

Vi ser till att järnvägssystemet
fungerar bättre för samhället.

Vägledning

Krav på säkerhetsstyrningssystem för gemensamt säkerhetsintyg eller säkerhetstillstånd

	<i>Utarbetade av</i>	<i>Godkända av</i>	<i>Fastställd av</i>
<i>Namn</i>	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
<i>Befattning</i>	Projektansvarig	Projektledare	Enhetschef
<i>Datum</i>	04/09/2018	04/09/2018	04/09/2018
<i>Underskrift</i>			

Dokumenthistorik

<i>Version</i>	<i>Datum</i>	<i>Kommentarer</i>
1.0	29/06/2018	Sista version för publicering
1.1	10/07/2018	Figur 2 uppdaterad, bildtext tillagt till Figur 3
1.2	04/09/2018	Figur 2 uppdaterad

Detta dokument är en icke juridiskt bindande vägledning från Europeiska unionens järnvägsbyrå. Den påverkar inte de beslutsprocesser som föreskrivs i gällande EU-lagstiftning. Dessutom är det endast Europeiska unionens domstol som har befogenhet att tolka unionslagstiftningen på ett bindande sätt.

0 Inledning

I en ansökan om ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd ska det framgå att de säkerhetsstyrningssystemkrav som fastställs i kommissionens delegerade förordning (EU) 2018/762 som är relevanta är uppfyllda [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*]. Den sökande ska därför tillhandahålla dokument till den nationella säkerhetsmyndigheten eller, i förekommande fall, Europeiska unionens järnvägsbyrå (nedan även kallad *järnvägsbyrån*), som styrker att säkerhetsstyrningssystem har inrättats i enlighet med artikel 9 i direktiv (EU) 2016/798.

Denna vägledning är ett levande dokument som har utarbetats i samarbete med nationella säkerhetsmyndigheter och branschföreträdare, i avsikt att utvecklas över tid genom bidrag från användare och med hänsyn till de erfarenheter som görs vid tillämpningen av direktiv (EU) 2016/798, relaterade gemensamma säkerhetsmetoder och övrig relevant EU-lagstiftning.

0.1 Vägledningens syfte

Denna vägledning har tagits fram i följande syften:

- *Förklara avsikten med de bedömningskrav som fastställs i bilagorna I och II till ovannämnda gemensamma säkerhetsmetoder, vid behov kompletterade med förklarande anmärkningar med detaljerad information om särskilda termer eller idéer i kraven.*
- *Ange vilka bevis en organisation kan tillhandahålla för att styrka att kraven i ovannämnda gemensamma säkerhetsmetoder efterlevs.*
- *Ge en förteckning över exempel på bevis som vid bedömningen kan observeras i ansökningar om gemensamt säkerhetsintyg eller säkerhetstillstånd, eller som kan användas av den sökande som referensmaterial vid ansökan.*
- *Ge exempel på referenser och standarder som kan användas som hjälpmedel vid bedömning, utveckling, genomförande eller kontinuerlig förbättring av säkerhetsstyrningssystem.*
- *Ange vilka typer av problem nationella säkerhetsmyndigheter kan behöva beakta när de genomför tillsyn av järnvägsföretag eller infrastrukturförvaltare.*

Notera: I bedömningen av en ansökan för gemensamt säkerhetsintyg rörande transport av farligt gods på järnväg, kan en nationell säkerhetsmyndighet ha en direkt roll som ansvarig myndighet i bedömningen av relevanta delar av ansökan. Alternativt kan den nationella säkerhetsmyndigheten ha en koordinerande roll som när nödvändigt kontaktar andra myndigheter ansvariga för transport av farligt gods, för att söka deras råd för de relevanta delarna i bedömningen.

0.2 Vem är denna vägledning till för?

Detta dokument riktar sig till följande:

- *Nationella säkerhetsmyndigheter och Europeiska unionens järnvägsbyrå när de bedömer hur järnvägsföretagens säkerhetsstyrningssystem uppfyller relevanta säkerhetsstyrningssystemkrav och nationella säkerhetsmyndigheter när de genomför tillsyn.*
- *Nationella säkerhetsmyndigheter när de bedömer hur infrastrukturförvaltarens säkerhetsstyrningssystem uppfyller relevanta säkerhetsstyrningssystemkrav och när de genomför tillsyn efter tilldelning av kontrakt.*
- *Järnvägsföretagen och infrastrukturförvaltare (nedan även kallade sökande) för att hjälpa dem att utveckla, genomföra, underhålla och kontinuerligt förbättra sina säkerhetsstyrningssystem i enlighet*

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.

med relevanta säkerhetsstyrningssystemkrav (och andra tillämpliga säkerhetsföreskrifter) och för att de ska veta vad de kan förvänta sig under tillsynen.

0.3 Omfattning

Denna vägledning innehåller inga föreskrifter om vilka bevis en sökande bör lägga fram. Den grundläggande orsaken till detta är att varje organisations säkerhetsstyrningssystem ska skräddarsys efter de specifika risker organisationen i fråga behöver kontrollera. Varje säkerhetsstyrningssystem är alltså ett unikt system av dokumenterad information som ger en indikation om vilka specifika åtgärder och system för riskkontroll som finns på plats inom en enskild organisation. Systemet utvecklas över tid i takt med att organisationen förändras. Att föreskriva vilken information en sökande bör tillhandahålla skulle därför inte vara korrekt. Det skulle göra bedömningsprocessen meningslös eftersom alla ansökningar skulle se likadana ut, även om säkerhetsstyrningssystemen är olika.

0.4 Vägledningens struktur

Detta dokument ingår i järnvägsbyråns vägledningskompendium till stöd för järnvägsföretag, infrastrukturförvaltare, nationella säkerhetsmyndigheter och järnvägsbyrån i utövandet och genomförandet av deras roller och uppdrag i enlighet med direktiv (EU) 2016/798.



Figur 1: Förteckning över byråns vägledningar

Informationen som tillhandahålls i denna vägledning ska kompletteras med specifika riktlinjer från nationella säkerhetsmyndigheter, som beskriver och förklarar innebörden av de anmälda nationella regler som gäller för det avsedda området för verksamheten och de dokument som ska bifogas ansökan om ett gemensamt säkerhetsintyg i enlighet med föreskrifterna i artikel 10.3 b och artikel 10.8 i direktiv (EU) 2016/798 (se även

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.

Ansökan om gemensamt säkerhetsintyg – en vägledning för myndigheter). För infrastrukturförvaltare gäller att den här vägledningen ska kompletteras med vägledning från den nationella säkerhetsmyndigheten, gällande kraven för säkerhetstillstånd som beskrivs i artikel 12.1 i direktiv (EU) 2016/798. Med anmälda nationella regler avses endast de regler som anmälts till kommissionen av en medlemsstat. I enlighet med skäl 12 i direktiv (EU) 2016/798 förväntas antalet anmälda nationella regler minska över tid. Dessa kommer antingen att ersättas av åtgärder som fastställts i tekniska specifikationer för driftskompatibilitet (TSD), andra EU-förordningar eller företagsregler. Företagsregler eller företagsstandarder kommer i förekommande fall att bedömas utifrån förenlighet med den TSD som hör samman med delsystemen för drift och trafikledning på järnvägsnätet i Europeiska unionen (nedan även kallad *TSD drift och trafikledning*), vilket återspeglas genom de säkerhetsstyrningssystemkrav som förklaras i denna vägledning.

Denna vägledning är upplagd enligt samma struktur som de krav som fastställs i bilaga I och bilaga II i kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*]. I avsnitten nedan visas varje krav i en gul ruta för att underlätta hänvisningar. I de fall det förekommer skillnader mellan de krav som gäller järnvägsföretag och dem som gäller infrastrukturförvaltare visas de krav som gäller de sistnämnda i **blått**.

En jämförelse sida vid sida eller jämförelsetabeller mellan bedömningskriterierna i de tidigare förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010, och föreskrifterna i kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] görs i bilaga 1 till denna vägledning. Tabellerna innehåller också korshänvisningar till punkterna i ISO-högnivåstrukturen (*ISO High Level Structure*), i förekommande fall. Dessa tillhandahålls för att hjälpa sökandena att visa att deras säkerhetsstyrningssystem uppfyller de nya kraven, i synnerhet i de fall där den sökande redan har beviljats ett säkerhetsintyg eller säkerhetstillstånd och/eller sökanden redan har ett annat ISO-styrningssystem (t.ex. ISO 9001, 14001 eller 45001) på plats (så att de kan integreras tillsammans) eller planerar att utveckla ett system utifrån denna modell. Att använda tabellerna ger inga systematiska garantier för överensstämmelse med de krav som fastställs i kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] är uppfyllda för de organisationer som innehar ett ISO-intyg. Ytterligare förklaringar och exempel ges i bilaga 2.

0.5 ISO/IEC-direktiven del 1 och konsoliderad ISO-komplettering

ISO har utvecklat officiella förfaranden som ska följas när nya internationella standarder utvecklas och upprätthålls. I bilaga SL tillägg 2 till [ISO/IEC-direktiven del 1 och den konsoliderade ISO-kompletteringen](#) antas en högnivåstruktur för ISO (*ISO High Level Structure* (HLS)) för användning av huvudtext i alla standarder för styrningssystem.

Bilaga I och bilaga II till kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] säkerställer en struktur som är förenlig med ISO HLS genom att integrationen av olika styrningssystem i förekommande fall underlättas, när systemen har samma huvudsakliga organisatoriska principer och krav men där lagenlighet och riskområden är specifika för varje disciplin (t.ex. säkerhet, miljö eller kvalitet).

ISO-standarder och relevanta vägledningar kan hjälpa järnvägsföretag och infrastrukturförvaltare att utveckla sina säkerhetsstyrningssystem. ISO 31000 är t.ex. ett generiskt dokument för bättre förståelse för riskhantering, ISO 31010 ger information för att välja och tillämpa riskhanteringstekniker såsom analys av allvarligheten hos fel tillstånd och felorsaker, felträdsanalys (*fault tree analysis*, FTA), händelseträdsanalys (*event tree analysis*, ETA), faro- och operabilitetsanalys (*hazard and operability studies*, Hazop), och ISO 55000 innehåller föreskrifter för förvaltning av tillgångar. Dessa kan dock endast vara till hjälp om det finns goda kunskaper om förutsättningarna för de järnvägsrelaterade riskerna.

Om användningen av HLS säkerställer ett konsekvent förhållningssätt till ISO-standarder för styrningssystem, måste det understrykas att ovanstående gemensamma säkerhetsmetoder är regler som främst används av nationella säkerhetsmyndigheter eller järnvägsbyrån i bedömningen av ansökningar om beviljande av säkerhetsintyg eller säkerhetstillstånd. Bedömningar gällande tillstånd för gemensamt säkerhetsintyg eller säkerhetstillstånd görs därför mot säkerhetsstyrningssystemkraven och inte mot ISO HLS i sig. Förtydligande: ISO-standarderna bygger på frivilliga intyg, men enligt vissa juridiska ramar ska de ge presumtion om överensstämmelse med tillämpliga regler för ett visst område. Det finns inga bestämmelser som säger att ISO-standarderna ska utgöra underlag för presumtion om överensstämmelse med föreskrifterna i direktiv (EU) 2016/798 eller med kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*].

Klausulerna 4–10.2 tagna från ISO/IEC-direktiven och konsoliderad komplettering 2016, bilaga SL tillägg 2, är reproducerade eller anpassade med tillstånd från Internationella standardiseringsorganisationen, ISO. Se källdokumentet för originaltexten. Detta dokument finns tillgängligt på [webbplatsen för ISO:s centralsekretariat](#). Upphovsrätten innehas av ISO.

0.6 Säkerhetsstyrningssystemets syfte

Syftet med säkerhetsstyrningssystemet är att säkerställa att organisationen på ett säkert sätt har kontroll över de risker som uppstår till följd av dess verksamhetsmål, och uppfyller alla tillämpliga säkerhetsföreskrifter. I dagens föränderliga och allt mer komplexa järnvägsmiljö är det nödvändigt att uppfylla dessa mål.

Genom strukturerade metoder kan man identifiera faror och kontinuerligt hantera de risker som är kopplade till en organisations egna verksamheter. Syftet är att förebygga olyckor. Med detta tillvägagångssätt tar man hänsyn till gemensamma risker vid gränssnitten för operativa förbindelser med andra järnvägsaktörer (framför allt järnvägsföretag, infrastrukturförvaltare och enheter som är ansvariga för underhåll, men även alla andra aktörer med potentiell inverkan på järnvägssystemets säkra drift, däribland tillverkare, underhållsleverantörer, fordonsinnehavare, tjänsteleverantörer, upphandlande enheter, transportörer, avsändare, mottagare, lastare, lossare, utbildningscenter, passagerare och andra individer som interagerar med järnvägssystemet osv). En organisation som på lämpligt sätt tillämpar alla relevanta delar i ett säkerhetsstyrningssystem kan vara trygg med att den har alla risker förknippade med sina verksamheter under kontroll, och att den kommer att fortsätta att ha det under alla omständigheter.

I mogna organisationer finns en medvetenhet om att effektiv riskkontroll enbart kan uppnås genom en process som sammanför tre kritiska dimensioner: en teknisk komponent med de verktyg och den utrustning som används, en mänsklig komponent bestående av personer i frontlinjen och deras kompetens, utbildning och motivation, samt en organisatorisk komponent bestående av förfaranden och metoder som fastställer förhållandet mellan uppgifter.

För att ett säkerhetsstyrningssystem ska vara adekvat måste följaktligen dess riskkontrollåtgärder övervakas och förbättras utifrån alla tre dimensioner. Säkerhetsstyrningssystemen för järnvägar har många likheter med de styrningsmetoder som förespråkas för att främja kvalitet, arbetsmiljö, miljöskydd och för att skapa framstående företag. Goda styrningsmetoder kan därför som tidigare nämnts lättare införas genom användning av en gemensam säkerhetsmetod som bygger på ISO HLS. Organisationer som redan har dessa system på plats måste därför inte nödvändigtvis utforma metoderna på nytt.

Det är känt att strukturerade styrningssystem skapar mervärde för företag genom den effektiva styrningen av operativa förbindelser. Detta bidrar till att förbättra resultaten generellt, inför operativa effektivitetsvinster, förbättrar förbindelserna med kontraktsparter och underleverantörer, kunder och tillsynsmyndigheter samt bidrar till att skapa en positiv säkerhetskultur.

En sökande måste utforma sitt säkerhetsstyrningssystem på ett sätt som gör det förenligt med kraven i artikel 9 i direktiv (EU) 2016/798 för att garantera en säker förvaltning av dess verksamheter. I detta syfte måste det uppvisa förenlighet med de krav som fastställs i bilagorna I och II till de gemensamma säkerhetsmetoderna för säkerhetsstyrningssystem. Dessa krav är utformade för att ge en fullständig bild av organisationens säkerhetsstyrningssystem enligt en så kallad PGSA-modell (planera, göra, studera, agera, *Plan, Do, Check, Act*). Sökanden måste beakta varje enskilt krav samt hur kraven passar ihop för att bilda ett sammanhängande säkerhetsstyrningssystem som kontrollerar de relevanta riskerna.

0.7 Säkerhetsstyrningssystem och processmetod

Ett säkerhetsstyrningssystem är ett medel för att samla de olika delar som behöver bilda en helhet för att kunna bedriva verksamhet på ett säkert och framgångsrikt sätt. Systemets element kommer att utgöra mekanismerna för att kunna uppfylla internationella och nationella regleringar och standarder, krav på sektor- och företagsnivå, omhändertar utfallet av riskbedömningar och lära av goda arbetssätt över hela organisationen. Därför bör säkerhetsstyrningssystemet integreras i organisationens företagsprocesser, och inte bli ett pappersbaserat system som tagits fram enbart för att visa att man efterlever regelverket. Säkerhetsstyrningssystemet bör vara ett levande redskap som mognar och utvecklas i takt med den organisation för vilken det tagits fram. För att bygga ett säkerhetsstyrningssystem krävs att organisationen förstår de risker de behöver ha kontroll över, liksom det legala ramverk som organisationen verkar i. Organisationen behöver även ha en tydlig bild av hur "gott utförande" ser ut. Den här vägledningen tar upp de element som behöver vara tillgodosedda för att den bedömande myndigheten ska kunna utfärda ett gemensamt säkerhetsintyg. Det bör dock beaktas att säkerhetsstyrningssystemets kvalitet är mer än bara summan av dess delar. Säkerhetsstyrningssystemet måste även fungera som en helhet, där uppfyllelse av varje del säkerställer att hela systemet fungerar korrekt. De krav som ligger till grund för bedömningen av ett säkerhetsstyrningssystem kan tillgodoses genom en dokumenterad process (eller ett förfarande e.d.), men de ska också integreras inom och över organisationens olika affärsområden. Den nationella säkerhetsmyndigheten kan till exempel kontrollera att det finns en policyförklaring, men den ska också kontrollera att förklaringen uppfylls av organisationen. Ett konkret sätt för den nationella säkerhetsmyndigheten att göra detta på är att kontrollera hur säkerhetsstyrningssystemet övervakas och granskas på högsta chefsnivå, hur involverade de anställda är och hur resultaten kommuniceras till dem. Det kan också hända att organisationen inte har något särskilt förfarande eller förfaranden för att hantera säkerhetsrelevant information. Den måste dock beskriva hur de relevanta delarna i företaget hanterar denna information på lämpligt sätt (t.ex. genom att säkerhetsrelevant information kommuniceras till lokföraren).

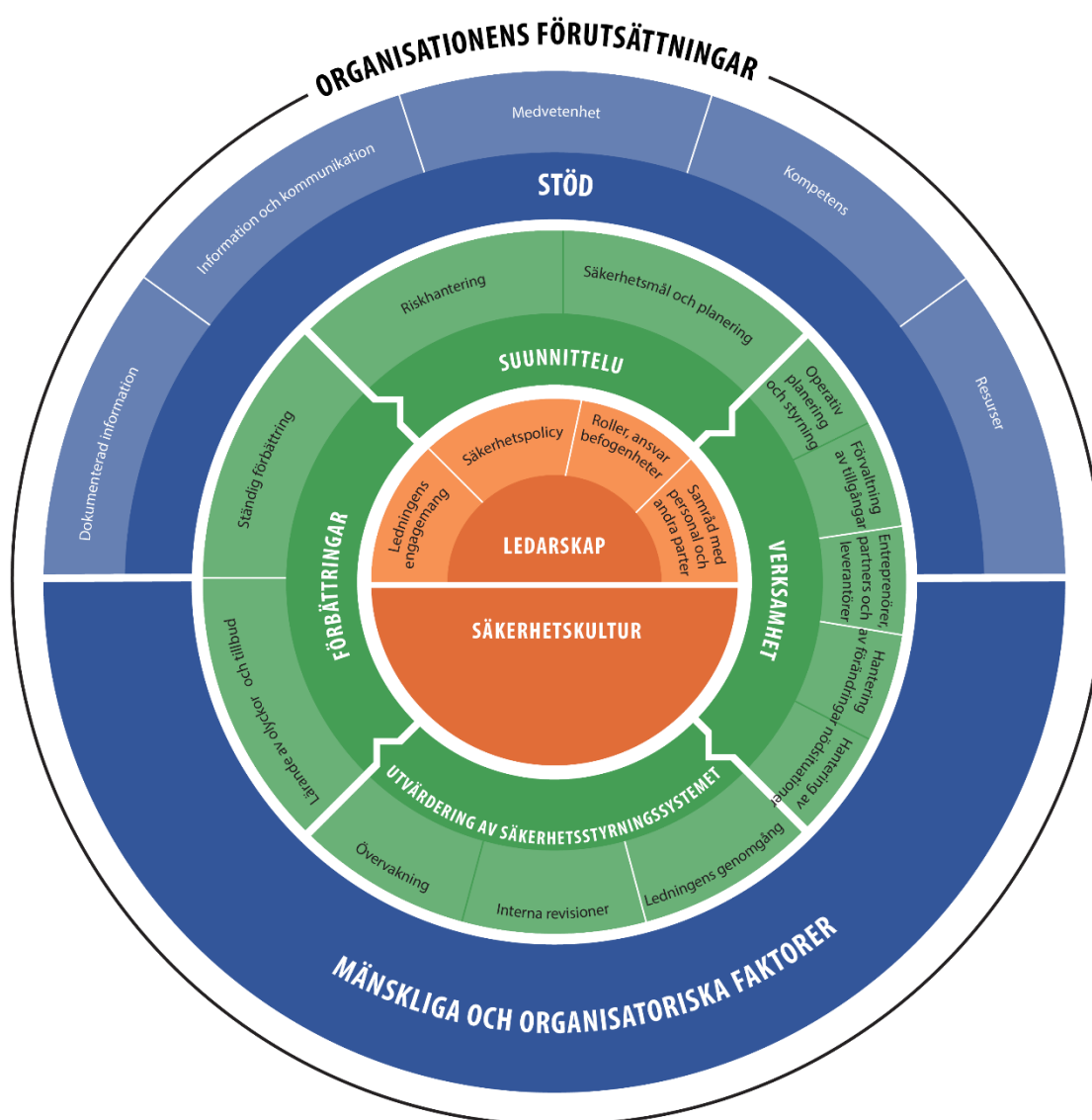
En viktig utveckling i bilaga I och bilaga II till kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] är införandet av en processmetod. Detta lyfts även fram i ISO-standarder för styrningssystem, där styrningssystemets olika processer är nära sammankopplade och deras kontinuerliga drift bidrar till att uppnå organisationens mål. Bilaga I och bilaga II till kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] identifieras några viktiga kopplingar mellan processer för att underlätta förståelsen för processmetoden, vilket dock inte betyder att enbart dessa kopplingar finns eller att de bör uppvisas som bevis på efterlevnad. En organisations förmåga att presentera hur processerna i dess styrningssystem är sammankopplade ger en god indikation för hur väl den förstår hur styrningssystemet fungerar effektivt.

