompetensen hos de personer som utför utredningarna kan ifrågasättas.

Det finns få eller inga tecken på att människans roll i olyckor och incidenter beaktas på lämpligt sätt.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 2 – acceptabel

Incidenter utreds men det finns inte mycket vägledning till hur utredningen ska gå till eller vad som ska utredas.

Omedelbara orsaker utreds.

Det urval incidenter som utreds begränsas i huvudsak till olyckor, och de rekommendationer som blir resultatet av utredningarna begränsas till att förhindra att samma sak sker igen. Områden för mer omfattande förbättringar identifieras inte.

Det förekommer vissa försök att lära sig av andra olyckor i olika delar av branschen.

Personal som kan utföra utredningar har fått en del utbildning men inte som en del i ett effektivt kompetensstyrningssystem.

Det finns en medvetenhet om att mänskliga och organisatoriska faktorer spelar en roll i olyckor och incidenter och man försöker till viss del att utforska detta i utredningarna, men detta går ofta förlorat när rapporterna godkänns på ledningsnivå. Även om det finns en förståelse för att dessa faktorer kan ha betydelse för olyckor och incidenter så ligger fokus fortfarande på att hitta syndabockar snarare än att hantera systemiska brister i organisationen.

Organisationen uppfyller nått och jämnt de minimivillkor för regelefterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Nivå 3 – konsekvent

Som nivå 2 samt det finns standardiserade upplägg för när och hur utredningarna utförs.

I utredningarna utreds underliggande orsaker och utredningar genomförs även efter incidenter.

Personalen har fått övergripande utbildning i olycks- och incidentutredningar som en del i ett kompetensstyrningssystem.

Beaktandet av mänskliga och organisatoriska faktorerers betydelse för olyckor och incidenter är en standardaspekt vid utredning. Ledningen anser att dessa är lika viktiga som andra orsaker till en händelse och arbetar för att korrigera problem när de uppstår. Det finns en stark betoning på uppfattningen om en rättvis kultur där fokus ligger på att identifiera vad som gått fel, snarare än att hitta syndabockar.

Nivå 4 – förebyggande

Som nivå 3 samt att utredningarnas kvalitet leder till rekommendationer som kan tillämpas både inom och utanför organisationen.

Det urval av incidenter som utreds inbegriper, i tillämpliga fall, störningar av arbetet och förekomst av resultat som inte uppfyller förväntningarna.

Den högsta ledningen informeras om resultaten av utredningarna och om rekommendationerna och ser till att de implementeras i tillämpliga fall.

Rekommendationer från incidentutredningar i andra järnvägsföretag eller affärsverksamheter utanför organisationen studeras för att se om resultaten är av relevans för verksamheten.

Organisationen försöker använda de lärdomar om mänskliga och organisatoriska faktorer som kan dras av egna och andras utredningar inom järnvägsbranschen och utanför denna, och att implementera dessa inom ramen för sitt säkerhetsstyrningssystem. Organisationen framstår som en rättvis organisation. Det förekommer inget skuldbeläggande.

Nivå 5 – utmärkt

Som nivå 4 samt att det finns en förståelse för innebörden av resultaten av andra organisationers utredningar.

Det finns en villighet att lära sig av incidenter genom att förändra beteenden i hela verksamheten.

Den högsta ledningen deltar i att sprida sina egna erfarenheter till andra företag i järnvägssektorn och bortom denna, och agerar utifrån lärdomar som dragits av andra järnvägsföretag eller i andra branscher.

Organisationen strävar efter att lyfta fram lärdomar om mänskliga och organisatoriska faktorer som har dragits från olyckor och incidenter, och vikten av en rättvis och lärande kultur, i kommunikationen med partner, leverantörer och entreprenörer och i en vidare krets.