Delarna i styrningssystemet kan observeras för att tillämpa en så kallad PGSA-modell (*Plan, Do, Check, Act*) – se Figur 2. PGSA-konceptet återspeglar det funktionella sambandet mellan de centrala delarna i ett säkerhetsstyrningssystem:

- **Planering:** identifiera risker och möjligheter, fastställa säkerhetsmål och identifiera processer och åtgärder som krävs för att leverera resultat i enlighet med organisationens säkerhetspolicy.
- **Verksamhet:** utveckla, genomföra och tillämpa processer och åtgärder som planerat.
- **Utvärdering:** övervaka och utvärdera de resultat som uppnåtts av de processer och åtgärder som genomförts i förhållande till mål och planering, och redovisa resultaten.
- **Förbättringar:** vidta åtgärder för att kontinuerligt förbättra säkerhetsstyrningssystemet och säkerheten för att nå de mål som ställts upp.

Denna centrala PGSA-process kompletteras av andra delar i säkerhetsstyrningssystemet:

- **Organisationens förutsättningar**, information som bidrar till planeringsfasen.
- **Ledarskap**, som driver PGSA-modellen framåt.
- **Olika funktioner för stöd**, som stödjer alla delar i säkerhetsstyrningssystemet.



Figur 2: Säkerhetsstyrningssystem för järnväg

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.

0.8 Säkerhetsstyrningssystem och säkerhetskultur

Säkerhetskultur är en uppsättning beteende- och tankemönster som i stor utsträckning delas inom en organisation, när det gäller hanteringen av betydande risker kopplade till deras verksamhet. Det här implicerar förstås att det kan uppstå flera kulturer inom en organisation beroende på arbetsroller, geografiska lägen eller andra delade värderingar. Säkerhetskultur är därmed något som skapas hela tiden, genom att olika aktörer interagerar med varandra, när en organisation både behöver anpassa sig till sin omgivning och säkerställa att alla dess medlemmar integreras.

Ett rakt sätt att beskriva säkerhetskultur är därför att titta på de faktorer som inverkar på beteende. Säkerhetsstyrningssystemet lägger grunden: genom att definiera förmodade arbetsförhållanden och förväntade resultat kan en organisation fastställa en arbetsmetod som är att föredra och tekniska hjälpmedel för att stötta verksamheten. För att fungera säkert behöver organisationen på bästa möjliga sätt föregripa negativa situationer, och tillämpa regler och verktyg för att hantera dem. Organisationen består också av en "beteendevärld": egenskaper, känslor, uppfattningar och förhållanden som skapar förutsättningar för interaktionsmönster bland individer inom organisationen på ett sätt som påverkar hur de tänker och agerar. Med denna kulturella aspekt avses framför allt de "oskrivna regler som styr beteenden och beslut hos en grupp individer". Tillsammans underlättar (eller hämmar) den strukturella och kulturella delen organisationens resultat.

Det finns dock en stor risk att ett alltför byråkratiskt tillvägagångssätt för säkerhetsstyrning går stick i stäv med den operationella verkligheten och resulterar i ett säkerhetsstyrningssystem som lever sitt eget liv, dvs. alla ansträngningar läggs på att utforma, underhålla och till och med bevisa existensen av ett dokumenterat system utan hänsyn till de operationella bidrag som är nödvändiga för att systemet faktiskt ska fungera som det var tänkt, vilket skapar ett glapp mellan "arbetet som det var tänkt" och "arbetet som det utförts".

Samtidigt är det dock möjligt att använda säkerhetsstyrningssystemet som ett instrument för att inverka positivt på en organisations säkerhetskultur och påverka den fysiska miljön, liksom beteenden hos de anställda, på ett sätt som gynnar och underlättar säkerheten. I slutändan är det när de strukturella och kulturella delarna i en organisation matchar varandra som säkerhet skapas. För att kunna hjälpa folk att utföra sina uppgifter måste en organisation förstå hur människor (med sina förmågor och begränsningar) använder specifikationer för att lösa problem och beakta denna kunskap i utformandet av sin arbetsmiljö. Samma sak gäller för regler och bestämmelser: om ingen hänsyn tas till de anställda som tillämpar reglerna när arbetsrutinerna utformas, kommer dessa personer att vara tvungna att bryta mot reglerna för att utföra sitt arbete när motsättningar eller konflikter uppstår.

Grundläggande faktorer som man vet bidrar till en positiv säkerhetskultur lyfts fram genom hela detta dokument. I bilaga 4 presenteras säkerhetskulturens grunder och annan användbar information för att organisationen ska kunna utveckla sin egen strategi.

0.9 Stödjande bevis och dokumenterad information

Detta dokument ger en indikation om vilka bevis sökanden (dvs. järnvägsföretaget eller infrastrukturförvaltaren) behöver tillhandahålla i samband med ansökningsen om säkerhetsintyg eller säkerhetstillstånd. Några specifika angivelser om vad som måste bifogas ges inte, av de skäl som anges ovan. För varje krav ges en indikation om vilka bevis den sökande bör tillhandahålla tillsammans med en lämplig hänvisning till kravet. Dessutom ges exempel på hur dessa bevis kan se ut i praktiken. Exempelen ska ses som ett hjälpmedel för underlätta förståelsen och inte som de enda sätten på vilka man kan bevisa att kraven uppfylls. De utgör inte heller en fullständig lista över alla möjliga alternativ. Det ska även påpekas att den sökande i samband med sin ansökan ska förklara hur varje krav uppfylls. Bedömare eller sökanden kan begära eller lämna som bevis den typ av information som föreslagits för att klargöra eller styrka hur kraven

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.

uppfylls. För sökanden och bedömaren är den viktigaste punkten för varje krav att se till att redogörelserna om överensstämmelse är kopplade till referenser som förklarar var ytterligare bevis finns att tillgå för att backa upp de påståenden som gjorts. Syftet med exempelavsnittet för varje krav är att ge en fingervisning om vad detta referensmaterial kan bestå av.

Referenser som kan vara användbara för de sökande när de utarbetar sina ansökningar anges efter detta avsnitt. Slutligen är det sista avsnittet under varje element avsett att fastställa den nödvändiga kopplingen till tillsyn. Här ges en indikation på sådant som en bedömare kan vilja belysa för de nationella säkerhetsmyndigheternas tillsynsteam som intressanta områden för att pröva säkerhetsstyrningssystemets omfattning.

Likaledes är den metod som föreskrivs i ISO-standarder för styrningssystem, bilaga I och bilaga II till förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*], inte normativ, undantaget i specifika fall, när det gäller typen av bevis (t.ex. förfaranden) som förväntas av sökanden. Syftet med att ge sökanden flexibilitet är att organisationen ska ha möjlighet att presentera sina säkerhetsstyrningssystemsanordningar på ett sätt som speglar affärsverksamhetens natur och står i proportion till dess storlek. Det bidrar också till en övergång från pappersbaserade prövningar av överensstämmelse till bedömningar av levande system i utveckling, som på ett korrekt sätt återspeglar affärsverksamheternas säkerhetsstyrningssystem som de ser ut i praktiken.

Termen "dokumenterad information" infördes som en del i ISO HLS och gemensamma termer för förvaltningssystemstandarder. Definitionen för dokumenterad information finns i *ISO 9000 punkt 3.8*. Dokumenterad information kan användas för att kommunicera ett budskap, ge bevis på vad som planerades och faktiskt har gjorts, eller för att utbyta kunskap. Det inbegriper men är inte begränsat till dokument och register såsom förfaranden, mötesprotokoll, rapporter, formell kommunikation om mål, resultat, avtal, kontrakt etc. Mer information finns i *Guidance on the requirements for Documented Information of ISO 9001:2015* som finns på ISO:s webbplats:

https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/documented_information.pdf

Termen "förfarande" bör inte tolkas som bevis på att det finns ett fristående dokument, som enbart och på ett heltäckande sätt omfattar styrningen av varje enskild del i säkerhetssystemet, eller som skäl för att begära utarbetandet av en specifik uppsättning nya dokument. När hänvisning i detta dokument görs till ett förfarande avses dokumenterad information (t.ex. pappersdokument) där de steg som tillämpas beskrivs. Där hänvisning görs till en process avses medlen för att klara en uppgift eller nå ett mål, som inte nödvändigtvis anges i ett förfarande.

0.10 Korshänvisningar till andra EU-förordningar och tillämpliga rättsliga krav

Hänvisningar till andra EU-förordningar förstärker samstämmigheten mellan de olika rättsliga texterna samtidigt som kopplingarna mellan dem tydliggörs. Säkerhetsstyrningssystemanordningarna bör alltid överensstämma med gällande lagstiftning om inte annat anges (t.ex. särskilda övergångsbestämmelser, fördröjd tillämpning). När en EU-förordning upphävs tolkas vanligtvis alla hänvisningar som hänvisningar till den nya förordningen (om det anges i förordningen).

Alla järnvägsföretag och infrastrukturförvaltare måste efterleva en rad rättsliga skyldigheter utöver dem som enbart behandlar säkerhetsfrågor. Några av dessa andra skyldigheter har en direkt eller indirekt inverkan på hur organisationen hanterar sitt ansvar för säkerheten genom sitt säkerhetsstyrningssystem, till exempel överensstämmelse med lagstiftning som härrör från interoperabilitetsdirektivet (EU) 2016/797 eller säkerhetsrelevans för den tjänst som tillhandahålls av infrastrukturförvaltarna till järnvägsföretagen inom ramen för direktiv 2012/34/EU. Det säkerhetsstyrningssystem som järnvägsföretag och

infrastrukturförvaltare använder för att hantera säkerhetsrisker måste därför organiseras på ett sätt som i tillämpliga fall säkerställer efterlevnad av sådana andra rättsliga förpliktelser.

Innehåll

0	INLEDNING	2
0.1	VÄGLEDNINGENS SYFTE	2
0.2	VEM ÄR DENNA VÄGLEDNING TILL FÖR?	2
0.3	OMFATTNING	3
0.4	VÄGLEDNINGENS STRUKTUR	3
0.5	ISO/IEC-DIREKTIVEN DEL 1 OCH KONSOLIDERAD ISO-KOMPLETTERING	4
0.6	SÄKERHETSSTYRNINGSSYSTEMETS SYFTE.....	5
0.7	SÄKERHETSSTYRNINGSSYSTEM OCH PROCESSMETOD	6
0.8	SÄKERHETSSTYRNINGSSYSTEM OCH SÄKERHETSKULTUR	8
0.9	STÖDJANDE BEVIS OCH DOKUMENTERAD INFORMATION	8
0.10	KORSHÄNVISNINGAR TILL ANDRA EU-FÖRORDNINGAR OCH TILLÄMPLIGA RÄTTSLIGA KRAV	9
1	ORGANISATIONENS FÖRUTSÄTTNINGAR	16
1.1	REGLERANDE KRAV	16
1.2	SYFTE.....	16
1.3	FÖRKLARANDE ANMÄRKNINGAR	16
1.4	BEVIS.....	18
1.5	EXEMPEL PÅ BEVIS.....	18
1.6	REFERENSER OCH STANDARDER.....	19
1.7	TILLSYNSFRÅGOR.....	19
2	LEDARSKAP	20
2.1	LEDARSKAP OCH ÅTAGANDEN	20
2.1.1	<i>Reglerande krav</i>	20
2.1.2	<i>Syfte</i>	20
2.1.3	<i>Förklarande anmärkningar</i>	21
2.1.4	<i>Bevis</i>	21
2.1.5	<i>Exempel på bevis</i>	22
2.1.6	<i>Referenser och standarder</i>	22
2.1.7	<i>Tillsynsfrågor</i>	22
2.2	SÄKERHETSPOLICY	24
2.2.1	<i>Reglerande krav</i>	24
2.2.2	<i>Syfte</i>	24
2.2.3	<i>Förklarande anmärkningar</i>	24
2.2.4	<i>Bevis</i>	24
2.2.5	<i>Exempel på bevis</i>	25
2.2.6	<i>Tillsynsfrågor</i>	25
2.3	ROLLER, ANSVAR, ANSVARSSKYLDIGHET OCH BEFOGENHETER INOM ORGANISATIONEN	26
2.3.1	<i>Reglerande krav</i>	26
2.3.2	<i>Organisationen ska säkerställa att personal med delegerat ansvar för säkerhetsrelaterade arbetsuppgifter ska ha behörighet, kompetens och lämpliga resurser för att utföra sina arbetsuppgifter utan att påverkas negativt av andra funktioner inom verksamheten.</i>	26
2.3.3	<i>Delegering av ansvaret för säkerhetsrelaterade arbetsuppgifter ska dokumenteras och meddelas berörd personal, samt godtas och förstås.</i>	26
2.3.2	<i>Syfte</i>	26
2.3.3	<i>Förklarande anmärkningar</i>	26
2.3.4	<i>Bevis</i>	27
2.3.5	<i>Exempel på bevis</i>	27
2.3.6	<i>Referenser och standarder</i>	28

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.

2.3.7	Tillsynsfrågor.....	28
2.4	SAMRÅD MED PERSONAL OCH ANDRA PARTER.....	29
2.4.1	Reglerande krav.....	29
2.4.2	Syfte.....	29
2.4.3	Förklarande anmärkningar.....	29
2.4.4	Bevis.....	29
2.4.5	Exempel på bevis.....	30
2.4.6	Tillsynsfrågor.....	30
3	PLANERING	31
3.1	ÅTGÄRDER FÖR ATT HANTERA RISER	31
3.1.1	Reglerande krav.....	31
3.1.2	Syfte.....	31
3.1.3	Förklarande anmärkningar.....	32
3.1.4	Bevis.....	33
3.1.5	Exempel på bevis.....	34
3.1.6	Referenser och standarder.....	35
3.1.7	Tillsynsfrågor.....	35
3.2	SÄKERHETSMÅL OCH PLANERING	36
3.2.1	Reglerande krav.....	36
3.2.2	Syfte.....	36
3.2.3	Förklarande anmärkningar.....	36
3.2.4	Bevis.....	37
3.2.5	Exempel på bevis.....	37
3.2.6	Tillsynsfrågor.....	37
4	STÖD	38
4.1	RESURSER.....	38
4.1.1	Reglerande krav.....	38
4.1.2	Syfte.....	38
4.1.3	Förklarande anmärkningar.....	38
4.1.4	Bevis.....	38
4.1.5	Exempel på bevis.....	38
4.1.6	Tillsynsfrågor.....	39
4.2	KOMPETENS.....	40
4.2.1	Reglerande krav.....	40
4.2.2	Syfte.....	40
4.2.3	Förklarande anmärkningar.....	41
4.2.4	Bevis.....	41
4.2.5	Exempel på bevis.....	42
4.2.6	Referenser och standarder.....	43
4.2.7	Tillsynsfrågor.....	43
4.3	MEDVETENHET	44
4.3.1	Reglerande krav.....	44
4.3.2	Syfte.....	44
4.3.3	Bevis.....	44
4.3.4	Exempel på bevis.....	44
4.3.5	Tillsynsfrågor.....	44
4.4	INFORMATION OCH KOMMUNIKATION	46
4.4.1	Reglerande krav.....	46
4.4.2	Syfte.....	46
4.4.3	Förklarande anmärkningar.....	46
4.4.4	Bevis.....	47

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.

4.4.5	Exempel på bevis.....	47
4.4.6	Tillsynsfrågor.....	48
4.5	DOKUMENTERAD INFORMATION.....	49
4.5.1	Reglerande krav	49
4.5.2	Syfte	49
4.5.3	Förklarande anmärkningar	50
4.5.4	Bevis	51
4.5.5	Exempel på bevis.....	51
4.5.6	Referenser och standarder.....	52
4.5.7	Tillsynsfrågor.....	52
4.6	INTEGRERING AV MÄNSKLIGA OCH ORGANISATORISKA FAKTORER	53
4.6.1	Reglerande krav	53
4.6.2	Syfte	53
4.6.3	Förklarande anmärkningar	53
4.6.4	Bevis	53
4.6.5	Exempel på bevis.....	54
4.6.6	Referenser och standarder.....	55
4.6.7	Tillsynsfrågor.....	55
5	VERKSAMHET	56
5.1	OPERATIV PLANERING OCH STYRNING	56
5.1.1	Reglerande krav	56
5.1.2	Syfte	57
5.1.3	Förklarande anmärkningar	58
5.1.4	Bevis	59
5.1.5	Exempel på bevis.....	60
5.1.6	Referenser och standarder.....	61
5.1.7	Tillsynsfrågor.....	62
5.2	STYRNING OCH KONTROLL AV (OPERATIVA) TILLGÅNGAR	63
5.2.1	Reglerande krav	63
5.2.2	Syfte	64
5.2.3	Förklarande anmärkningar	64
5.2.4	Bevis	65
5.2.5	Exempel på bevis.....	67
5.2.6	Referenser och standarder.....	71
5.2.7	Tillsynsfrågor.....	71
5.3	ENTREPRENÖRER, PARTNER OCH LEVERANTÖRER	72
5.3.1	Reglerande krav	72
5.3.2	Syfte	72
5.3.3	Förklarande anmärkningar	73
5.3.4	Bevis	73
5.3.5	Exempel på bevis.....	73
5.3.6	Tillsynsfrågor.....	74
5.4	HANTERING AV FÖRÄNDRINGAR	75
5.4.1	Reglerande krav	75
5.4.2	Syfte	75
5.4.3	Förklarande anmärkningar	75
5.4.4	Bevis	76
5.4.5	Exempel på bevis.....	76
5.4.6	Tillsynsfrågor.....	76
5.5	HANTERING AV NÖDSITUATIONER	77
5.5.1	Reglerande krav	77
5.5.2	Syfte	77

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.

5.5.3	Förklarande anmärkningar	78
5.5.4	Bevis	78
5.5.5	Exempel på bevis	78
5.5.6	Tillsynsfrågor	79
6	UTVÄRDERING	80
6.1	ÖVERVAKNING	80
6.1.1	Reglerande krav	80
6.1.2	Syfte	80
6.1.3	Förklarande anmärkningar	80
6.1.4	Bevis	81
6.1.5	Exempel på bevis	81
6.1.6	Tillsynsfrågor	81
6.2	INTERNREVISION	82
6.2.1	Reglerande krav	82
6.2.2	Syfte	82
6.2.3	Förklarande anmärkningar	82
6.2.4	Bevis	82
6.2.5	Exempel på bevis	83
6.2.6	Referenser och standarder	83
6.2.7	Tillsynsfrågor	83
6.3	LEDNINGENS GENOMGÅNG	84
6.3.1	Reglerande krav	84
6.3.2	Syfte	84
6.3.3	Bevis	84
6.3.4	Exempel på bevis	85
6.3.5	Tillsynsfrågor	85
7	FÖRBÄTTRINGAR	86
7.1	LÄRDOMAR AV OLYCKOR OCH TILLBUD	86
7.1.1	Reglerande krav	86
7.1.2	Syfte	86
7.1.3	Förklarande anmärkningar	87
7.1.4	Bevis	87
7.1.5	Exempel på bevis	87
7.1.6	Referenser och standarder	88
7.1.7	Tillsynsfrågor	88
7.2	KONTINUERLIG FÖRBÄTTRING	89
7.2.1	Reglerande krav	89
7.2.2	Syfte	89
7.2.3	Förklarande anmärkningar	89
7.2.4	Bevis	91
7.2.5	Exempel på bevis	92
7.2.6	Tillsynsfrågor	92
	BILAGA 1 – JÄMFÖRELSETABELLER	93
	BILAGA 2 – ÖMSESIDIGT GODKÄNNANDE AV TILLSTÅND, ERKÄNNANDEN ELLER INTYG FÖR PRODUKTER ELLER TJÄNSTER SOM BEVILJAS ENLIGT EU-LAGSTIFTNINGEN	102
	BILAGA 3 – SIDOSPÅR, AVTALSVILLKOR OCH PARTNERSKAP	106
	BILAGA 4 – SÄKERHETSKULTUR	110
	BILAGA 5 – INTEGRERING AV MÄNSKLIGA OCH ORGANISATORISKA FAKTORER	115

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.