4.7.2 12 – Kontinuerlig förbättring

Organisationen behöver visa att de hela tiden försöker förbättras genom att dra lärdom av händelser, kontakter med tillsynsmyndigheter och på andra sätt. Vid tillsyn förväntas organisationerna visa att de har ett förfarande för att identifiera och genomföra positiva förändringar av sina säkerhetsstyrningssystem, bland annat genom sitt arbete med kontinuerliga förbättringar av säkerhetskulturen. Korrigerande åtgärder omfattar fastställandet, fördelningen i organisationen och genomförandet av de åtgärder som identifierats som nödvändiga baserat på övervakning, utredning, revisioner och genomgångar.

Nivå 1 – otillräcklig

Trots processerna och förfarandena i organisationens säkerhetsstyrningssystem resulterar övervakning, revisioner och genomgångar i små eller inga förändringar, antingen på grund av att de inte utförs alls eller att de inte följs upp.

Organisationen når inte upp till den nivå som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Incidenter och olyckor "kommer alltid att hända" – en fatalistisk kultur dominerar. Det finns ingen riktig strategi för kontinuerlig förbättring av säkerhetskulturen. Den mänskliga faktorn i utförandet av arbetsuppgifter fastställs alltid som orsak och det görs inga försök att driva utredningarna vidare. Det finns ingen rättvisekultur och de personer som är inblandade i incidenter och olyckor görs ofta till syndabockar. Ledningen och personalen är i allmänhet ointresserade av säkerhet och använder eventuellt säkerhet endast som grund för andra argument, såsom lön, arbetstid, osv.

Nivå 2 – acceptabel

Enkla rön från övervakning, utredningar, revisioner och genomgångar ger upphov till enkla åtgärder och förändringar av säkerhetsstyrningssystemets lägre nivåer. I hela organisationen görs få försök att utifrån en systematisk genomgång av information inhämtad från övervakning, utredning och revisioner söka efter underliggande orsaker till problem.

Organisationen uppfyller nätt och jämnt de minimivillkor för regelefterlevnad som förväntas av en innehavare av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

Säkerhetsavdelningen uppfattas som ansvarig för säkerheten, men ledningen lägger ner tid och arbete på att förebygga incidenter och olyckor eftersom dessa ses som möjliga att förebygga. Det finns en strategi för kontinuerlig förbättring av säkerhetskulturen som omfattar rätt områden, men de korrigerande åtgärderna inriktas främst på fel orsakade av den mänskliga faktorn i utförandet av arbetsuppgifter och avhjälpas genom negativa åtgärder såsom straff eller liknande för att minska farliga beteenden, eftersom dessa anses vara orsaken till incidenter och olyckor. Kulturen är alltså inte alltid rättvis. Säkerhetsprestandan mäts i eftersläpande indikatorer såsom arbetsskador som lett till frånvaro, medicinska skador, urspårningar, obehöriga stoppsignalpassager, osv. Organisationens incidenter och olyckor är fler eller av allvarligare karaktär än dess konkurrenters.

Nivå 3 – konsekvent

Som nivå 2 samt att det finns en process för att säkerställa att nödvändiga åtgärder som identifierats genom övervakning, revisioner och genomgångar genomförs och för att identifiera vem som har ansvar för åtgärderna och tidplanen för att genomföra dem.

Det finns förfaranden för övervakning av säkerhetsstyrningssystemets lämplighet, tillräcklighet och verkningsfullhet som tar hänsyn till det ramverk som fastställs i den gemensamma säkerhetsmetoden, och dessa förfaranden leder till konsekventa resultat.

Korrigerande åtgärder kan vidtas på alla nivåer av säkerhetsstyrningssystemet.

Ledningen är medveten om att incidenter och olyckor orsakas av flera olika faktorer, och att vissa av dessa har sitt ursprung i ledningsbeslut. Allvarliga incidenter och olyckor utreds och en systematisk process har inletts för att dra lärdom av dem. Det finns en konsekvent strategi för kontinuerlig förbättring av säkerhetskulturen och denna strategi är välkonstruerad och kan bedömas utifrån sitt resultat. Organisationen odlar en rättvis kultur.