BILAGA 6 – DEFINITIONER.....119

1 Organisationens förutsättningar

1.1 Reglerande krav

1.1 Organisationen ska:

- (a) beskriva typ och omfattning av samt området för verksamheten,
(a) beskriva karaktären hos och omfattning av verksamheten,
- (b) identifiera de allvarliga risker för säkerheten som uppstår i samband med dess järnvägsverksamhet, vare sig den utförs av organisationen själv eller av entreprenörer, partner eller leverantörer som står under dess kontroll,
- (c) identifiera de berörda parter (t.ex. regleringsorgan, myndigheter, järnvägsföretag, infrastrukturförvaltare, entreprenörer, leverantörer, partner), inklusive parter som står utanför järnvägssystemet, som är relevanta för säkerhetsstyrningssystemet,
- (d) identifiera och upprätthålla rättsliga och andra säkerhetsrelaterade krav från de berörda parter som avses i punkt c,
- (e) säkerställa att de krav som avses i punkt d beaktas vid utarbetandet, genomförandet och upprätthållandet av säkerhetsstyrningssystemet,
- (f) beskriva säkerhetsstyrningssystemets omfattning, och ange vilken del av verksamheten som omfattas eller inte och beakta de krav som avses i punkt d.

1.2 I denna bilaga gäller följande definitioner:

- (a) *karaktär*: bestäms i samband med järnvägsverksamhet som bedrivs av infrastrukturförvaltare. Med karaktär menas egenskaper för järnvägsverksamheten inklusive utformning och konstruktion av infrastruktur, underhåll av infrastruktur, trafikplanering, och trafikstyrning, och användningen av järnvägsinfrastrukturen, vilket inbegriper konventionella linjer och/eller högastighetslinjer, transport av passagerare och/eller gods.
- (b) *omfattning*: bestäms i samband med järnvägsverksamhet som bedrivs av infrastrukturförvaltare. Med omfattning menas spårlängd och infrastrukturförvaltarens uppskattade storlek mätt i antalet anställda som arbetar inom dess järnvägsverksamhet.

1.2 Syfte

Sökanden bör så tydligt som möjligt visa för myndigheten att dess säkerhetsstyrningssystem omfattar dess fulla drift. Den bedömande myndigheten bör kunna se tydligt vilken typ av drift det rör sig om och hur den hanteras via säkerhetsstyrningssystemet. Sökanden bör visa att den har en tydlig förståelse för sina förbindelser med berörda parter och de allvarliga risker som är involverade, vem som berörs och hur dessa frågor behandlas i säkerhetsstyrningssystemet.

1.3 Förklarande anmärkningar

Kravet på att redogöra för organisationen, de omgivande faktorerna och omfattningen av säkerhetsstyrningssystemet (1.1) syftar till att från bedömarens perspektiv skapa bättre förståelse för organisationens affärsverksamhet, berörda aktörers förväntningar och organisationens verksamhetsmiljö. Organisationstypen är bedömningens utgångspunkt. Att denna information finns tillgänglig i början av ansökningen gör det möjligt för en sökande att beskriva vad organisationen gör och hur den är uppbyggd,

vilket i sin tur gör att bedömarens kan fatta beslut om hur bedömningen ska planeras. Om organisationen till exempel är centraliserad eller driver olika slags verksamheter med omfattande lokal frihet att planera och organisera sin verksamhet eller om organisationen sysselsätter fler eller färre entreprenörer kan det innebära motsvarande förväntningar på att sökandens organisation och dess säkerhetsstyrningssystem är utformade för att hantera de problem som uppstår. Förklaringen av de övergripande förutsättningarna för organisationen kan också indikera hur mänskliga och organisatoriska faktorer hanteras. Den struktur som fastställs i punkt 4 i ISO HLS kan vara till hjälp för att förstå vilket förberedande arbete som krävs för att inrätta säkerhetsstyrningssystemet. Det är viktigt att bedömarens förstår driftens omfattning för att han eller hon ska kunna göra en korrekt bedömning.

Verksamhetstypen **(1.1 a)** omfattar per definition transport av passagerare (med eller utan höghastighetstjänster) och varor (med eller utan farligt gods) och växlingstjänster. Den kan också omfatta andra speciella typer av verksamheter såsom provning av fordon, drift av fordon för underhåll av järnvägsinfrastrukturen, drift på privatägda sidospår. Mer information om typ, omfattning och område för verksamheten finns i dokumentet *Ansökningsvägledning för beviljande av gemensamma säkerhetsintyg – En vägledning för sökande*. Ytterligare information om verksamhet på sidospår finns i bilaga 3.

För en infrastrukturförvaltare definieras begreppen karaktär och omfattning i 1.2; begrepp som berör verksamhetens typ, dess geografiska storlek och komplexitet. Karaktären speglar vilken sorts infrastruktur som används, hur modern den är och om den är avsedd för höghastighets- eller konventionell trafik eller båda. Omfattning innebär istället vilken typ av verksamhet som bedrivs.

Identifiering av allvarliga risker betyder i detta fall att de sökande genom sin analys ska visa att de känner till de främsta riskerna som deras verksamhet innebär. . Identifiering av allvarlig risk innebär också att sökanden har upprättat ett system för riskhantering (eller förbereder sig för att upprätta det), och från detta kan

- *analysera farliga händelser och bedöma risker,*
- *bli medveten om de viktigaste farliga händelserna och riskerna (i termer av konsekvenser och frekvens), och*
- *prioritera åtgärder som syftar till att förebygga olyckor. (1.1 b)*

Detta hjälper till att identifiera organisationens förutsättningar och visar den bedömande myndigheten att sökanden har förståelse för sin verksamhetsmiljö. Verksamhet som bedrivs av andra parter utanför järnvägssystemet **(1.1 c)** kan påverka driftsäkerheten och måste också beaktas i riskbedömningen. Ytterligare information om avtalsvillkor och partnerskap finns i bilaga 3.

Identifieringen av tillämpliga krav relaterade till säkerhet **(1.1.1 d)** spänner från bestämmelserna i tillämpliga EU-förordningar (t.ex. relevant gemensam säkerhetsmetod för säkerhetsstyrningssystem och i synnerhet bilagorna I och II, gemensam säkerhetsmetod för riskbedömning och utvärdering, gemensam säkerhetsmetod för övervakning, relevanta TSD:er, genomförandeakt om de praktiska arrangemangen för fordonsgodkännande och förordning för enheter som ansvarar för underhåll) och nationell lagstiftning (t.ex. anmälda nationella regler, nationella lagar) till alla andra krav som organisationen har förbundit sig till (t.ex. driftregler på sektor- eller industrinivå eller styrningssystem och tekniska standarder såsom ISO, CEN/Cenelec, UIC).

Vid tillämpningen av detta dokument ska termerna "personal", "anställda" och "arbetare" ha samma betydelse, det vill säga personer som arbetar under direkt kontroll av sökandens organisation.

1.4 Bevis

- För järnvägsföretag: Information om typ av verksamhet, t.ex. passagerar- eller godstransport, transport av farligt gods, geografisk täckning (genom bifogande av en karta eller tågplan) och verksamhetens omfattning (inklusive typer av rullande järnvägsmateriel, antal anställda), samt vid förnyelse ändringar sedan senaste bedömningen. **(1.1 a)**
- För infrastrukturförvaltare: Information om den typ av verksamhet de ombesörjer, t.ex. gods eller passagerartransport, växlingstjänster eller andra anläggningstjänster (såsom avses i bilaga II till direktiv 2012/34/EU) som inverkar på järnvägssäkerheten, geografisk täckning (genom bifogande av en karta eller färdplan) och omfattningen av den verksamhet som järnvägsföretagen bedriver på nätet. Infrastrukturförvaltaren bör även tillhandahålla information om all rullande järnvägsmateriel (inklusive anläggningar för underhåll av infrastruktur eller mätning) som kan omfattas av dess verksamhet och ange antalet anställda, samt eventuella ändringar sedan senaste bedömningen i händelse av förnyelse. **(1.1 a)**
- Den som ansöker om ett säkerhetsintyg eller säkerhetstillstånd måste visa hur de relevanta kraven i lagstiftningen har identifierats, t.ex. bedömningskraven i de gemensamma säkerhetsmetoderna, de tekniska specifikationerna för driftskompatibilitet och särskilt den som avser delsystemet för drift och trafikledning (TSD drift och trafikledning) och de tillämpliga nationella reglerna, samt hur efterlevnad av dessa upprätthålls (säkerhetsstyrningssystemprocesserna för att säkerställa överensstämmelse). **(1.1 c–d)**
- Sökanden måste identifiera berörda parter som är relevanta för en framgångsrik implementering av dess säkerhetsstyrningssystem, det vill säga parter som med sin verksamhet har en påverkan eller potentiell påverkan på säkerhetsstyrningssystemet (t.ex. entreprenörer eller partners). Sökanden ska även ange varför parterna behövs för en framgångsrik tillämpning av säkerhetsstyrningssystemet. **(1.1 c–d)**
- För båda: Sökanden ska ange var i dokumentationen om säkerhetsstyrningssystemet samtliga krav i detta system uppfylls, inklusive de relevanta kraven i de tillämpliga tekniska specifikationerna för driftskompatibilitet och i synnerhet TSD drift och trafikledning, samt var relevanta anmälda nationella regler uppfylls. **(1.1 e)**
- Sökanden ska ange de mest allvarliga säkerhetsriskerna som påverkar dess verksamhet. **(1.1 b)**
- Sökanden måste tillhandahålla information om säkerhetsstyrningssystemets omfattning (inklusive vilka gränserna är mot andra delar av verksamheten). **(1.1 f)**

1.5 Exempel på bevis

En karta som visar det geografiska verksamhetsområdet. Information om rullande järnvägsmateriel godkänd för drift (inklusive i tillämpliga fall all rullande materiel som det föreslås ha i drift under intygets eller tillståndets giltighetstid och eventuella begränsningar för användningsområdet). Information om typerna av tjänster som verksamheten avses omfatta (passagerartrafik och/eller gods) ingår.

När sökanden är en infrastrukturförvaltare kan denna information lämnas genom hänvisning till exempelvis

- uppgifterna i infrastrukturregistret som fastställs i direktivet om driftskompatibilitet (artikel 49),
- innehållet i den beskrivning av järnvägsnätet (särskilt i avsnitt I) som inrättats i enlighet med direktiv 2012/34/EU, och
- linjeboken (TSD drift och trafikledning).

Den information som ges för att erhålla säkerhetstillstånd eller säkerhetsintyg är korrekt refererad och tillräckligt dokumenterad för att kunna påvisa efterlevnad av relevant EU-lagstiftning..

Uppgifter om nuvarande och föreslagen bemanning inom livslängden för det gemensamma säkerhetsintyget så långt detta är känt.

Ett järnvägsföretag tillhandahåller information om gränssnitten för sina operativa förbindelser, inbegripet med infrastrukturförvaltaren/-förvaltarna, andra järnvägsföretag, entreprenörer och räddningstjänst. Den här informationen inkluderar alla specifika krav från infrastrukturförvaltaren som påverkar järnvägsföretagets säkerhetsstyrningssystem.

För järnvägsföretag kan en tabell användas för att förklara hur lagstiftning och andra relevanta krav efterlevs. Tabellen kan bifogas i One Stop Shop, som en del av en ansökan om säkerhetsintyg.

Infrastrukturförvaltare bör tillhandahålla en liknande förteckning över de aktörer som de har operativa förbindelser med, till exempel järnvägsföretag som är verksamma på den kontrollerade infrastrukturen, dess entreprenörer, angränsande infrastrukturförvaltare, byggarbetsplatser, lokala myndigheter (för gränssnitt på vägar) och räddningstjänsten.

Information om rättsliga bestämmelser (både nationella och europeiska) som kommer att uppfyllas.

En beskrivning (inklusive ett organisationsschema) som fastställer hur säkerhetsstyrningssystemet är strukturerat och hanteras inom organisationen, som också innehåller länkar till de olika avsnitten i säkerhetsstyrningssystemet där mer detaljerad information såsom driftsregler kan hittas.

En kopia av den senaste årliga rapporten som specificerar de mest allvarliga risker som organisationen hanterar och de mål man har för att kontrollera dessa risker, den metod som används för att bedöma riskerna och hur de prioriteras.

1.6 Referenser och standarder

- *Tillämpningsvägledningar för TSD drift och trafikledning*

1.7 Tillsynsfrågor

Kontrollera riktigheten i den information som tillhandahålls mot känd informationen om befintlig verksamhet när det gäller ansökningar om förnyelse av intyg, eller mot andra tillgängliga uppgifter när det gäller nya aktörer.

Kontrollera att säkerhetsstyrningssystemet såsom det beskrivs uppfyller säkerhetsåtagandena i praktiken.

Kontrollera att alla operativa förbindelser som organisationen har med andra aktörer återspeglas i säkerhetsstyrningssystemets anordningar för att kontrollera riskerna.

2 Ledarskap

2.1 Ledarskap och åtaganden

2.1.1 Reglerande krav

2.1.1 Den högsta ledningen ska visa prov på ledarskap och åtaganden vad gäller utveckling, genomförande, upprätthållande och förbättring av säkerhetsstyrningssystemet genom att:

- (a) ha en övergripande ansvarsskyldighet och ta ett övergripande ansvar vad gäller säkerheten,
- (b) säkerställa att det finns åtaganden vad gäller säkerheten hos ledningen på olika nivåer, genom dess verksamhet och i dess förbindelser med personal och entreprenörer,
- (c) säkerställa att säkerhetspolicy och säkerhetsmål upprättas, förstås och är förenliga med organisationens strategiska inriktning,
- (d) säkerställa att säkerhetsstyrningssystemets krav integreras i organisationens verksamhetsprocesser,
- (e) säkerställa att nödvändiga resurser för säkerhetsstyrningssystemet finns tillgängliga,
- (f) säkerställa att säkerhetsstyrningssystemet klarar att kontrollera de säkerhetsrisker som uppstår inom organisationen på ett ändamålsenligt sätt,
- (g) uppmuntra personalen att stödja efterlevnaden av säkerhetsstyrningssystemets krav,
- (h) främja kontinuerlig förbättring av säkerhetsstyrningssystemet,
- (i) säkerställa att säkerhet beaktas i samband med identifiering och hantering av organisationens verksamhetsrisker och beskriva hur konflikt mellan säkerhet och andra verksamhetsmål kommer att uppmärksammas och lösas,
- (j) främja en positiv säkerhetskultur.

2.1.2 Syfte

En tydlig och positiv riktning för säkerhetsstyrningen har en stor inverkan på hur risker hanteras. Den bedömande myndigheten behöver kunna lita på sökandens åtaganden när det gäller att avsätta resurser för att möjliggöra att organisationen ska fungera säkert, för att effektivt kunna hantera sina risker och för att ledarskapet inom den sökande organisationen är där för att se till att detta händer. Ledningens åtaganden i fråga om mänskliga och organisatoriska faktorer demonstreras genom verksamhetens policy och mål och i styrnings- och ledarskapsbeteenden. Ett ledarskap vars filosofi bygger på mänskliga och organisatoriska faktorer säkerställer också att utvecklingen av utbildning och förfaranden utgår från uppgiften som ska utföras i dess naturliga miljö, vilket bidrar till att optimera både riskkontroll och resultat.

I säkerhetspolicyn fastställs vikten av säkerhet och hur den prioriteras, inklusive integreringen av mänskliga och organisatoriska faktorer och främjandet av säkerhetskulturen.

Organisationen främjar en konstant och kollektiv vaksamhet, motverkar självbelåtenhet ("allt är under kontroll") och överdriven förenkling ("att respektera förfaranden är tillräckligt för att tillhandahålla säkerhet") och utveckla en ifrågasättande attityd. Dessutom är alla aktörer i organisationen medvetna om att det, oavsett kvaliteten på planering och organisation, tekniska hinder och förfaranden, alltid kan finnas ett glapp mellan vad som förutspåddes och vad som faktiskt hände. Alla tänkbara källor används för att upptäcka och gemensamt analysera dessa situationer som inte kunnat förutspås på lämpligt sätt.

Organisationens kommunikation om säkerhet är dessutom i linje med verkligheten när det gäller beslut på ledningsnivå.

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.

För att ett säkerhetsstyrningssystem ska fungera effektivt och utvecklas och förbättras i framtiden är det av största vikt att individer i ledande befattningar visar sin personal och andra berörda parter att de har en positiv agenda med utrymme för att hantera säkerhet. Det är individerna i de ledande befattningarna som har det största inflytandet på organisationskulturen och det är därför avgörande att de kan kommunicera sitt budskap till dem som arbetar för dem. Beteendet hos chefer på alla nivåer i organisationen, och den betydelse de tillskriver säkerhet i sina dagliga beslut, har mycket stor inverkan på andra aktörers beteende när de fullgör sina uppgifter på ett säkert sätt. Chefer bör även skapa de fysiska och sociala arbetsmiljöerna för att på ett säkert sätt kunna utföra arbetet i frontlinjen.

2.1.3 Förklarande anmärkningar

”Verkställande ledning” (**2.1.1**) avser i detta sammanhang dem som fattar beslut som sätter kursen för organisationsfilosofin. Detta omfattar vanligtvis verkställande direktören, medlemmar i verkställande ledningsgruppen, styrelseordförande och styrelseledamöter. Såväl inom en grupp som för individer krävs en ”verkställande ledning” för att visa ledarskap och engagemang om och genom säkerhetsstyrningssystemet.

Tillräckligt stor vikt ska läggas vid säkerhetsrisker (**2.1.1 i**) för att balansera andra affärsrisker, för att undvika situationer där ledningen prioriterar verksamhetens behov på ett sätt som innebär att säkerheten försvagas. Den verkställande ledningen måste se till att målen behandlas på ett sådant sätt att säkerheten bibehålls och risker tas itu med så långt det är praktiskt möjligt. Målkonflikter bör inte leda till att individers uppgifter står i konflikt med varandra, vilket kan leda till säkerhetsproblem.

En ledarskaps- och förvaltningsstrategi som integrerar mänskliga och organisatoriska faktorer innebär att sätta mål, förväntningar och fördela ansvar i fråga om säkerhetsbeteenden på alla nivåer i organisationen samt säkerställa lämplig feedback och kommunikation.

2.1.4 Bevis

- *Det finns en säkerhetspolitik och mål samt bevis för att dessa är tillgängliga för och uppfattas av alla medarbetare, och det görs klart hur dessa passar in andra affärsprocesser. (2.1.1 a, b, g, e)*
- *I säkerhetspolicyn anges vikten av att tillämpa en strategi som utgår från mänskliga och organisatoriska faktorer i alla säkerhetsrelaterade förfaranden för att uppnå en hög säkerhetsnivå i organisationen. Organisationen visar hur mänskliga och organisatoriska faktorer hanteras i de organisatoriska processerna. (2.1.1 c)*
- *Förhållandet mellan säkerhetsstyrningssystemet och annan affärsverksamhet anges tydligt i ett förfarande eller organisationsschema. (2.1.1 e, i)*
- *Det finns information i säkerhetspolicyn eller i andra processer som visar att ledningen förbundit sig att tillhandahålla och upprätthålla tillräckliga resurser för att säkerhetsstyrningssystemet ska fungera effektivt. (2.1.1 e)*
- *Det finns bevis som visar att ledarskapet främjar en positiv säkerhetskultur. (2.1.1 j)*
- *Bevis som klargör hur man ser till att personalen förstår sina roller och ansvarsområden i fråga om säkerhet och hur deras agerande påverkar organisationens förmåga att styra risker genom säkerhetsstyrningssystemet. (2.1.1 d, f, i)*
- *Det finns bevis i säkerhetspolicyn eller annan dokumentation på att organisationen strävar efter att hålla de anställda informerade om deras viktiga roll för att säkerställa att säkerhetsstyrningssystemet fungerar i praktiken, för att på ett meningsfullt sätt kontrollera risker. (2.1.1 e)*
- *Det finns processer som anger hur mänskliga och organisatoriska faktorer bör hanteras och kommuniceras inom organisationen i förhållande till organisationens affärs mål och organisatoriska processer, t.ex. projekt, utredningar av tillbud och olyckor, riskanalyser och andra*

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.

säkerhetsrelaterade aktiviteter för organisationens egen personal, entreprenörer, partner och leverantörer. (2.2.1 c, d, e)

- *Det finns bevis som visar att ledningen har skapat processer för att säkerställa att mänskliga och organisatoriska faktorer hanteras av organisationens underleverantörer. (2.2.1 c, d, e)*

2.1.5 Exempel på bevis

En daterad säkerhetspolicy undertecknad av verkställande direktör som klargör ledningens åtaganden när det gäller säkerhet och säkerhetsförbättringar, samt hur personalen involveras i hanteringen av säkerhetsrisker. I säkerhetspolicyen anges också hur den kommer att granskas.

En tydlig uppsättning säkerhetsmål för organisationen som är specifika, mätbara, uppnåbara, realistiska och tidsbundna (*Significant, Measurable, Achievable, Realistic and Time bound, Smart*). Det finns också en tydlig metod fastställd i ett förfarande för att skapa dessa mål och för att analysera framgångar eller misslyckanden med att uppnå dem.

Ett tydligt uttalande från ledningen om hur de främjar en positiv säkerhetskultur och hur personalen involveras och engageras i processen.

En översikt av ledningens möten och deras frekvens, där säkerhet är en stående punkt på agendan.

Ett tydligt uttalande om organisationens åtagande att tillhandahålla tillräckliga resurser för att säkerhetssystemet ska fungera effektivt för att kontrollera riskerna.

Ett organisationsschema som tydligt fastställer säkerhetssystemets funktioner och vem som ansvarar för vad.

En strategi baserad på mänskliga och organisatoriska faktorer antas i utformningen av ny utrustning, t.ex. nya tåg. Denna strategi inbegriper att man tar hänsyn till användarnas erfarenheter i utformandet av nya konstruktionskrav, analyserar uppgifter för att identifiera kognitiva och fysiologiska utmaningar, minskar risken för felaktiga resultat på grund av konstruktionsfel genom att tillämpa riktlinjer för mänskliga faktorer såsom olika ISO- eller UIC-standards, analyserar hur arbetsbelastning och utmattning hanteras för att säkerställa de anställdas prestationer, utför riskanalyser för att identifiera potentiella problem och identifierar kompenserande åtgärder för dessa m.m. Miljöfaktorer såsom snö, värme, regn etc. beaktas, liksom socioekonomiska faktorer såsom organisatoriska prioriteringar, upphandling och nationell kultur.

Genom dokumenterade platsbesök visar ledningen sitt engagemang för att främja en positiv säkerhetskultur och sin önskan att föregå med gott exempel.

2.1.6 Referenser och standarder

- [Säkerhetskultur \(SKYbrary\)](#)

2.1.7 Tillsynsfrågor

Omfattningen av eventuella luckor mellan riktlinjer och förfaranden som tillhandahålls som en del av bevisningen ovan och den verklighet som observeras vid tillsynen, och i vilken utsträckning organisationen är medveten om dem, är centrala frågor för tillsynen.

Omfattningen av ledningens verkliga engagemang när det gäller säkerhetsstyrningssystemet och främjandet av en säkerhetskultur liksom de anställdas engagemang gentemot organisationen bör prövas vid tillsynen genom att organisationens egna mekanismer för att förstå och utveckla denna kultur och säkerhetsstyrningssystemet undersöks.

Kontrollera att organisationen kan visa att tillräckliga resurser avsätts för utveckling, genomförande, underhåll och kontinuerlig förbättring av säkerhetsstyrningssystemet.

Genom intervjuer med ledning och annan personal kontrollera hur ledningen uttrycker sitt engagemang för förbättring av säkerhet. Ta reda på hur ofta och på vilket sätt de har kontakt med personalen angående säkerhetsfrågor och/eller för att främja säkerhetskultur (workshoppar, forum, dedikerade säkerhetsdagar etc.).

Kontrollera om ledningen kommunicerat med de anställda om målen, antingen för att uppmuntra dem att bidra till att de uppfylls, eller för att tacka alla för förbättrade resultat.

2.2 Säkerhetspolicy

2.2.1 Reglerande krav

- 2.2.1. Ett dokument som beskriver organisationens säkerhetspolicy ska upprättas av högsta ledningen och ska vara:
- (a) anpassat till järnvägsverksamhetens typ och omfattning,
 - (b) godkänt av organisationens verkställande direktör (eller en företrädare för högsta ledningen),
 - (c) aktivt genomfört, kommunicerat och tillgängligt för all personal.
- 2.2.2. Säkerhetspolicyen ska:
- (a) omfatta ett åtagande att uppfylla alla rättsliga och andra krav kopplade till säkerhet,
 - (b) tillhandahålla en ram för att fastställa säkerhetsmål och utvärdera organisationens säkerhetsnivå i förhållande till dessa mål,
 - (c) omfatta ett åtagande att ha kontroll över både säkerhetsrisker som uppstår på grund av organisationens egen verksamhet och säkerhetsrisker som orsakas av andra,
 - (d) omfatta ett åtagande att kontinuerligt förbättra säkerhetsstyrningssystemet,
 - (e) upprätthållas i enlighet med verksamhetsstrategin och utvärderingen av organisationens säkerhetsnivå.

2.2.2 Syfte

Säkerhetspolicyen är ett viktigt dokument för att visa hur organisationen hanterar sitt säkerhetsansvar och sitt ledarskap och engagemang att hantera säkerheten på ett korrekt sätt. Sökanden bör kunna visa att den har en säkerhetspolicy som uppfyller kraven ovan, och som innehåller en sammanfattande beskrivning av grundstrukturen för riskkontroll.

I punkt 2.2.1 a i det reglerande kravet ovan menas för infrastrukturförvaltare *karaktär* istället för *typ*.

2.2.3 Förklarande anmärkningar

Säkerhetspolicyen är ett uttryck för ledningens filosofi, och detta avsnitt hänger därför nära samman med avsnitt 3.1. I ovannämnda reglerande krav nämns till exempel inte uttryckligen de mänskliga och organisatoriska faktorerna.

2.2.4 Bevis

- För järnvägsföretag: En skriftlig säkerhetspolicy undertecknad av den verkställande direktören som återspeglar driftens typ och omfattning, främjar efterlevnad av lagstiftning och andra föreskrifter, kontinuerliga förbättringar av säkerheten och som ger en ram för att fastställa säkerhetsmål. **(2.2.1 a, b, 2.2.2 a–c)**
- För infrastrukturförvaltare: En skriftlig säkerhetspolicy undertecknad av den verkställande direktören som återspeglar karaktären och omfattningen av järnvägsverksamheten och infrastrukturutvecklingen, främjar efterlevnad av lagstiftning och andra föreskrifter, kontinuerliga förbättringar av säkerheten och som används för att fastställa säkerhetsmål. **(2.2.2 a–c)**
- För båda: Information som anger att säkerhetspolicyen har kommunicerats till all personal. **(2.2.1 c)**

- Information om att säkerhetspolicyn hålls uppdaterad så att den alltid är i linje med organisationens affärsstrategi. **(2.2.2 d)**
- Bevis för att säkerhetspolicyn innehåller ett åtagande att övervaka säkerhetsnivån och att den revideras periodiskt som ett resultat av analys av säkerhetsnivån. Även bevis för att policyn ändras när säkerhetsnivån utvärderas mot de fastställda målen. **(2.2.2 b, d)**

2.2.5 Exempel på bevis

En daterad säkerhetspolicy, undertecknad av verkställande direktör, som återspeglar driftens typ, omfattning och karaktär. Dokumentet innehåller ett åtagande om kontinuerlig förbättring av säkerhetsstyrningssystemet.

Säkerhetspolicyn är aktuell och har en definierad granskningscykel i linje med företagets affärsstrategi.

Säkerhetsmålen överensstämmer med uppdraget och visionen såsom de presenteras i säkerhetspolicyn, och av detta framgår att målen värdesätts av personalen och att ansträngningar görs för deras engagemang med att uppnå dem.

Säkerhetspolicyn innehåller information eller referenser där processen beskrivs för hur policyn ska ändras när säkerhetsnivån i organisationen ses över mot de fastställda målen.

Det finns en process för att kommunicera säkerhetspolicyn genom organisationens intranät och för att visa den på strategiska/operativa platser.

2.2.6 Tillsynsfrågor

Vid tillsynen är det viktigt att pröva hur väl säkerhetspolicyn har kommunicerats till och uppfattas av all personal och vilken roll den spelar i verkligheten när den säkerhetsram inom vilken organisationen är verksam ska fastställas. En central fråga är huruvida dokumentet hjälper till att sätta agendan eller om det enbart existerar eftersom det krävs enligt lagen.

Kontrollera att förändringar i den organisatoriska säkerheten har utlöst en översyn av säkerhetspolicyn.

Kontrollera att säkerhetspolicyn speglar verkligheten i organisationen.

2.3 Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen

2.3.1 Reglerande krav

- 2.3.1. Ansvarsområden, ansvarsskyldighet och befogenheter för den personal som innehar en roll som påverkar säkerheten (inklusive ledningen och annan personal som har säkerhetsrelaterade arbetsuppgifter) ska fastställas på alla nivåer inom organisationen och ska dokumenteras, tilldelas och kommuniceras till denna personal.
- 2.3.2. Organisationens ska säkerställa att personal med delegerat ansvar för säkerhetsrelaterade arbetsuppgifter ska ha behörighet, kompetens och lämpliga resurser för att utföra sina arbetsuppgifter utan att påverkas negativt av andra funktioner inom verksamheten.
- 2.3.3. Delegering av ansvaret för säkerhetsrelaterade arbetsuppgifter ska dokumenteras och meddelas berörd personal, samt godtas och förstås.
- 2.3.4. Organisationens ska beskriva fördelningen av roller enligt 2.3.1. mellan verksamhetsfunktioner i, och i tillämpliga fall utanför, organisationen (se 5.3 Entreprenörer, partner och leverantörer).

2.3.2 Syfte

Syftet med detta krav är att få sökanden att ge en tydlig bild av strukturen i organisationen och hur roller och ansvar fördelas och upprätthålls över tid, från personer som arbetar i frontlinjen till den högsta ledningen. Detta är centralt för att förstå hur väl organisationens säkerhetsstyrningssystem kontrollerar risker. Sökanden ska visa hur behörig personal väljs ut för verksamheter, hur man säkerställer att dessa personer har en klar förståelse för sina roller och ansvarsområden och hur människor hålls ansvariga för sina resultat. Organisationsstrukturen och individens roller och ansvar balanserar mellan efterlevnad och säkerhetskultur – en kultur som baseras på tänkande snarare än på säkerhet driven av regelefterlevnad.

2.3.3 Förklarande anmärkningar

Det kan finnas ett glapp mellan förståelsen för säkerhetsstyrningsbestämmelserna på operativ nivå och de processer som är tänkta att driva säkerhetsstyrningssystemet (t.ex. riskbedömning, övervakning). Identifieringen av relevanta roller inom säkerhetsstyrningssystemet (**2.3.1**) är inte begränsad till dem med ansvar för hantering av säkerhetsprocesser, såsom säkerhetschefen eller säkerhetsteamet, utan inbegriper alla i befattningar som är involverade i säkerhetsrelaterade uppgifter, såsom driftpersonalen. Detta är oberoende av deras ledande eller icke-ledande befattningar inom organisationen (dvs. högre chefer, linjechefer, andra anställda/arbetstagare).

Befattningar, skyldigheter, ansvarsområden och befogenheter (**2.3.1**) bör omfatta utbyte av säkerhetsrelaterad information (**se även 4.4.1 och 4.4.2**). Till exempel vem som är ansvarig för att meddela lokförare sena ändringar.

Säkerhetsstyrningssystemet bör överensstämma med kraven i de gemensamma säkerhetsmetoderna för säkerhetsstyrningssystemet (**1.1.1 d**), och den högsta ledningen är ansvarig för att säkerställa att dess säkerhetsstyrningssystem uppfyller dem. Högsta ledningen får delegera vissa av sina skyldigheter till lämplig personal. Resultatrapportering sker i enlighet med kraven för ledningens översyn (**6.3**), där relevant personal har ansvar för att rapportera om säkerhetsstyrningssystemets resultat till högsta ledningen.

”Säkerhetsrelaterade uppgifter” (**2.3.1**) är inte begränsade till de uppgifter där säkerhet hanteras direkt (dvs. säkerhetskritiska uppgifter, som utförs av personal när de påverkar eller kontrollerar ett tågs rörelser, vilket kan påverka människors hälsa och säkerhet, såsom anges i TSD drift och trafikledning). De inbegriper även icke-operativa uppgifter som påverkar säkerheten.

”Delegering” **(2.3.3)** betyder överföring av ansvar till en underordnad från en överordnad, och sker oftast i syfte att påskynda organisationens reaktion i ärenden som uppstår. Säkerhetsansvar kan delegeras, dvs. spridas nedåt, inom tillämpningsområdet för de definierade arbetsuppgifterna, förutsatt att en sådan delegering dokumenteras. Ansvarsskyldighet för säkerhet kan inte delegeras. Det avser ansvarsskyldigheten för den person som hålls ansvarig om något inte görs, inte fungerar eller misslyckas med att uppnå sitt mål, att fastställa att han eller hon på ett tillfredsställande sätt fullgör sitt ansvar för säkerheten. Kommunikation om och godkännande av uppgifter **(2.3.3)**, inklusive säkerhetsrelaterade uppgifter, ingår i den normala verksamhetsprocessen för hur personal ska tilldelas funktioner, och detta bör vara kontrollerbart.

Hur roller fördelas **(2.3.4)** kan visas genom tillhandahållandet av ett lämpligt organisationsschema.

Ledningen bör ha tillräcklig kunskap och förståelse för mänskliga och organisatoriska faktorer för att säkerställa att specialister är engagerade när det behövs. Roller, skyldigheter, ansvarsområden för specialister inom mänskliga och organisatoriska faktorer bör definieras utifrån de uppgifter som ska slutföras. **(2.3.3)**.

Det bör finnas en process för att säkerställa att individer kan rapportera tillbud, incidenter och olyckor utan rädsla för återverkningar. Policyn stöder individers rättigheter och ansvar när det gäller att lyfta säkerhetsfrågor och tolererar inte trakasserier, hotelser, repressalier eller diskriminering för att detta görs. Nyckeln till framgång för en rättvis kultur är tillit och öppenhet i organisationen. Detta byggs upp över tid och är beroende av ledningens vilja att utföra omfattande analyser när tillbud och olyckor inträffar, samt att lyssna och lära innan man reagerar. Konsekvens i hantering av säkerhetsfrågor är viktigt för att etablera en rättvis kultur.

2.3.4 Bevis

- Ett organisationsschema och relevant text som beskriver hur organisationens säkerhetsansvar är strukturerat och hur säkerhetsstyrningssystemet är inrättat, och hur det kopplas samman med organisationens förutsättningar. **(2.3.1), (2.3.4)**
- En förteckning över annan information där ansvaret för säkerheten inom organisationens struktur beskrivs. **(2.3.1), (2.3.3)**
- Bevis för att ett kompetensstyrningssystem är på plats och underhålls för all personal som bedömer uppgifternas lämplighet, med fördelning av ansvar, kompetens och resurser. **(2.3.2)**
- Bevis från kompetensstyrningssystemet eller andra förfaranden på att organisationen säkerställer att roller och ansvar kommuniceras till, godtas och uppfattas av de anställda och att de kommer att hållas ansvariga för att utföra dem. **(2.3.3)**
- En beskrivning av ansvar för drift och underhåll, inklusive en definition av de krav som personal och entreprenörer i tillämpliga fall bör uppfylla. **(2.3.4)**
- Strategin för mänskliga och organisatoriska faktorer bör visa krav för när och hur expertis inom mänskliga och organisatoriska faktorer involveras och hur deras roll och ansvar ser ut. **(2.3.1), (se även 4.6)**

2.3.5 Exempel på bevis

Ett organisationsschema åtföljt av ytterligare text som möjliggör för bedömaren att se hur säkerhetsstyrningssystemet är strukturerat och hur dess olika delar relaterar till varandra.

Den process som omfattar hur säkerhetsansvaret fördelas och där delegeringsbefogenheter är tillåtna, med några exempel som visar hur processen har fungerat.

Exempel på arbetsbeskrivningar för säkerhetsrelaterade uppgifter, även de som inte är direkt kopplade till driften men som indirekt påverkar hur den fungerar (dvs. arbetsfördelning, driftsplanering och tillhandahållande av driftsinformation till personal, tillsynsverksamhet).

Hänvisning till kompetensstyrningssystemet med information om hur detta är strukturerat och länkar till platser där mer detaljerade uppgifter finns.

Den feedbackprocess som är i bruk för att säkerställa att information som har delgivits inom organisationen tydligt har uppfattats.

Förfarandet/förfarandena för att ta reda på vilken kompetens och vilka resurser som krävs för att backa upp säkerhetsuppgifter och säkerhetsansvar på alla nivåer i hierarkin.

Strategin för mänskliga och organisatoriska faktorer visar hur detta är integrerat i processer och projekt. Expertis och verksamheter med anknytning till mänskliga och organisatoriska faktorer är anpassade till storleken på den organisatoriska processen eller projektet. Roller, skyldigheter och ansvarsområden samt vid vilka steg experten inom mänskliga faktorer involveras anges i processen eller projektplanen.

2.3.6 Referenser och standarder

- [Säkerhetsskyldighet och säkerhetsansvar \(Skybrary\)](#)

2.3.7 Tillsynsfrågor

För tillsynen handlar detta om i vilken grad något görs eller sker. Frågan som måste besvaras är ”i vilken utsträckning återspeglar den tillhandahållna informationen verkligheten”?

En undersökning av kompetensstyrningssystemets funktionssätt är vägen att följa för att besvara de flesta frågorna i detta avsnitt.

2.4 Samråd med personal och andra parter

2.4.1 Reglerande krav

- | |
|--|
| <p>2.4.1. Personalen, dess företrädare och berörda parter utanför organisationen ska, i tillämpliga fall och vid behov, göras delaktiga i fråga om utveckling, upprätthållande och förbättring av säkerhetsstyrningssystemet i de för dem relevanta delar som de ansvarar för, inbegripet säkerhetsaspekterna av operativa förfaranden.</p> <p>2.4.2. Organisationen ska underlätta samråd med personalen genom att tillhandahålla de metoder och medel som krävs för att involvera personalen och ska dokumentera personalens synpunkter och ge återkoppling på personalens synpunkter.</p> |
|--|

2.4.2 Syfte

Sökanden bör styrka att man aktivt involverar såväl den egna personalen (eller deras företrädare) som externa berörda parter i att använda och utveckla säkerhetsstyrningssystemen och i att kontrollera riskerna över tid. Detta ger också en indikation för den bedömande myndigheten om hur säkerhetskulturen ser ut inom organisationen och hur aktivt man involverar relevanta tredje parter i riskhanteringen på de områden där risken delas.

Organisationen erkänner att ingen enskild person själv har all information som behövs för att hantera säkerheten på ett hållbart sätt. Processexperter, säkerhetsexperter, stödtjänster, personal i frontlinjen, chefer på alla nivåer, fackföreningar och externa entreprenörer – alla har och använder de kunskap och information som är avgörande för säkerheten. De måste ges möjlighet att träffas, diskutera och uttrycka sina åsikter för att få den bästa möjliga förståelsen av verkligheten på arbetsplatsen. Särskild uppmärksamhet behövs vid de organisatoriska gränssnitten mellan tjänster, avdelningar och organisationer. Utbytet av idéer och information om analys och behandling av risker, olyckor och tillbud bör främjas.