Nivå 4 – förebyggande

Samma som för nivå 3 men med mekanismer för att göra framsteg spårbara och genomföra korrigerande åtgärder fullt ut.

De korrigerande åtgärderna är kopplade till mål som fastställs i säkerhetsstyrningssystemet.

Resultaten av säkerhetsmål och säkerhetsplanering, riskbedömning, personals och andra parter medverkan, information och kommunikationer, övervakning, revisioner, ledningens genomgångar och lärdomar från olyckor och incidenter används för att utarbeta strategier och planer för kontinuerlig förbättring.

Analyser av underliggande orsaker utförs för alla incidenter och olyckor, och man accepterar att de flesta har sitt ursprung i ledningsbeslut. Det finns en förståelse för att alla är ansvariga inte endast för sin egen säkerhet utan även för sina kollegers. Ledningen och personalen behandlar varandra med respekt och det finns en systematisk strategi för att säkerställa rättvis behandling. Man förespråkar en hälsosam livsstil och olyckor utanför arbetstid övervakas. Strategin för kontinuerlig förbättring av säkerhetskulturen och för att odla en rättvis kultur följer bästa praxis med realistiska och mätbara mål.

Nivå 5 – utmärkt

Som nivå 4 samt att korrigerande åtgärder leder till att ledningen går igenom liknande processer utanför det omedelbara område där incidenten inträffade för att utröna om det finns liknande brister och identifiera eventuella förändringar som måste genomföras.

Organisationen prioriterar att förebygga incidenter och olyckor som leder till fysiska och psykologiska skador hos personalen eller hos tredjeparter. Organisationen har inte haft någon registrerbar incident eller olycka på flera år, men man känner sig ändå inte självbelåten. Gradvis beteendemässig eller organisatorisk försämring övervakas hela tiden och åtgärder inleds för att förhindra att detta sker. Organisationen använder sig av en rad ledande indikatorer för att övervaka prestandan. Organisationens strategi för att kontinuerligt förbättra säkerhetskulturen och organisationens sätt att odla en rättvis kultur anses i branschen vara ledande på området och följa bästa praxis inom och utanför järnvägssektorn.

En ifrågasättande kultur genomsyrar organisationen och förändringar granskas ingående.