Engagemanget för att rapportera säkerhetskritisk information och delta i analysen av farliga situationer och händelser gynnas av ett klimat baserat på förtroende. Vid riskbedömning, utformning eller omvandling av tekniska installationer eller utarbetande av nya förfaranden söker man också aktivt efter driftspersonalens synpunkter på ett tidigt stadium.

2.4.3 Förklarande anmärkningar

Dessa externa parter (**2.4.1**) kan konsulteras i frågor som är relevanta för styrningssystemet. Exempelvis kan entreprenörer vara ansvariga för vissa säkerhetsrelaterade uppgifter som iordningställande av tåg eller infrastrukturunderhåll. När förfarandena för att iordningställa tåg eller för infrastrukturunderhåll bedöms är det god praxis att dessa entreprenörer deltar i processen.

Med externa parter avses organisationer som har ett gränssnitt med sökanden, såsom entreprenörer, partners, leverantörer, relevanta myndigheter, lokala styrande instanser eller räddningstjänst.

Utvecklingen av en positiv säkerhetskultur främjas genom relevant kommunikation av god kvalitet riktad till dem som behöver den.

2.4.4 Bevis

- Sökanden bör tillhandahålla information om processen för samråd med personalen (eller deras företrädare) och relevanta externa berörda parter, som inbegriper information om hur dessa samråd omvandlas till förändringar i säkerhetsstyrningssystemet eller specifika operativa förfaranden. (**2.4.1**), (**2.4.2**)

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.

- *Sökanden bör tillhandahålla information om det befintliga systemet för att ge återkoppling till personalen om samrådets resultat. (2.4.2)*

2.4.5 Exempel på bevis

Processen eller förfarandet för samråd med personalen (och, i förekommande fall, deras företrädare) och berörda parter för att utveckla säkerhetsstyrningssystemet.

Exempel på protokoll från samrådsmöten som hållits med personalen (och/eller deras företrädare) med redovisade resultat.

Exempel på hur åsikter och förslag från personalen samlas in i hanteringen av en förändring (dvs. i ett utkast till/ändrat/nytt operativt förfarande) och hur de behandlas.

Ett dokument/ett förfarande som visar hur driftspersonalen, som kommer att arbeta med nya eller utvecklade tekniska system, involveras i ett tidigt skede (planering och utveckling) av arbetet, för att samla in synpunkter rörande t.ex. samspelet människa–maskin.

Det finns förfaranden som anger hur mänskliga och organisatoriska faktorer bör hanteras och hur resultaten bör kommuniceras inom organisationen i förhållande till organisationens affärsmål och organisatoriska processer, t.ex. projekt, utredningar av tillbud och olyckor, riskanalyser och andra säkerhetsrelaterade aktiviteter för den egna personalen, entreprenörer, partner och leverantörer.

Organisationen bör tydligt definiera förväntningar i fråga om säkerhet och vilket beteende som krävs. De organisatoriska prioriteringarna är justerade för att undvika motstridiga mål. En process beskrivs för planering, riskbedömning och kontroll av verksamheter, t.ex. genom traditionellt beslutsfattande, för att se till att säkerheten inte äventyras av andra verksamhetsintressen. Säkerhetsmålen är kopplade till säkerhetskulturen. Ledningen tar en aktiv roll i planering och genomförande av nödvändiga förändringar av säkerhetskulturen.

2.4.6 Tillsynsfrågor

Samråd med och medverkan av relevant personal både internt och externt är viktigt för att säkerställa att personer med relevant erfarenhet har möjlighet att inverka positivt på säkerhetsstyrningssystemet i organisationen.

Tillsynen inom detta område bör inriktas på redovisningar om hur personalen och externa parter konsulteras och hur deras synpunkter beaktas, samt på dokumentation av förändringar i det säkerhetsstyrningssystem som utgår från detta område.

Särskild uppmärksamhet bör ägnas åt hur feedback ges och vilka lärdomar som dras därav.

3 Planering

3.1 Åtgärder för att hantera risker

3.1.1 Reglerande krav

3.1.1 Riskbedömning

3.1.1.1 Organisationen ska

- (a) identifiera och analysera alla operativa, organisatoriska och tekniska risker som är relevanta för typen och omfattningen av och området för den verksamhet som organisationen utför; sådana risker ska även omfatta dem som uppstår på grund av mänskliga och organisatoriska faktorer som arbetsbörda, arbetets utformning, utmattning eller lämplighet i förfaranden, samt andra berörda parter aktiviteter (se 1. Organisationens förutsättningar),
- (b) utvärdera risker som avses i punkt a genom att tillämpa lämpliga metoder för riskbedömning,
- (c) utveckla och införa säkerhetsåtgärder, och fastställa ansvar knutet till dessa (se 2.3 Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen),
- (d) utveckla ett system för att övervaka säkerhetsåtgärdernas effektivitet (se 6.1 Övervakning),
- (e) erkänna behovet av att, i tillämpliga fall, samarbeta med andra berörda parter (t.ex. järnvägsföretag, infrastrukturförvaltare, tillverkare, underhållsleverantörer, underhållsansvarig enhet, fordonsinnehavare, tjänsteleverantörer och upphandlande enheter) om delade risker och införandet av lämpliga säkerhetsåtgärder,
- (f) kommunicera risker till personal och berörda parter utanför organisationen (se 4.4 Information och kommunikation).

3.1.1.2 När organisationen bedömer risker ska den beakta behovet av att definiera, erbjuda och upprätthålla en säker arbetsmiljö som uppfyller kraven i tillämplig lagstiftning, i synnerhet direktiv 89/391/EEG.

3.1.2 Planering av ändringar

3.1.2.1 Organisationen ska identifiera potentiella säkerhetsrisker och lämpliga säkerhetsåtgärder (se 3.1.1 Riskbedömning) innan en ändring införs (se 5.4 Hantering av ändringar), i enlighet med den riskhanteringsprocess som anges i förordning (EU) nr 402/2013 (1), samt beakta de säkerhetsrisker som kommer av själva ändringsprocessen.

3.1.2 Syfte

Detta krav rör själva kärnan i säkerhetsstyrningssystemet och syftar till att få sökanden att visa hur dess system identifierar och kontrollerar de risker de möter. Det ställer också krav på sökanden att visa hur resultaten av riskbedömningen används i praktiken för att förbättra riskkontrollen och hur man kontrollerar detta över tid. Det är viktigt att komma ihåg att detta krav inte direkt behandlar hur riskerna från förändringar hanteras (vilket är ett annat krav), men att det är relaterat till det. Det bör också noteras att det finns ett specifikt krav på att hantera frågor som rör mänskliga prestationer via riskbedömning, såsom utformning av arbete och riskhantering i fråga om utmattning.

Hur denna information organiseras och kommuniceras som en del av säkerhetsstyrningssystemet ankommer på den sökande att beskriva, och innehållet bör spegla de risker organisationen stöter på mot bakgrund av driftens typ, omfattning och område (se organisationens förutsättningar). Det är lämpligt att hantera både de risker som sökanden ansvarar för och de risker som härrör från verksamheter utförda av tredje parter.

En gemensam förståelse, i hela organisationen, för hur man kan förebygga betydande risker ses som en prioritering vid god säkerhetsstyrning. Att ett visst scenario inträffar sällan bör inte leda till det ignoreras. För att säkerställa att ett scenario som valts ut för riskbedömning är realistiskt i förhållande till den verkliga driften, bidrar både experter inom säkerhetsstyrning och operatörer i spetsen av verksamheten till säkerhetsanalysen och riskbedömningen. Resultaten av dessa bedömningar kommuniceras i ett tillgängligt

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.

och begripligt format till alla aktörer som bidrar till säkerheten. Chefer och ledning främjar diskussioner om betydande risker som ska hanteras, för att säkerställa en gemensam förståelse och medvetenhet. Förekomsten av betydande risker betonas också under hela livscykeln för systemet.

3.1.3 Förklarande anmärkningar

Vid bedömningen av en ansökan bör sökanden visa hur överensstämmelse med rådets direktiv 89/391/EEG och tillhörande förordningar säkerställs. Bedömningen fokuserar på hur sökanden visar att dessa frågor hanteras, och inte på själva frågorna. Frågor som utmattnings- eller stresshantering, liksom prövning av fysisk och psykisk lämplighet, kan behandlas som en rättslig fråga inom ramen för arbetsmiljöfrågor. De angränsar dock till kompetensstyrningssystemen (t.ex. för utbildning efter lång frånvaro) och har även att göra med arbetsfördelning (personalen bör tilldelas vissa jobb endast om man konstaterat att de är lämpliga för dem), vilket anges i TSD drift och trafikledning.

I punkt 3.1.1.1 a i det reglerande kravet har för infraförvaltare ordet "typ" ersatts med "karaktär" i bedömningen.

"Verksamhet" (**3.1.1.1 a**) avser i det här fallet både de åtgärder som de berörda parterna (entreprenörer, leverantörer och andra) genomför på uppdrag av eller i samarbete med en sökande och även de tillgångar som används som stöd för dessa åtgärder. Det viktiga är att sökanden måste visa att man har en robust process för riskbedömning och att alla relevanta risker behandlas. Vissa risker (t.ex. hydrogeologiska risker, risker vid plankorsningar, stenar som kastas på tåg, inkräktare) måste också beaktas av organisationen när det är lämpligt och rimligt. Dessa problem är relaterade till operativa risker (eftersom de alla påverkar tågtrafik) och har inte nödvändigtvis att göra med enbart mänskliga prestationer.

"Andra berörda parter" avser både organisationer och individer. Dessa parter kan vara externa till järnvägssystemet (**1.1.1 c**).

En förändring kan vara eller inte vara säkerhetsrelaterad (**3.1.2.1**). Effekterna av eventuella säkerhetsrelaterade ändringar bör bedömas och lämpliga säkerhetsåtgärder identifieras för att minska riskerna till en acceptabel nivå. Genomförandet av förändringshanteringsprocessen kan också leda till säkerhetsrisker, särskilt när man beslutar att senarelägga genomförandet av en förändring för att man, delvis eller helt, måste undvika att skapa en annan säkerhetsrisk. Riskhantering (**3.1.1.1**) är dock inte exklusivt för förändringshantering. I allmänhet bör organisationen säkerställa att de säkerhetsrisker som rör verksamheten hanteras på lämpligt sätt. Behovet av att identifiera, hantera och kontrollera dessa säkerhetsrisker, som en del av sökandens säkerhetsstyrningssystem, sträcker sig därför längre än förändringshanteringen och tillämpningen av de gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning.

De gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning gäller för alla tekniska, driftsmässiga eller organisatoriska förändringar (för de senare avses förändringar med konsekvens för drift eller underhåll). För varje säkerhetsrelaterad förändring måste sökanden/förslagsställaren först avgöra om förändringen är betydande (eller inte). Om den anses vara det måste sökanden, med användning av de principer som beskrivs i de gemensamma säkerhetsmetoderna, visa att de risker som är relaterade till förändringen är godtagbara och att de krav som uppstår vid denna demonstration har införlivats effektivt i systemet som genomgår förändring. Den utförda riskbedömningen bedöms sedan av ett oberoende eller erkänt bedömningsorgan som skriver en rapport om huruvida analysen är godtagbar eller inte. De nationella säkerhetsmyndigheterna beaktar dessa rapporter i sin tillsynsverksamhet, men de utmanar inte resultaten i rapporterna om de inte har anledning att tro att processen för att utvärdera riskbedömningen inte har följts korrekt. När förändringen är säkerhetsrelaterad men inte väsentlig, måste sökanden/förslagsställaren dokumentera sitt beslut och fortfarande göra en riskbedömning av förändringen i enlighet med

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.

riskhanteringsprocessen i säkerhetsstyrningssystemet. Det är i detta fall sökandens ansvar att välja lämplig riskbedömningsmetod för att motivera att befintliga riskkontrollåtgärder är lämpliga för att styra riskerna till en godtagbar nivå. Det bör noteras att medan det som triggar i gång tillämpningen av de gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning är huruvida en förändring är väsentlig eller inte, så kan en organisation välja att tillämpa dessa metoder under andra omständigheter, till exempel om man anser att en oberoende utvärdering av det arbete som organisationen gjort motiveras av kommersiella eller samhälleliga skäl.

De gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning innehåller sex kriterier som bör undersökas för att avgöra "väsentlighet". Här avses följande:

- **Konsekvens av bristande funktion:** ett trovärdigt "värsta fall"-scenario om det system som bedöms inte skulle fungera, med beaktande av säkerhetsbarriärer utanför systemet.
- **Innovation som används för att genomföra ändringen:** det kan röra sig både om en innovation för hela järnvägssektorn och om en nyhet just för den organisation som genomför ändringen. **Ändringens komplexitet.**

Övervakning: Det är inte möjligt att övervaka den genomförda ändringen under systemets hela livscykel och göra lämpliga ingripanden. **Reverserbarhet:** Det saknas möjligheter att återgå till det system som rådde före ändringen. **Additionalitet:** Bedömning av ändringens betydelse med beaktande av alla nyligen vidtagna säkerhetsrelaterade ändringar av det system som står under bedömning, vilka inte har bedömts som väsentliga. Dessa element bör användas för att bedöma hur organisation nått fram till beslut om "väsentlighet" inom ramen för de gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning.

Även om riskhanteringsprocessen som anges i de gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning tillämpas vid säkerhetsrelaterade och väsentliga förändringar, är det vanlig praxis att använda de principer som ligger till grund för riskhanteringsprocessen som ingår i denna förordning, och de kan därför tillämpas i alla andra situationer där riskbedömning behövs.

Det finns en systematisk metod för att identifiera säkerhetskritiska arbetsuppgifter och processer, och metoder inom ramen för mänskliga och organisatoriska faktorer används för att analysera säkerhetskritiska arbetsuppgifter, t.ex. uppgiftsanalyser, hierarkiska uppgiftsanalyser (HTA) och uppgiftsanalyser i tabellform (TTA). Experter inom mänskliga och organisatoriska faktorer bör användas för att välja och tillämpa lämpliga metoder.

Riskbedömningsprocessen bör beskriva hur experter inom mänskliga och organisatoriska faktorer och relevanta kompetenser involveras, liksom användare och andra berörda parter. Detta kan till exempel omfatta en beskrivning av i vilken utsträckning experter inom mänskliga och organisatoriska faktorer bör involveras i riskanalysen och vilken nivå av mänsklig och organisatorisk kompetens som behövs.

Lämpliga metoder för att integrera mänskliga och organisatoriska faktorer i riskbedömningen beskrivs, såsom uppgiftsanalys, användbarhetsanalys, simulering, faro- och operabilitetsanalys (Hazop) av mänskliga faktorer och olycksfjärilsanalys (bowtie-metod).

3.1.4 Bevis

- *Sökanden bör tillhandahålla bevis för att den har en riskbedömningsprocess (med en beskrivning av de metoder som används, vilken personal som berörs och all validering eller kontroll som genomförts) som omfattar både risker som identifierats som betydande förändringar utifrån de gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning (kommissionens genomförandeförordning (EU) 2015/402) och risker som ej anses vara väsentliga men som ändå bör kontrolleras och processen omfattar alla operativa, organisatoriska och tekniska risker. (3.1.1.1 a, b)*

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.

- Bevis på att risker associerade med mänskliga och organisatoriska faktorer beaktas i riskbedömningarna. Strategin för mänskliga och organisatoriska faktorer borde visa hur och när mänskliga och organisatoriska faktorer är en integrerad del av riskbedömningen och demonstrera användningen av lämpliga metoder och expertis. **(3.1.1.1 a)**
- Bevis på hur lämplig tredje part kan involveras i riskbedömningen, inklusive hur risker från tredje part påverkar driften för järnvägsföretaget eller infrastrukturförvaltaren. **(3.1.1.1 a), (3.1.1.1 e), (3.1.1.1 f)**
- Bevis för att sökanden har en process på plats för att utveckla och införa riskkontrollåtgärder, inbegripet vem som ansvarar för att de är klara. **(3.1.1.1 c)**
- Sökanden bör ange hur man engagerar och kommunicerar resultaten av riskbedömningen och de associerade kontrollåtgärderna till berörd personal. **(3.1.1.1 f)**
- Sökanden bör visa hur man övervakar effektiviteten av sina åtgärder för riskkontroll, inklusive hur processer eller förfaranden uppdateras efter behov. **(3.1.1.1 d)**
- I den bevisning som sökanden tillhandahåller bör det anges hur man tar hänsyn till behovet att efterleva annan tillämplig lagstiftning, som exempelvis den som införts i enlighet med rådets direktiv 89/391/EEG. **(3.1.1.2)**
- Sökanden ger bevis som styrker att man, som en del av sin förändringshanteringsprocess, systematiskt utvärderar effekterna av alla förändringar. Detta innebär användning av riskbedömning inklusive användning av de gemensamma säkerhetsmetoderna för riskvärdering och riskbedömning för att identifiera riskerna och de nödvändiga kontrollåtgärderna. Sökanden ger också bevis för att de kontrollåtgärder som identifierats under förändringshanteringsprocessen har genomförts. **(3.1.2.1)**

3.1.5 Exempel på bevis

En process eller ett förfarande för riskbedömning där det i förekommande fall beskrivs hur och när felanalys och felbedömning, faro- och operabilitetsanalys (Hazop) eller andra tekniker används för att stödja genomförandet av kontrollåtgärder för att hantera risker.

Bevis såsom ett faroregister som visar att organisationen har en process för att systematiskt utvärdera risker som ett första steg i sin riskhantering. Registret bygger på resultaten från övervakningen och uppdateras så fort nya risker upptäcks, kompletterat med lämplig information om de säkerhetsåtgärder som antagits för att hålla risker under kontroll (t.ex. teknisk utrustning, operativt förfarande eller personalutbildning).

En översikt över de delar i processen som hanterar hur mänskliga faktorer beaktas i riskbedömningen, och hur i förekommande fall tredje parter är involverade.

Förfarandet för att kommunicera resultaten av riskbedömningar till personalen, med belysande exempel vid behov.

Förfarande för att säkerställa överensstämmelse med annan relevant EU-lagstiftning såsom rådets direktiv 89/391/EEG, i de fall där risker relaterade till personalen (dödsfall, tillfälliga eller permanenta skador eller tillbud) kan omfattas av den rättsliga ramen för arbetsmiljö, men kontrollåtgärderna bör ingå i eller vara ett komplement till driftsregler.

En indikation på att processen för att säkerställa att de säkerhetsrelaterade uppgifterna som delegerats till varje personalkategori är utformade på ett sådant sätt att

- volymen av uppgifter som ska slutföras inte är för stor vid tidpunkter när säkerhetsrelaterade uppgifter genomförs,

- *i de fall säkerhetsrelaterade uppgifter slås ihop, organisationen kan visa att säkerhetsnivån upprätthålls,*
- *inga motsättningar finns mellan fullgörandet av säkerhetsrelaterade uppgifter och andra mål som tilldelats personalen (i enlighet med 2.1.1 j).*

Det finns en strategi baserad på mänskliga och organisatoriska faktorer kopplad till riskbedömningsprocesser, som visar att resultaten från riskanalyser används och att säkerhetsförbättrande åtgärder genomförs och utvärderas.

3.1.6 Referenser och standarder

- [Vägledning för tillämpningen av kommissionens förordning om antagande av en gemensam säkerhetsmetod för riskvärdering och riskbedömning](#)
- [Kriterier för riskacceptans i tekniska system och driftsprocedurer som används i olika industrier](#)
- [Vägledning som stödjer implementeringen av förordning 2015/1136 gällande harmoniserade designmål \(CSM DT\) inom ramen för en gemensam säkerhetsmetod för riskvärdering och riskbedömning.](#)
- ISO 31000:2009 Riskhantering
- ISO 31010:2009 Riskhantering – riskbedömningstekniker

3.1.7 Tillsynsfrågor

Tillsynen bör fokusera på riskbedömningsprocessen, säkerhetsstyrningssystemets kärna. Det bör därför vara möjligt att från intervjuer och kontroller av dokumentation och processer upptäcka om den även är det i verkligheten. Alla tillsynsresultat som är relevanta för den framtida förnyelsen av ett gemensamt säkerhetsintyg eller säkerhetstillstånd är viktiga här. I den mån det behövs bör dessutom alla resultat från tillsyn av riskbedömningsprocesser bidra till de nationella säkerhetsmyndigheternas tillsynsstrategier.

Följande information kan vara till hjälp för framtida tillsyn:

- *Förteckning över faror.*
- *Risikanalyseresultat, inklusive rapporter från det eller de organ som utför riskbedömning, i förekommande fall.*
- *Motiv för användningen av riskbedömningsmetoder (t.ex. analys av allvarligheten av feltillstånd och felorsaker, FTA, ETA, Hazop), inklusive hur riskbedömningskriterier och farors allvarlighetsgrad och sannolikhet för förekomst fastställs.*
- *I förekommande fall, en klassificering av farliga händelser efter ämne, effekter eller orsaker (t.ex. en preliminär förteckning över faror).*

Anställda vars ansvarsområden är kopplade till riskbedömning bör vara medvetna om innebörden av deras roll och vikten av processen samt vara behöriga att utföra den effektivt.

Det är särskilt viktigt att flera exempel på riskbedömningar undersöks eftersom det visar om riskerna behandlas korrekt med hjälp av en lämplig metod. Fältobservationer bör sedan visa att de identifierade kontrollåtgärderna finns på plats.

3.2 Säkerhetsmål och planering

3.2.1 Reglerande krav

3.2.1	Organisationen ska fastställa säkerhetsmål för relevanta funktioner på relevanta nivåer för att upprätthålla och, när så är praktiskt genomförbart och rimligt, förbättra säkerhetsnivån.
3.2.2	Säkerhetsmålen ska <ul style="list-style-type: none">(a) vara förenliga med säkerhetspolicyn och organisationens strategiska mål (i tillämpliga fall),(b) vara kopplade till de prioriterade risker som påverkar säkerhetsnivån inom organisationen,(c) vara mätbara,(d) beakta tillämpliga rättsliga samt andra krav,(e) ses över med avseende på hur de uppnås, och revideras vid behov,(f) kommuniceras.
3.2.3	Organisationen ska ha en plan/planer för att beskriva hur den ska uppnå sina säkerhetsmål.
3.2.4	Organisationen ska beskriva den strategi och den plan/de planer som används för att övervaka att säkerhetsmålen uppnås (se 6.1 Övervakning).

3.2.2 Syfte

Säkerställa att organisationen uppfyller rättsliga krav och se till att konceptet ständig förbättring i fråga om säkerhet kommuniceras till personalen, och att ledningen tror på det.

Sökanden måste visa att man har meningsfulla mål och en process för att genomföra och övervaka dessa mål under deras livstid.

3.2.3 Förklarande anmärkningar

Med säkerhet avses i detta fall organisationens resultat i förhållande till dess säkerhetsmål och resultaten för säkerhetsstyrningssystemet och alla de processer och förfaranden som stöder det.

[Utgår ur den svenska översättningen.] Säkerhetsmålen skiljer sig från de gemensamma säkerhetsmål som fastställts på medlemsstatsnivå. Vissa företag kan dock använda de sistnämnda som mål som ska uppnås, för att bibehålla eller förbättra sin säkerhet.

Säkerhetsmålen är kopplade till risker, eftersom dessa påverkar organisationens säkerhet (dvs. säkerhetsstyrningssystemets avsedda resultat och därmed framgången med att uppfylla målen). Säkerhetsmålen kan vara kvantitativa, angivna som en minskning av antalet händelser i absolut värde eller procentuellt. Säkerhetsmålen kan också vara kvalitativa, uttryckta som ett generiskt värde som "säkerheten vid plankorsningar kommer att förbättras" eller "den nuvarande säkerhetsnivån kommer att bibehållas".

Med användning av en PGSA-strategi (*Plan, Do, Check, Act*) bör målen ses över regelbundet. När prioriteringar fastställs för att upprätthålla och om möjligt förbättra säkerheten bör hänsyn tas till riskbedömningsresultat och resultat från tidigare övervakning och utredningar av olyckor och tillbud.

Fastställandet och övervakningen av säkerhetsindikatorer som stöder organisationens beslutsprocesser för riskkontroll och huruvida dessa är effektiva, är information som bidrar till fastställandet och granskningen av säkerhetskraven.

3.2.4 Bevis

- *Det finns en uppsättning säkerhetsmål för organisationen som är specifika, mätbara, uppnåbara, realistiska och tidsbundna (Significant, Measurable, Achievable, Realistic and Time bound, Smart) för organisationens bredare affärsbehov. (3.2.1), (3.2.2 a, b, c)*
- *En förklaring om de rättsliga kraven och hur de efterlevs. (3.2.2 d)*
- *En beskrivning av hur dessa mål kan uppnås och kommuniceras till berörda anställda. (3.2.2 f), (3.2.3)*
- *Det finns en övervakningsprocess, förenlig med de krav som anges i den gemensamma säkerhetsmetoden för övervakning (förordning (EU) nr 1078/2012), för att säkerställa att de konsekvent är lämpliga för ändamålet och att organisationen uppnår sina mål. (3.2.2 e), (3.2.4)*

3.2.5 Exempel på bevis

Den process som fastställer säkerhetsmålen prioriteras och övervakas samt bevis på hur konflikter med andra mål har undvikits och, om de inte har kunnat undvikas, hur de har lösts. Detta bör omfatta nivån målen sätts på och hur de i tillämpliga fall bidrar till andra mål på andra nivåer, samt gränssnitt, tidsplanering och eventuella nödvändiga stödjande kvalitativa eller kvantitativa data.

Säkerhetsmålen och planen för att leverera dem tillsammans med den process som ska följas när det framgår att säkerhetsmålen inte kommer att nås.

Process eller förfarande för att omvandla resultaten från övervakningen till säkerhetsmål, planering av åtgärder för att uppnå dem och relaterade resultatindikatorer.

3.2.6 Tillsynsfrågor

En central fråga för tillsynen är hur uppnåbara de fastställda målen är i praktiken och vad som faktiskt händer om det börjar framkomma att det är osannolikt att de kommer att uppfyllas.

Hur säkerhetskraven fastställs och granskas – att målen inriktas på utsatta eller kritiska verksamheter/kontrollerar och utnyttjar resultat och verksamhetsindikatorer.

Hur organisationen uppvisar kontinuerliga förbättringar av riskkontrollen genom sina säkerhetsmål.

Utvärdera om organisationen effektivt kan övervaka sin säkerhet och därför använda de gemensamma säkerhetsmetoderna för övervakning för att bedöma sina resultat i förhållande till säkerhetsmålen och relaterade säkerhetsindikatorer.

Ta ett exempel på ett mål (som t.ex. definierats några år tidigare) och se om och hur det har spårats från fastställandet till det slutliga resultatet (eller misslyckandet).

4 Stöd

4.1 Resurser

4.1.1 Reglerande krav

4.1.1 Organisationen ska tillhandahålla de resurser, inbegripet kompetent personal och effektiv och användbar utrustning, som behövs för att införa, genomföra, upprätthålla och kontinuerligt förbättra säkerhetsstyrningssystemet.

4.1.2 Syfte

Syftet med detta krav är att se till att organisationen har processer på plats för att kunna tillhandahålla de resurser som krävs i fråga om t.ex. teknisk utrustning, tekniska system eller kompetent personal för att dess säkerhetsstyrningssystem ska ha möjlighet att kontrollera risker i enlighet med sina mål.

4.1.3 Förklarande anmärkningar

Att avsätta tillräckliga resurser är en grundförutsättning för att uppnå en lämplig säkerhetsnivå.

4.1.4 Bevis

- Information om kompetensstyrningssystemet eller, i den händelse att ett kompetensstyrningssystem inte finns, belägg för hur organisationen säkerställer att den har tillräckligt kompetent personal på plats. **(4.1.1)**
- Information om vad organisationen gör för att säkerställa att den har den utrustning som krävs för att kunna fullgöra sina skyldigheter att tillhandahålla tjänster och upprätthålla ett effektivt säkerhetsstyrningssystem som kontrollerar risker. **(4.1.1)**
- Information om hur underhållsfunktioner organiseras och på vilket sätt de är kopplade till tillhandahållandet av tillräckliga resurser för att organisationen ska kunna uppfylla sina skyldigheter att tillhandahålla tjänster. **(4.1.1)**

4.1.5 Exempel på bevis

En redogörelse för hur beslut om bemanningskrav fattas för säkerhetsstyrningssystemets effektiva fungerande samt upplysningar om relevanta referensförfaranden eller referensprocesser där ytterligare information kan hittas.

Förfarandet för hantering av kompetens eller upplysningar om den process som syftar till att säkerställa att organisationen har kompetent personal i relevanta befattningar, med detaljerad information om utbildningsprogram i tillämpliga fall **(se även 4.2)**.

Uppgifter om processen för resursallokering för att uppfylla operativa behov tillsammans med relevanta referenser till stöddokument.

Ett dokument som anger hur resurser allokeras för planerade stora förändringar i organisationen (inklusive bemanning och leverans av nödvändig utrustning).

4.1.6 Tillsynsfrågor

Kontrollera att kraven på kompetensramen och utrustningen är tydligt kopplade till riskbedömningsresultaten.

När kompetensstyrningssystemet kontrolleras bör den nationella säkerhetsmyndigheten kontrollera att organisationen har möjlighet att identifiera och behålla personal med rätt kompetens för att kunna utföra sina uppgifter på ett säkert sätt. En central fråga är hur kompetensstyrningssystemet hålls uppdaterat.

Vid granskning av underhållsaktiviteter som relaterar till detta krav bör tillsynsutövarna sträva efter att säkerställa att, där dessa verksamheter läggs ut på entreprenad, järnvägsföretaget eller infrastrukturförvaltaren utövar sin översynsfunktion för att säkerställa att entreprenörerna levererar en lämplig produkt som är säker att använda.

Kontroller av vakansluckor inom utvalda områden av säkerhetsstyrningssystemet kan användas som en indikator för om det är lämpligt eller ej att använda mänskliga resurser.

På samma sätt kan hur utrustningen används, t.ex. hur många reservdelar som tas till platsen, indikera kvaliteten på den utrustning som tillhandahålls och därmed resursernas lämplighet.

4.2 Kompetens

4.2.1 Reglerande krav

4.2.1	Organisationens kompetensstyrningssystem ska säkerställa att personal som har en roll som påverkar säkerheten har kompetens för de säkerhetsrelaterade arbetsuppgifter som de ansvarar för (se 2.3 Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen), vilket minst ska omfatta: <ul style="list-style-type: none">(a) fastställande av den kompetens (dvs. kunskap, färdigheter, beteenden och attityder på andra områden än tekniska områden) som krävs för säkerhetsrelaterade arbetsuppgifter,(b) urvalsprinciper (krav på grundläggande utbildningsnivå, psykisk och fysisk lämplighet),(c) grundläggande utbildning, erfarenhet och kvalifikationer,(d) fortlöpande utbildning och regelbunden uppdatering av befintlig kompetens,(e) regelbunden kompetensbedömning och kontroll av psykisk och fysisk lämplighet för att säkerställa att kvalifikationer och färdigheter upprätthålls fortlöpande,(f) särskild utbildning avseende relevanta delar av säkerhetsstyrningssystemet så att de kan utföra sina säkerhetsrelaterade arbetsuppgifter.
4.2.2	Organisationen ska tillhandahålla ett utbildningsprogram enligt punkt 4.2.1 c, d och f för personal som utför säkerhetsrelaterade arbetsuppgifter, som säkerställer att: <ul style="list-style-type: none">(a) programmet genomförs med hänsyn till de identifierade kompetenskraven och personalens enskilda behov,(b) programmet säkerställer, i tillämpliga fall, att personalen kan fungera under alla former av driftsförhållanden (normala, vid störning och i nödsituationer),(c) utbildningens varaktighet och den frekvens med vilken repetitionsutbildning anordnas anpassas till utbildningsmålen,(d) dokumentation förs för all personal (se 4.5.3 Kontroll över dokumenterad information),(e) programmet regelbundet ses över och internrevideras (se 6.2 Internrevision) och ändras vid behov (se 5.4 Hantering av ändringar).
4.2.3	Det ska finnas rutiner för återgång i arbete för personal efter olyckor/tillbud eller lång frånvaro från arbetet, inbegripet extra utbildning om ett sådant behov identifieras.

4.2.2 Syfte

Syftet med detta krav är att säkerställa att organisationen har lämpliga strukturer och resurser på plats för att kontrollera de risker den möter och ha möjlighet att sätta in anställda med behörighet att fullgöra säkerhetsfunktionerna, och i synnerhet dem som är av säkerhetskritisk natur, som den utför. Kompetensstyrningssystemet möjliggör också för organisationen att upprätthålla personalens kompetens, kunskap och erfarenhet över tid.

Kompetens spelar en central roll i att säkerställa att verksamheten bedrivs på ett tillfredsställande sätt. Behovet av att ha kompetent personal omfattar både stöd i frontlinjen (inklusive entreprenörer, konsulter och leverantörer av säkerhetsrelaterade tjänster) och ledningspersonal. Krav på ledningspersonalens kompetens förbises ofta, men chefer fattar viktiga beslut som kan ha grundläggande och omfattande effekter på hälsa och säkerhet. Dessa krav bör innehålla bestämmelser om utbildning för alla anställda om de säkerhetsnormer som gäller och om hur kompetens upprätthålls oavsett omständigheter, och inbegripa frågor som personaltillgänglighet och övervakning av kompetensnivåer i förhållande till de standarder som gäller.

I detta sammanhang ses säkerhet som en integrerad del i ett professionellt beteende och professionalism – och inte som ett ”extra lager” att lägga ovanpå yrkeskunskaperna. En organisations förmåga att i realtid hantera oväntade händelser är också mycket beroende av kompetensen hos personalen i frontlinjen och dess arbetsledare. Dessa kompetenser kan till exempel utvecklas genom simuleringar av och regelbunden utbildning om komplexa scenarier.

4.2.3 Förklarande anmärkningar

Ett utbildningsprogram **(4.2.2)** kan tillhandahållas via ett utomstående utbildningscentrum. I detta fall bör organisationen säkerställa att utbildningscentret har behörighet att tillhandahålla de relevanta tjänsterna antingen eftersom det har certifierats som ett erkänt centrum i ett nationellt eller europeiskt system eller genom att utbildningsaktiviteterna och resultaten från utbildningen övervakas direkt. Utbildningscentrum kan tillhandahålla en organisations samtliga utbildningsbehov eller endast några av dem, baserat på deras kompetens inom olika områden. När ett utomstående utbildningscentrum erbjuder utbildning till en organisation, måste organisationen ifråga kontrollera att utbildningen omfattar relevanta delar. Där så inte är fallet behöver organisationen komplettera sådan extern utbildning med intern utbildning.

”Attityd” **(4.2.1 a)** används för att beskriva hur människor reagerar på vissa situationer och hur de beter sig i allmänhet (de kan t.ex. vara proaktiva, komma bra överens med andra människor). Detta är mycket viktigt för sammankopplingarna mellan arbetet inom säkerhetsstyrningssystemet.

Det bör finnas en systematisk metod för att säkerställa att kompetens om mänskliga och organisatoriska faktorer finns tillgänglig, antingen hos personal i relevanta roller som baserats på en behovsanalys, eller genom jourtjänstgörande personal.

Kompetens inom mänskliga och organisatoriska faktorer bör till exempel användas i projekt i samband med nya eller ändrade mönster, vid olycksanalyser för att tillhandahålla ett icke-tekniskt perspektiv eller när det är fråga om problem kopplade till mänskliga prestationer.

4.2.4 Bevis

- Sökanden ska tillhandahålla information om sitt kompetensstyrningssystem och hur det fungerar för att uppfylla de angelägenheter som anges i kraven. **(4.2.1), (4.2.2 a–e)**
- Bevisen ska omfatta uppgifter om de utbildningsprogram som finns för personalen (inklusive, där det är nödvändigt, organisationens krav på behörighet hos utbildare) och hur dessa hålls uppdaterade och granskade (inklusive när nödvändigt, för säkerhetsrådgivare-rollen inom ramen för bestämmelserna om internationella järnvägstransporter av farligt gods (RID)). **(4.2.2 a–f)**
- Bevisen ska omfatta befintliga mekanismer för att hjälpa personal att återgå till arbetet efter olyckor och incidenter eller lång frånvaro från arbete som inbegriper hur ytterligare utbildningsbehov identifieras. **(4.2.3)**
- Om sökanden använder ett erkänt utbildningscentrum som är certifierat enligt EU-regler, ger en kopia av det relevanta certifikatet presumtion om överensstämmelse med elementen i ovanstående i den mån de omfattas av certifieringsprocessen. **(4.2.1 a, c–f, 4.2.2)**
- Sökanden ska ange hur den säkerställer att det för samma typ av arbetsuppgift inte finns någon skillnad mellan kompetensen hos den egna personalen och den hos entreprenörer, leverantörer och konsulter som den anlitar. **(4.2.1 a–f)**
- Sökanden ska ange hur kompetensbehov för mänskliga och organisatoriska faktorer bedöms, vilket inbegriper att definiera i vilka roller och i vilka processer kompetens inom mänskliga och organisatoriska faktorer behövs och vilken nivå av kompetens som krävs. Den kapacitet inom

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.

mänskliga faktorer som finns tillgänglig (t.ex. formella kvalifikationer på området, dvs. akademisk examen, internt/externt erkänd kompetens och erfarenhet) är skräddarsydd och står i proportion till företagets mognad och komplexitet. (4.2.1 a–f)

- *Sökande bör tillhandahålla information gällande processen för att godkänna personal att inneha nyckelfunktioner, inklusive den löpande hanteringen av personalens kompetenser.*

4.2.5 Exempel på bevis

Kompetensstyrningssystemet med en förklaring av hur det fungerar över tid, i tillämpliga fall även för personal som inte är i frontlinjen, samt länkar till den dokumentation som stöder det, inklusive de olika utbildningsprogrammen och hur utbildningscentrum tillhandahåller av underleverantörer hanteras.

Avtalsvillkoren (inklusive kravspecifikation) med alla certifierade utbildningscentrum tillsammans med bevis på deras certifiering tillhandahålls.

Exempel på utbildningsprogram för personalgrupper.

Kvalifikationer inklusive psykologiska eller fysiska krav som bedöms vara nödvändiga för vissa säkerhetsrelaterade roller.

Granskningsförfaranden vid olyckor och tillbud i den utsträckning det behandlar åtgärder för att ändra utbildningsprogram mot bakgrund av olyckor och tillbud, tidigare tillsyn etc.

Förfarandet eller processen för att säkerställa att personalen har särskild utbildning och fortutbildning när det gäller

- *förväntade förändringar som påverkar bland annat interna regelverk, infrastruktur och organisationsstruktur, och*
- *uppdateringar av arbetsuppgifterna (t.ex. när det gäller lokförare, nya linjer, nya loktyper, ny typ av tjänst).*

Processen för att säkerställa att följande villkor är uppfyllda:

- *Kompetens upprätthålls genom tillräcklig praxis på fältet (t.ex. när det gäller lokförare, kunskap om driftsförhållanden, kategorier av tåg, dragenheter, linjer och stationer) och/eller genom schemaläggning av specifik utbildning, särskilt efter lång frånvaro från arbetet (på grund av t.ex. sjukdom) eller olycka/tillbud.*
- *Nödvändiga åtgärder vidtas där det finns identifierade avvikelser eller olämpliga beteenden, såsom att en person eller del av utrustning tas ur tjänsten under en period, begränsningar avseende erkända kompetenser om icke-överensstämmelse konstateras, specifik utbildning etc.*
- *Lämpliga åtgärder vidtas för personalen efter olyckor och tillbud (t.ex. för lokförare som passerar en signal, olyckor med personer inblandade etc. Organisationen säkerställer t.ex. att lokföraren är mogen att återuppta tjänsten eller i annat fall ersätts med en person som är behörig att utföra den).*
- *Lärdomar som dras till följd av allvarliga olyckor eller andra betydande händelser delas, särskilt när nya risker upptäcks och måste hanteras på operativ nivå.*
- *Övervakningsprocessen för kompetensstyrningssystemet, inklusive hur dess effektivitet mäts.*

Processen för att säkerställa att lämpliga kompetenser för mänskliga och organisatoriska faktorer är fastställda och att det finns en systematisk metod för att säkerställa att tillräcklig tid och tillräckliga resurser allokeras för mänskliga och organisatoriska faktorer.

Kompetens om säkerhetskultur baseras på en behovsanalys. Kompetensbehov i fråga om säkerhetsbehov bedöms, och strategier för att säkerställa rätt kompetens och resurser demonstreras. Bevis som styrker att grundläggande kunskaper om säkerhetskultur och dess betydelse främjas av ledningen.

4.2.6 Referenser och standarder

- *ISO 10015:1999 Quality Management Guideline for Training*
- *ISO 10018: Quality Management – Guidelines on people and competence.*

4.2.7 Tillsynsfrågor

Hur resultaten från riskbedömning är kopplade till en översyn av kompetensstyrningssystemet.