Bilaga – Vägledning rörande nivåer

Mognadsnivåer	Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5
Benämning	Otillräcklig	Acceptabel	Konsekvent	Förebyggande	Utmärkt
Kortfattad definition	På denna nivå har den organisation som bedöms ett säkerhetsstyrningssystem, men det står klart att det finns brister som drar ner prestandanivån till under det som krävs för beviljandet av ett gemensamt säkerhetsintyg eller säkerhetstillstånd. Det finns förfaranden och anvisningar för styrning av säkerhetsverksamhet, men under tillsynen står det klart att det finns allvarliga problem om hur sammanhängande dessa är som helhet. Enskilda risker hanteras, men de övergripande processerna som styr detta är bristfälliga. Organisationen verkar i praktiken på ett sätt som verkar ha stora brister när det gäller överensstämmelsen med det sätt som beskrivs i säkerhetsstyrningssystemet. Ledande principer, förfaranden och anvisningar tycks tillämpas på sätt som inte stämmer överens med de	På denna nivå presterar organisationen på miniminivån för regelefterlevnad, det vill säga att säkerhetsstyrningssystemet fungerar på en nivå som var tillräcklig för att ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd skulle beviljas på bedömningsstadiet. Det finns ett dokumenterat säkerhetsstyrningssystem som används för att styra säkerhetsrisker, men det har brister när det gäller struktur och samordning. Systemet är sammanhängande i det stora hela, men det finns luckor och en del bristande överensstämmelse vad gäller strategin på olika områden. Organisationen klarar i huvudsak av att uppfylla sina skyldigheter när det gäller säkerhet, men med knapp nöd. Det skulle inte behövas mycket för att ett betydande problem skulle skapas och	Säkerhetsstyrningssystemet har utvecklats för att skapa en systematisk och konsekvent strategi för riskhantering. Alla delar är på plats och fungerar, och alla säkerhetsaspekter har beaktats. Säkerhetskulturen inom organisationen övervägs till viss del. Samtidigt som organisationen är konsekvent försöker man inte förebygga risker i förväg och inte heller är kulturen inom organisationen tillräckligt utvecklad för att riskhanteringsprocessen ska vara självgående. Brandsläckningsstrategin har ersatts av en mer väl övervägd strategi för riskhantering, men det skulle inte behövas mycket (t.ex. brister i hanteringen av centrala processer eller arbetssätt över tid) för att	När det gäller nivå 3 och därutöver hanterar säkerhetsstyrningssystemet kontinuerligt risker på ett proaktivt sätt. Här övervakar organisationen förebud till risker och vidtar åtgärder i förväg för att förhindra att farliga incidenter uppkommer. Organisationen har åtagit sig att utveckla en säkerhetskultur, och de anställda är engagerade i att styra säkerheten på ett konsekvent och framåtblickande sätt. På denna nivå förekommer det sant ledarskap från organisationens ledning och personalen tror på och respekterar ledningens strategier. Mycket arbete ägnas åt att regelbundet granska prestandan och att förstå beskaffenheten hos de risker organisationen möter och vad som kan göras åt dem.	Vad gäller nivå 4 och därutöver har det skriftliga säkerhetsstyrningssystemet utformats på ett sätt som möjliggör kontinuerliga förbättringar. Organisationen söker aktivt efter möjligheter att förbättra säkerheten och utvecklar sin säkerhetskultur på ett positivt sätt med hjälp av information både inifrån järnvägsbranschen och utifrån. Organisationen jämför sin egen prestanda med andra organisationers, både inom och utanför järnvägssektorn. Det finns bevis för att man i organisationen är medveten om de problem den har eller kan komma att ha i framtiden och aktivt försöker åtgärda dem genom säkerhetsstyrningssystemet. På denna nivå litar organisationen på sin förmåga att hantera de risker den möter och vänder sig utåt för att utbilda dem som den samverkar med, och den försöker dra lärdom från andra områden som kan införlivas i verksamheten.

The NSA SE has kindly provided its assistance to the revision of the translation of this guide.
Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

	<p>sätt som anges i säkerhetsstyrningssystemet, och därför hanteras inte nödvändigtvis de risker som följer av organisationens och dess entreprenörers verksamhet på lämpligt sätt. På denna nivå bör den nationella säkerhetsmyndigheten överväga att vidta åtgärder för att få organisationen att åter uppnå lagefterlevnad (se byråns vägledning till en modell för verkställighetsförvaltning för mer information om hur denna process kan fungera).</p>	<p>organisationen skulle falla tillbaka till nivå 1 på grund av att bristen på integrering mellan förfaranden och riskhantering kan bli ett stort problem när det gäller tekniska, operativa och organisatoriska risker. En del områden inom verksamheten klarar sig bättre när det gäller säkerhetsstyrning än andra. Riskerna begränsas mer genom organisationens anställdas handlingar än genom säkerhetsstyrningssystemets utformning. En brandsläckningsstrategi för riskhantering är mer regel än undantag, vilket gör att företaget agerar reaktivt när det gäller olyckor och incidenter i stället för att proaktivt vidta åtgärder för att förhindra dem.</p>	<p>organisationen ska falla tillbaka till nivån acceptabel.</p>		<p>Säkerhet är en integrerad del av organisationens verksamhet.</p>
--	--	--	---	--	---



The NSA SE has kindly provided its assistance to the revision of the translation of this guide.
Where it appears that there are differences between the translated version and the English version, the English version takes precedence.