När man tittar på kompetensstyrningssystem är det viktigt att komma ihåg att det finns kompetenskrav som sträcker sig utöver personalen i organisationen och även har en inverkan på entreprenörer och andra.

Kompetensstyrningssystemet bör kontrolleras för att se hur uppdaterat det är och om den utbildningsverksamhet som ägt rum inom ramen för systemet återspeglar organisationens aktuella behov.

Organisationen bör ha viss möjlighet att säkerställa att kontraktsanställda bedriver verksamhet som de har kompetens att utföra. Detta är en särskild fråga där entreprenörer som enbart tillhandahåller arbetskraft berörs men där kontroller avseende kompetens kanske inte utförs lika noggrant.

Kompetensnivån som krävs för verksamheter som liknar varandra ska vara samma för företagsanställda som kontraktsanställda.

Det finns ett system som säkerställer att uppgifter och befattningar som inbegriper säkerhetselement, inklusive säkerhetskritiska verksamheter, är identifierade.

Det finns ett robust och effektivt kompetensstyrningssystem på plats som inbegriper identifiering av de kunskaper och färdigheter som krävs; utbildning, underhåll och resurser för kompetens; processerna för rekrytering, utbildning, bedömning, kompetensövervakning och dokumentering, där det framgår hur alla dessa element bidrar till att uppnå och upprätthålla kompetens på plats.

När det gäller mänskliga faktorer – hur man gör för att bedöma fysisk och psykisk lämplighet (för exempelvis lokförare och annan personal som utför viktiga säkerhetsuppgifter).

4.3 Medvetenhet

4.3.1 Reglerande krav

4.3.1 Den högsta ledningen ska säkerställa att den själv och den personal som har en roll som påverkar säkerheten är medvetna om relevansen, betydelsen och konsekvenserna av deras verksamhet och hur de bidrar till att säkerhetsstyrningssystemet tillämpas korrekt och ändamålsenligt, inbegripet att säkerhetsmålen uppnås (se 3.2 Säkerhetsmål och planering).

4.3.2 Syfte

Medvetenhet innebär att man ser till att de anställda är medvetna om organisationens säkerhetspolicy och hur de bidrar till säkerheten inom organisationen, och att de har kännedom om relevanta faror och risker samt resultaten av utredningar efter olyckor och tillbud. Begreppet omfattar också att göra personalen medveten om konsekvenserna av att inte bidra till genomförandet av säkerhetsstyrningssystemet, både från deras synvinkel och organisationens. Syftet med detta krav är att åtgärda problem som rör säkerhetskulturen inom organisationen. Det är den högsta ledningen som ska sätta dagordningen och fastställa riktningen för organisationen och hur affärer ska göras. Personal som arbetar inom organisationen inspireras av och följer ledningen. Sökanden måste visa hur dessa frågor hanteras i processer och förfaranden.

4.3.3 Bevis

- Sökanden ska ange var inom ramen för dess mänskliga resurser eller andra processer som den nyckelroll personalen har i att leverera målen för organisationen återspeglas, hur man försöker mäta detta och vilka åtgärder som sätts in för upprätthållande och förbättringar. **(4.3.1) (se också 2.3)**
- Information om kompetensstyrningssystemets funktionssätt. **(4.3.1)**

4.3.4 Exempel på bevis

En förklaring i säkerhetspolicyn eller någon annanstans om engagemanget hos dem som "sätter kursen" för organisationen när det gäller att främja organisationens säkerhetskultur och säkerställa att risker kontrolleras genom ett styrningssystembaserat tillvägagångssätt. I dokumentet ska det även anges hur personalen bidrar till att främja säkerhetspolicyn genom handlingar och efterlevnad av fastställda säkerhetskrav. Länkar finns till de särskilda förfaranden som syftar till att främja dessa idéer i hela organisationen.

Förklaringen innehåller information om hur organisationen framhåller sin säkerhetskultur i förhållande till entreprenörer, partner och leverantörer.

När det gäller själva policyn, kommunikation från ledningen till de anställda om målen, antingen för att uppmuntra dem att bidra till att uppnå dem, eller för att till exempel tacka alla för förbättrade resultat.

Information som visar att mellanchefer och driftspersonal är involverade i säkerhetsinitiativ för frontlinjen (workshoppar, forum, särskilda säkerhetsdagar, utbildningsprogram orienterade mot att utveckla medvetenhet om deras roller i säkerhetsstyrningssystemet etc.).

En beskrivning av kommunikationskanalerna och de kanaler som används.

4.3.5 Tillsynsfrågor

I intervjuer med personalen i denna fråga är det viktigt att fastställa hur folk uppfattar innebörden av de roller och ansvarsområden som gäller för dem. Detta visar om organisationen är kapabel att förstå vikten av

en effektiv organisationskultur eller är medveten om hur säkerhet levereras genom säkerhetsstyrningssystemet.

Vad organisationen grundar sin nuvarande kultur på och vilka steg som finns på plats för att förbättra och utveckla den är viktiga frågor för tillsynen.

Kontrollera övervakningen av tillhandahållandet för ansvarsområden och mål som rör hälsa och säkerhet, riskmedvetenhet, rapporteringskultur – genom att söka efter bortfall, fel, överträdelser och andra oförenligheter.

4.4 Information och kommunikation

4.4.1 Reglerande krav

- 4.4.1 Organisationen ska fastställa lämpliga kommunikationskanaler för att säkerställa att säkerhetsrelaterad information utbyts mellan de olika nivåerna i organisationen och med berörda parter utanför organisationen inklusive entreprenörer, partner och leverantörer.
- 4.4.2 För att säkerställa att säkerhetsrelaterad information når dem som gör bedömningar och fattar beslut ska organisationen hantera identifiering, mottagande, behandling, generering och spridning av säkerhetsrelaterad information.
- 4.4.3 Organisationen ska säkerställa att säkerhetsrelaterad information är
- (a) relevant, fullständig och begriplig för de avsedda användarna,
 - (b) giltig,
 - (c) riktig,
 - (d) konsekvent,
 - (e) kontrollerad (se 4.5.3 Kontroll över dokumenterad information),
 - (f) kommunicerad innan den träder i kraft,
 - (g) mottagen och förstådd.

4.4.2 Syfte

Överensstämmelsen med dessa krav är utformad för att visa att sökanden i sin ansökan i sin tur har visat att lämpliga metoder finns på plats för att identifiera säkerhetsrelaterad information på olika nivåer och kommunicera denna information vid rätt tidpunkt och till rätt personer. Att sökanden övervakar utvecklingen för att säkerställa att befintliga riskkontroller förblir relevanta och uppdaterade och kan identifiera nya hot och möjligheter från externa influenser (politiska, sociala, miljömässiga, tekniska, ekonomiska och juridiska). Att man ser till att nå ut till lämplig personal (särskilt säkerhetskritisk personal) inom organisationen, som behöver reagera. Detta inbegriper hur man tillhandahåller relevant säkerhetsrelaterad information till andra berörda parter som man har operativa förbindelser med.

4.4.3 Förklarande anmärkningar

Organisationen anger vilken typ av säkerhetsrelaterad information som måste förmedlas, hur den kommer att kommuniceras (**se även 4.5**), till vem och på vilka villkor detta kommer att initieras och bearbetas (**4.4.1**). Säkerhetsrelaterad information utbyts mellan anställda som utför uppgifter inom organisationen, med (under)leverantörer, partner eller leverantörer, mellan järnvägsföretag och infrastrukturförvaltare och, i förekommande fall, mellan infrastrukturförvaltare.

Olika typer av information kan urskiljas:

- *Säkerhetsstyrningssystemets dokumentationen (**se även 4.5**).*
- *Statisk information som infrastrukturförvaltaren behöver för att utforma järnvägsverksamheten såsom operativa regler och järnvägsinfrastrukturens egenskaper (t.ex. spårvidd, tåglängd, lutning och axelbelastning).*
- *Information som krävs för att planera järnvägsdrift såsom stationers tågplaner, listor över linjer, tillfälliga hastighetsbegränsningar, ändringar i järnvägsinfrastrukturen, pågående spårarbeten, begränsad spårvidd, tåg som omdirigeras från planerad rutt, att delar av linjen fungerar som enda*

spår, tågföringsprognoser (inklusive eventuella ändringar av tågsträckor och/eller pendlingstrafiktjänster).

- *Information om styrningen av tågtrafiken (mellan järnvägsföretag och infrastrukturförvaltare och, i förekommande fall, mellan infrastrukturförvaltare) inklusive identifiering av kompetent personal inom varje organisation som kan kontaktas vid driftstörningar eller nödsituationer (se även 5.5), under och utanför normal arbetstid.*

Grundläggande krav för utbyte av information **(4.4.2)** anges i TSD drift och trafikledning när det gäller informationsutbyte mellan järnvägsföretaget och infrastrukturförvaltaren, i förordningen för enheter som ansvarar för underhåll när det gäller informationsutbyte mellan järnvägsföretaget och underhållsenheten, i de gemensamma säkerhetsmetoderna för krav på säkerhetsstyrningssystem när det gäller informationsutbyte mellan järnvägsföretaget/infrastrukturförvaltaren och myndigheter (byrån, nationella säkerhetsmyndigheter).

Det finns rutiner på plats för utbytet av information med relevanta parter gällande säkerhetsrisker relaterat till defekter och konstruktionsfel eller fel på tekniska system, inklusive strukturella delsystem. Rutinerna för utbyte av information omfattar även information om korrigerande åtgärder som har vidtagits. Ett exempel på utbyte av sådan information är överenskommelsen om SAIT (Safety Alert IT System) som byrån har förespråkade inom järnvägssektorn. Genom att använda SAIT uppfylls kravet att utbyta sådan information som återfinns i järnvägssäkerhetsdirektivet artikel 4.5 och kravet i de gemensamma säkerhetsmetoderna för övervakning artikel 4, liksom kravet i förordningen för enheter som ansvarar för underhåll artikel 5.5.

”Giltig” har i ovanstående sammanhang **(4.4.3 b)** innebörden ”uppdaterad”.

”Konsekvent” betyder i ovanstående sammanhang **(4.4.3 d)** icke motstridig, om den kommer från olika källor.

”Uppfattad” betyder i ovanstående sammanhang **(4.4.3 g)** att sökanden visar att den har vidtagit åtgärder för att säkerställa att berörda mottagare tagit till sig av säkerhetskritisk information. Detta kan göras med ad hoc-utbildning, genom frågor för att kontrollera förståelse vid genomgångar eller i säkerhetskritisk kommunikation genom antagande av protokoll som kräver att viktiga meddelanden upprepas tillbaka, till exempel mellan tågklarerare och förare för att bekräfta att informationen har absorberats korrekt, eller genom andra medel som uppfyller kravet.

4.4.4 Bevis

- *Sökanden identifierar de olika kommunikationskanaler som finns i organisationen och deras syfte. **(4.4.1)***
- *Sökanden måste tillhandahålla bevis för till exempel alla inre säkerhetsvarningssystem, alla system som förser personalen med relevant men rutinmässig information och alla system som förser personalen med relevant men ad hoc-mässig information. **(4.4.2)***
- *Sökanden anger hur den förvisar sig om att den information som har spridits har nått dem den är avsedd att nå (särskilt de i säkerhetskritiska befattningar) och har uppfattats av dem. **(4.4.3)***

4.4.5 Exempel på bevis

En tydlig förklaring om hur kommunikationen såväl uppåt som nedåt fungerar för olika typer och nivåer av information, med länkar till de specifika förfarandena för säkerhetsvarningar och rutinmässig kommunikation.

I förklaringen anges i vilka steg olika typer av information kommuniceras för att säkerställa att den når avsedd personal och att denna personal förstår vad som kommuniceras, t.ex. säkerhetskritisk information.

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.

Processen eller förfarandet som säkerställer att alla anställda som är inblandade i säkerhetsrelaterade verksamheter förses med rätt version av dokument vid rätt tidpunkt.

Processen eller förfarandet för bekräftelse av tillhandahållande av säkerhetsrelaterade dokument.

Processen/förfarandet för att säkerställa att externa parter, till exempel infrastrukturförvaltare(n), (andra) järnvägsföretag, myndigheter etc. har en kontakt som kan kommunicera med dem (t.ex. har språkkunskaper) och har tillgång till information på rätt nivå.

Kännedom om blankettsamlingen (se TSD drift och trafikledning), som innehåller uppsättningen kommunikationsprotokoll eller kommunikationsmedier för tydligt och snabbt utbyte av formaliserad information (pappersbaserade eller papperslösa enheter såsom inspelningsenheter) som påverkar driften, särskilt tågens rörelser vid driftstörningar.

De säkerhetsvarningar som ska utbytas inom organisationen eller med andra berörda parter. Nedan följer ett par typiska exempel:

- *Järnvägsföretagen informerar infrastrukturförvaltaren om eventuella problem som påverkar tågens rörelser (fel på rullande materiel, t.ex. varmgång, så att infrastrukturförvaltaren kan vidta åtgärder för riskkontroll, t.ex. stoppa trafiken på intilliggande spår).*
- *Infrastrukturförvaltaren ger information om infrastrukturfel och eventuella tillfälliga säkerhetsåtgärder som hastighetsnedsättning till alla järnvägsoperatörer i det berörda området.*

För befattningar som medför ett ansvar för att hantera gränssnitt: bevis på vem säkerhetsvarningen skickas till, beroende på området i drift (detta kan t.ex. ingå i linjeboken).

Process eller förfarande för att sprida information om förändringar i den organisatoriska strukturen för organisationen, både på mikro- och makronivå.

Kopior av de instruktioner som ges till personal i företaget som utför säkerhetsrelaterade uppgifter och hanterar driftsregler som är relevanta för nätet/näten, som måste vara följande:

- *Fullständiga: alla regler och krav som är relevanta för säkerhetsrelaterade uppgifter som i sin tur är relevanta för järnvägsföretagets drift är identifierade och transkriberade i relevanta dokument.*
- *Korrekta: alla regler och krav är korrekt transkriberade utan fel (t.ex. hur man ska bete sig vid en signal, säkerhetsrelaterad kommunikation).*
- *Konsekventa: De krav som gäller enskilda personer eller enskilda team från olika ställen är kompatibla och konsekventa och strider inte mot varandra.*

4.4.6 Tillsynsfrågor

Kontrollera att det finns tekniker och processer som används för att hålla riskkontrollen uppdaterad, övervaka utvecklingen för att upptäcka möjligheter eller hot.

Kontrollera att det finns en process för att övervaka användningen av formaliserad information.

I tillsynen är nyckelfrågorna hur aktuell informationen är och om den når fram till **all** relevant personal, t.ex. den som arbetar nattsift eller som arbetar långt från organisationens huvudsakliga baser, i god tid.

4.5 Dokumenterad information

4.5.1 Reglerande krav

4.5.1 Dokumentation av säkerhetsstyrningssystem

4.5.1.1 Det ska finnas en beskrivning av säkerhetsstyrningssystemet som ska omfatta

- (a) identifiering och beskrivning av processer och aktiviteter som rör järnvägsdriftens säkerhet, inbegripet säkerhetsrelaterade arbetsuppgifter och ansvar kopplat till dessa (se 2.3 Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen),
- (b) samspel mellan dessa processer,
- (c) förfaranden eller andra dokument som beskriver hur dessa processer genomförs,
- (d) identifiering av entreprenörer, partner och leverantörer med en beskrivning av vilken typ av tjänster som levereras och tjänsternas omfattning,
- (e) identifiering av avtalsmässiga arrangemang och andra affärsavtal som ingåtts mellan organisationen och andra parter enligt punkt d, och som är nödvändiga för att ha kontroll över organisationens säkerhetsrisker och säkerhetsrisker i samband med anlitandet av entreprenörer,
- (f) hänvisningar till den dokumenterade information som krävs enligt denna förordning.

4.5.1.2 Organisationen ska säkerställa att en årlig säkerhetsrapport lämnas in till den berörda nationella säkerhetsmyndigheten (eller de berörda myndigheterna) i enlighet med artikel 9.6 i direktiv (EU) 2016/798, och den ska omfatta

- (a) en sammanfattning av besluten rörande de säkerhetsrelaterade ändringarnas grad av betydelse, inklusive en översikt över väsentliga ändringar, i enlighet med artikel 18.1 förordning (EU) nr 402/2013,
- (b) organisationens säkerhetsmål för de följande åren och hur allvarliga säkerhetsrisker påverkar fastställandet av dessa mål,
- (c) resultaten av interna utredningar av olyckor/tillbud (se 7.1 Lärdomar av olyckor och tillbud) och andra övervakningsaktiviteter (se 6.1 Övervakning, 6.2 Internrevision och 6.3. Ledningens genomgång), i enlighet med artikel 5.1 i förordning (EU) nr 1078/2012 (1),
- (d) uppgifter om framsteg när det gäller att hantera ännu ej åtgärdade rekommendationer från nationella utredningsorgan (se 7.1 Lärdomar av olyckor och tillbud),
- (e) organisationens säkerhetsindikatorer som fastställts för att utvärdera organisationens säkerhetsnivå (se 6.1 Övervakning),
- (f) i tillämpliga fall, slutsatserna i säkerhetsrådgivarens årsrapport, enligt vad som avses i RID (2), om organisationens verksamhet vad gäller transport av farligt gods (3).

4.5.2 Utformning och uppdatering

4.5.2.1 Organisationen ska säkerställa att den använder lämpliga format och medier när den utformar och uppdaterar dokumenterad information avseende säkerhetsstyrningssystemet.

4.5.3 Kontroll över dokumenterad information

4.5.3.1 Organisationen ska utöva kontroll över dokumenterad information avseende säkerhetsstyrningssystemet, i synnerhet lagring, distribution och hantering av ändringar, i syfte att säkerställa informationens tillgänglighet, lämplighet och skydd i tillämpliga fall.

4.5.2 Syfte

Sökanden ska visa att det övergripande säkerhetsstyrningssystemet är lämpligt för den typ och omfattning av tjänster som utförs och att det kan hantera de risker som genereras. För detta krävs

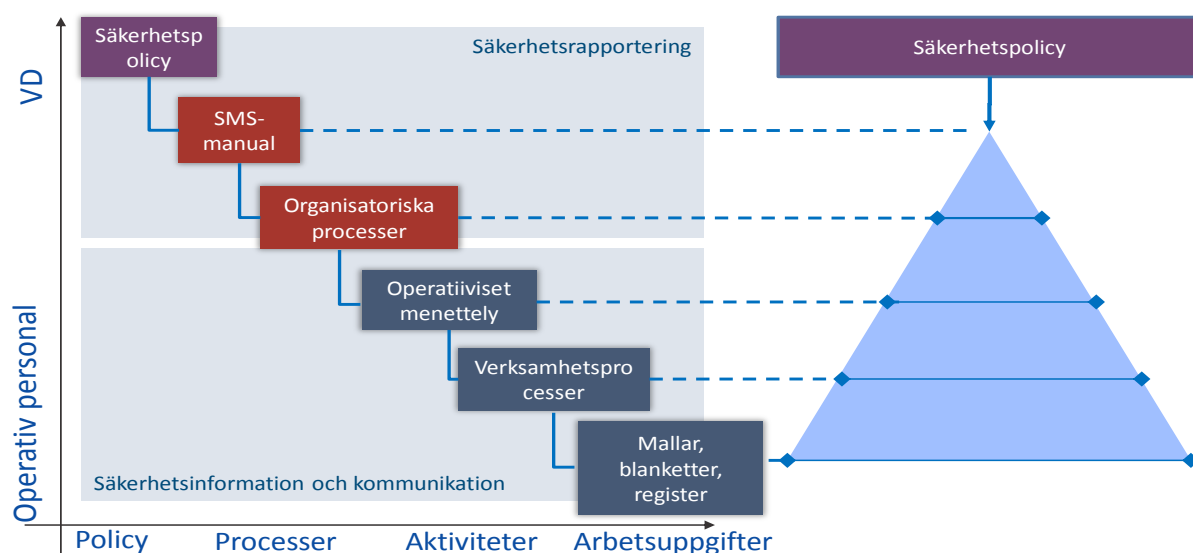
- en förklaring av sökandens säkerhetspolicy, organisation och övergripande strukturför säkerhetsstyrningssystemet, och
- de mer detaljerade arrangemangen som anges i kraven ovan i punkterna 4.5.1.1 a–f och 4.5.1.2 a–g.

Sökanden ska också visa hur dess dokumentation om säkerhetsstyrningssystemet hanteras, dvs. hur identifiering, skapande, underhåll, hantering, förvaring och lagring av dokumenterad information (dokument och register/data) sker för att säkerställa att den är uppdaterad och att korrekta versioner finns tillgängliga för relevant personal när det behövs.

4.5.3 Förklarande anmärkningar

Alla dokument där sökanden visar att dess säkerhetsstyrningssystem uppfyller tillämpliga krav **(4.5.1.1 f)** ingår i den dokumenterade informationen om säkerhetsstyrningssystemet.

Bilden nedan visar en typisk dokumentationsstruktur:



Figur 3: Typisk dokumentationsstruktur

Beroende på vilket driftområde det rör sig om kan järnvägsföretagen lämna olika rapporter **(4.5.1.2)** till de nationella säkerhetsmyndigheterna i de medlemsstater där de bedriver verksamhet. En rapport omfattar i allmänhet endast den del av verksamheten som bedrivs i medlemsstaten i fråga. Järnvägsbyrån rekommenderar emellertid att en och samma rapport täcker hela driftområdet, för att underlätta utbytet av information mellan nationella säkerhetsmyndigheter som övervakar samma järnvägsföretag.

Säkerhetsrådgivarens årsrapport **(4.5.1.2 f)**, när det gäller transport av farligt gods, i enlighet med föreskrifterna i direktiv 2008/68/EG i dess ändrade lydelse och bestämmelserna om internationella järnvägstransporter av farligt gods (RID). Årsrapporten från säkerhetsrådgivaren för farligt gods är också underlag för den årliga säkerhetsrapporten. Säkerhetsrådgivaren måste uppfylla angivna funktioner inklusive ge rådgivning till det företag som utsåg honom eller henne i frågor som rör hälsa, säkerhet och miljö i samband med transport av farligt gods och utarbetandet av nödvändiga rapporter.

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.

Identifiering, format (t.ex. språk, programvaruversion och grafik) och val av medier (t.ex. pappersbaserade, elektroniska) för dokumenterad information **(4.5.2.1)** överläts till organisationen. Det behöver inte vara en skriftlig pappersmanual.

Dokumentkontrollen **(4.5.3.1)** anger processen (eller förfarande) för interna kontroller, i synnerhet granskningen och godkännandet av lämplighet före utfärdande och användning, som ska beaktas och tillämpas för den information som måste dokumenteras. Den syftar till att identifiera den aktuella revideringsstatusen för dokument för att förhindra att ogiltiga eller föråldrade dokument används. Det säkerställer framför allt att

- *relevanta versioner av lämpliga dokument finns tillgängliga på varje plats där sådan verksamhet bedrivs som är av betydelse för att säkerhetsstyrningssystemet ska fungera på ett effektivt sätt,*
- *ogiltiga eller inaktuella dokument omedelbart avlägsnas överallt där de har upprättats eller använts, eller att man på annat sätt skyddar sig mot att inaktuella dokument kommer till användning,*
- *alla inaktuella dokument som arkiveras av legala eller i kunskapsbevarande syften är identifierade på lämpligt sätt.*

4.5.4 Bevis

- *Sökanden bör tillhandahålla en beskrivning av säkerhetsstyrningssystemet och hur det fungerar med lämpliga angivelser till relevanta förfaranden vid behov. **(4.5.1.1 a–c)***
- *Sökanden bör identifiera roller och ansvarsområden som gäller i förhållande till säkerhetsrelaterade uppgifter och hur riskerna från sökandens och andras verksamheter hanteras. **(4.5.1.1 a)***
- *Sökanden ska tillhandahålla bevis för att man har (eller har arrangemang för att producera) en årlig säkerhetsrapport som omfattar de poster som anges i 4.5.1.2 ovan. **(4.5.1.2 a–f)***
- *Sökanden ska ange hur dokumenthanteringssystemet fungerar samt hur information görs tillgänglig och är lämplig för användning där och när den behövs, hur den ändras på ett kontrollerat sätt inom systemet och hur den förvaras och underhålls på ett sätt som gör den lättåtkomlig. Dokumenthanteringssystemet bör möjliggöra att information förvaras på ställen där miljön är lämplig för att minimera försämring eller skador och förhindra förlust. **(4.5.2.1), (4.5.3.1)***

4.5.5 Exempel på bevis

En beskrivning av säkerhetsstyrningssystemet, dess övergripande struktur och länkar till de dokument som stöder processerna däri (t.ex. manuella, organisatoriska och operativa förfaranden, arbetsinstruktioner). Utan att det påverkar det nya begreppet dokumenterad information, som införts genom ISO, kan organisationen bevara den traditionella dokumentationsstrukturen om den är lämplig för ändamålet.

En översikt över hur de olika dokumenten är strukturerade, publicerade, tillgängliga, arkiverade, underhållna/ändrade och upphävida med hänvisning till relevanta kontrollförfaranden.

Förfarandet för att utarbeta årsrapporten, om ansökan avser ett första gemensamt säkerhetsintyg. I förfarandet anges den föreslagna layouten för rapporten.

Processen eller förfarandet för dokumenthantering som måste ange hur dokument uppdateras efter regelbundna översyner och efter olyckor eller tillbud. Processen eller förfarandet hanterar eskaleringsprocessen i fall där överenskomna uppdateringar inte har ägt rum inom den föreskrivna tidsramen eller där det inte finns någon överenskommelse om hur man uppdaterar dokumentet.

Ett kontrollerat språk (dvs. med korta, enkla meningar, och som undviker jargong) används för att främja gemensam förståelse och bra datakvalitet.

Personal med behörighet att godkänna dokument för utfärdande säkerställer att innehållet är korrekt och kan förstås av alla slutanvändare (eller mottagare) för vilka de gäller.

Där det är praktiskt möjligt identifieras förändringarnas karaktär i dokumentet eller i lämpliga bilagor, för att underlätta granskning och godkännande av dem.

Lagringstider för dokument och register är upprättade, dokumenteras och efterlevs.

4.5.6 Referenser och standarder

- Vägledning gällande kraven på dokumenterad information i ISO 9001:2015, ISO/TC 176/SC2/N1286, finns tillgänglig på: www.iso.org/tc176/sc02/public

4.5.7 Tillsynsfrågor

Kontrollera avtalsvillkoren för effektiv tillsyn och kontroll av risker genom organisationen (dvs. när tjänster läggs ut på entreprenad).

Av avgörande betydelse när tillsyn utförs är att fastställa hur förhållandet mellan dem som har kontroll över dokumenthanteringssystemet och dem som ansvarar för att uppdatera information och upprätthålla kontakt med de förstnämnda ser ut i praktiken. Det är på denna nivå en uppdelad kontroll av dokumentationen ofta kan uppstå, eftersom de två delarna av processen sannolikt finns i två olika styrningskedjor. Detta kan till exempel leda till att man har olika uppfattning om hur viktigt arbetet med att uppdatera dokumentationen är, vilket kan leda till tidsfördröjningar med att utveckla och uppdatera dokumentation och åtföljande risker.

Personalens möjlighet att få tillgång till aktuell information och dokumentation.

Säkerhetsstyrningssystemets struktur och funktionssätt bör återspegla hur arbetet bedrivs i praktiken och inte vara ett konstgjort lager som ligger utanför vanor och praxis.

4.6 Integrering av mänskliga och organisatoriska faktorer

4.6.1 Reglerande krav

- 4.6.1 Organisationen ska kunna uppvisa ett systematiskt tillvägagångssätt för att integrera mänskliga och organisatoriska faktorer inom säkerhetsstyrningssystemet. Tillvägagångssättet ska:
- (a) innefatta utarbetande av en strategi och användning av sakkunskap och erkända metoder från området mänskliga och organisatoriska faktorer,
 - (b) behandla risker kopplade till utformning och användning av utrustning, arbetsuppgifter, arbetsvillkor och organisatoriska arrangemang, med beaktande av mänsklig förmåga såväl som mänskliga begränsningar, och inflytandet på mänsklig prestation.

4.6.2 Syfte

Sökanden visar att användningen av en systematisk strategi baserad på mänskliga och organisatoriska faktorer är en integrerad del av säkerhetsstyrningssystemet. Att uppfylla dessa element är viktigt för sökanden för att demonstrera att den är behörig att bedriva järnvägsverksamhet och har riskkontrollsystem inbäddade i sitt säkerhetsstyrningssystem för att hantera de risker verksamheten innebär.

4.6.3 Förklarande anmärkningar

Mänskliga och organisatoriska faktorer innebär att man intar ett systemperspektiv där samspelet mellan mänskliga, tekniska och organisatoriska faktorer beaktas. Organisationen bör ta hänsyn till mänskliga och organisatoriska faktorer genom ett livscykelinriktat synsätt. Detta innebär att identifiera och ta itu med mänskliga och organisatoriska faktorer i säkerhetsstyrningsaktiviteter som är relaterade till affärsmål, ledning, verksamheter, mänskliga prestationer, utformning av uppgifter och arbetsplatser i alla skeden av systemets livscykel, t.ex. från idrifttagning till avveckling. En strategi för mänskliga och organisatoriska faktorer anger en systematisk metod för att integrera mänskliga och organisatoriska faktorer i säkerhetsstyrningsaktiviteter.

Organisationen bör engagera den relevanta expertis inom mänskliga och organisatoriska faktorer som den behöver till stöd för sin verksamhet. Med expertis inom mänskliga och organisatoriska faktorer avses att involverad personal bör vara kvalificerad utifrån en nationell och/eller internationell standard på området. Till exempel genom att uppfylla medlemskraven för registreringscentrumet för europeiska ergonomer (*Centre for Registration of European ergonomists*) eller liknande organ. Stora organisationer kan ha en avdelning för mänskliga faktorer med experter på området som stöder organisationen. Mindre organisationer kan ge chefer på alla nivåer ansvaret att när så är nödvändigt identifiera behovet av expertis inom mänskliga faktorer.

Mer information gällande en strategi för mänskliga och organisatoriska faktorer finns i bilaga 5.

4.6.4 Bevis

- Sökanden anger i en strategi detaljerna för hur mänskliga och organisatoriska faktorer är integrerade så att riskerna med samspelet mellan mänskligt beteende, organisatoriska förhållanden och teknik beaktas ordentligt inom de relevanta processerna i säkerhetsstyrningssystemet. Detta kan till exempel innebära att man har en plan för hur mänskliga och organisatoriska faktorer hanteras för ett nytt signalsystem i alla livscykelstadier. Sökanden bör här göra klart var närmare detaljer om relevanta förfaranden kan hittas. **(4.6.1)**

- *Det finns en proces för utformande som appliceras baserad på mänskliga och organisatoriska principer och metoder, där användaren sätts i centrum och involveras i processen. Processen tar till exempel hänsyn till ny eller modifierad design, förfaranden, utbildning, arbetsbörda och arbetsmiljö för att säkerställa ett systems livslånga säkerhet och effektivitet.*
- *Tillgängliga standarder och bästa praxis för mänskliga och organisatoriska faktorer används. Relevanta standarder är till exempel ISO-serien 11064 om ergonomisk utformning av kontrollcentraler och ISO-serien 9241 om ergonomi för interaktioner människa–system.*
- *Slutanvändare är involverade i designprocessen, till exempel i kravspecifikationen, påföljande utveckling och testprocess.*
- *En designprocess som sätter användaren i centrum är en iterativ process som innefattar flera faser. Analyser görs för att förstå och specificera kontexten där användningen sker (till exempel bemanning och kompetensanalys, analys av arbetsuppgifter och riskanalys). Användarkrav definieras baserat på dessa analyser. Designlösningar, inklusive design av gränssnitt, arbetsplatser, utbildning, förfaranden och organisation, möter användarkraven. Utvärdering av de här designerna genomförs med formella metoder, som till exempel uppgiftsanalys, simulering, riskbedömning, expertutvärderingar, användarutvärderingar, verifiering och validering.*

4.6.5 Exempel på bevis

En kopia av strategin för mänskliga och organisatoriska faktorer som visar hur användningen av expertis och tekniker inom mänskliga och organisatoriska faktorer beaktas.

Organisationen utför en analys, med evidensbaserade metoder, av de operativa processerna och stödprocesserna i livscykelns alla stadier, från utformande till avyttring. Analysen bör identifiera alla mänskliga och organisatoriska faktorer och de prestationspåverkande faktorer som kan inverka på järnvägssäkerheten, och de säkerhetsstyrningsverksamheter som behövs för att kontrollera riskerna.

Strategin för mänskliga och organisatoriska faktorer bör visa de säkerhetsstyrningsverksamheter som finns på plats, liksom att det finns en metod för att övervaka och förbättra effektiviteten i strategin. Strategin bör utgå från ett proaktivt tillvägagångssätt men bör inbegripa de reaktiva insatser som behövs.

Säkerhetsstyrningsaktiviteter bör identifieras som är relaterade till stödfunktioner och stödsystem, uppgiftsutformning, bemanningsnivåer, utbildning, utformning och användning av utrustning, förfaranden och kommunikationsprotokoll.

Exempelvis kan en sådan strategi inkludera hur mänskliga och organisatoriska faktorer integreras i processen för förändringshantering. Med integrering av mänskliga faktorer avses processen för att integrera mänskliga faktorer och ergonomi i systemets tekniska process. Integrationsplanen för mänskliga faktorer ger en systematisk metod för att definiera förhållandet mellan alla projektets verksamheter och området mänskliga faktorer. Ingenjörsvetenskap om mänskliga faktorer handlar om integrering av mänskliga egenskaper i systemdefinition, utformning, utveckling och utvärdering för att optimera människa–maskin-resultaten under driftsförhållanden.

Om de operativa processerna innebär komplexa arbetsmönster bör strategin för mänskliga och organisatoriska faktorer omfatta ett riskhanteringsprogram avseende utmattning.

4.6.6 Referenser och standarder

- Wickens, C.D., Lee, J.D., Liu, Y & Gordon Becker, S.E (2004). *An Introduction to Human Factors Engineering*. New Jersey: Pearson Education. ISBN-13: 978-0131837362
- ISO-standardserier, t.ex.
- ISO-serien 6385:2004 om ergonomiska principer vid utformning av arbetssystem
- ISO-serien 11064 om ergonomisk utformning av kontrollcentraler
- ISO-serien 9241 om ergonomi för interaktioner människa–system
- ISO-serien 10075 om ergonomiska principer relaterade till mental arbetsbörda
- EEMUA 191. *Alarm systems, a guide to design, management and procurement*
- UIC 651 *Layout of drivers' cabs in locomotives, railcars, multiple unit trains and driving trailers*
- Rail Safety & Standards Board (2008). *Understanding Human Factors, a guide for the railway industry*

4.6.7 Tillsynsfrågor

Kontrollera att frågor som rör mänskliga faktorer beaktas i beslutsfattandeprocesser för hantering av risker genom riskbedömning, förändringshantering och hantering av operativa tillgångar.

Kontrollera att operativa dokument återspeglar åtagandet att hantera mänskliga faktorer genom ergonomisk utformning (t.ex. användarvänlig design, enkelt språk, grafik för att stödja instruktioner, enkel hantering av uppdateringar), till stöd för hanteringen av risker.

Kontrollera att järnvägsföretaget/infrastrukturförvaltaren vid övervakning av resultaten fokuserar sin analys på mänskliga faktorer som primär eller underliggande orsak till olyckor, incidenter eller farliga händelser.

Kontrollera om det finns dokumenterade exempel på att korrigerande åtgärder har vidtagits, utformade för att ta bort faktorer som påverkar de mänskliga prestationerna och försämrar säkerheten.

5 Verksamhet

5.1 Operativ planering och styrning

5.1.1 Reglerande krav

- 5.1.1 Vid planering, utveckling, implementering och översyn av sina operativa processer ska organisationen säkerställa att följande sker under dess verksamhet:
- (a) Kriterier för en acceptabel risknivå och säkerhetsåtgärder tillämpas (se 3.1.1 Riskbedömning).
 - (b) Plan(er) för att uppnå säkerhetsmålen tillhandahålls (se 3.2 Säkerhetsmål och planering).
 - (c) Information samlas in för att mäta att operativa planer och rutiner tillämpas korrekt och är ändamålsenliga (se 6.1 Övervakning).
- 5.1.2 Organisationens ska säkerställa att dess operativa planer och rutiner uppfyller de säkerhetsrelaterade kraven i tillämpliga tekniska specifikationer för driftskompatibilitet samt relevanta nationella regler och alla andra relevanta krav (se 1 Organisationens förutsättningar).
- 5.1.3 För att hålla risker under kontroll, när detta är relevant för säkerheten i de aktiviteter som ingår i verksamheten (se 3.1.1 Riskbedömning), ska hänsyn tas till minst följande:
- (a) Planeringen av befintliga eller nya järnvägssträckor och ny tågtrafik, inklusive införande av nya fordonstyper, behovet att hyra in fordon och/eller att anlita personal från parter utanför organisationen och utbytet av information med underhållsansvarig enhet om underhållet i operativt syfte.
 - (a) Identifiering av säkerhetsgränserna för transporter i trafikplanerings- och kontrollsyste baserat på infrastrukturens utformning.
 - (b) Utarbetande och införande av tågplaner.
 - (b) Trafikplanering, inklusive tågplan och tilldelning av tåglägen.
 - (c) Förberedelse av tåg eller fordon före förflyttning, inklusive kontroller före avgång och tågsammansättning
 - (c) Trafikledning i realtid vid normala förhållanden och vid försämrade förhållanden med tillämpning av trafikrelaterade begränsningar för användning och hantering av trafikavbrott.
 - (d) Tågdrift eller fordonsförflyttning under de olika driftsförhållandena (normala, vid störning och i nödsituationer).
 - (d) Fastställande av villkor för specialtransporter.
 - (e) Anpassning av driften när underhållsansvarig enhet begär att fordon ska tas ur drift och anmäler att fordon kan återtas i drift.
 - (f) Tillstånd till förflyttning av fordon.
 - (g) Användbarhet hos gränssnitt i tågens förarhytter och i trafikledningscentraler, samt utrustning som används av underhållspersonal.
- e), f) och g) gäller ej för infrastrukturförvaltare.
- 5.1.4 För att kontrollera ansvarsfördelningen, när detta är relevant för en säker operativ verksamhet, ska organisationen ange ansvarsområden för samordning, hantering och styrning av en säker tågdrift och förflyttning av fordon samt fastställa hur de arbetsuppgifter som har betydelse för att

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.

alla tjänster tillhandahålls på ett säkert sätt fördelas till kompetent personal inom organisationen (se 2.3 Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen) och till andra parter med rätt kvalifikationer utanför organisationen (se 5.3 Entreprenörer, partner och leverantörer).

5.1.4 För att kontrollera ansvarsfördelningen, när detta är relevant för en säker operativ verksamhet, ska organisationen identifiera ansvaret för planering och drift av järnvägsnätet samt fastställa hur de arbetsuppgifter som har betydelse för säkerheten endast tilldelas kompetent personal inom organisationen (se 2.3 Roller, ansvar, ansvarsskyldighet och befogenheter inom organisationen) och till andra parter med rätt kvalifikationer utanför organisationen (se 5.3 Entreprenörer, partner och leverantörer).

5.1.5 För att utöva kontroll över information och kommunikation, när detta är relevant för en säker operativ verksamhet (se 4.4 Information och kommunikation), ska berörd personal (t.ex. tågpersonal) meddelas detaljerade uppgifter om alla specificerade körförhållanden, inbegripet relevanta ändringar som kan leda till fara, tillfälliga eller permanenta driftsrestriktioner (t.ex. på grund av särskilda fordonstyper eller särskilda sträckor) och villkor för specialtransporter, i tillämpliga fall.

5.1.5 För att utöva kontroll över information och kommunikation, när detta är relevant för en säker operativ verksamhet (se 4.4 Information och kommunikation), ska berörd personal (t.ex. trafikledningspersonal) informeras om krav på särskilda transportvägar för tåg och förflyttning av fordon inklusive relevanta ändringar som kan leda till fara, tillfälliga eller permanenta driftsrestriktioner (t.ex. på grund av spårunderhåll) och villkor för specialtransporter.

5.1.6 För att utöva kontroll över kompetens, när detta är relevant för en säker operativ verksamhet, (se 4.2 Kompetens), ska organisationen, i enlighet med tillämplig lagstiftning, säkerställa (se 1. Organisationens förutsättningar) följande för sin personal:

- (a) Att utbildnings- och arbetsinstruktioner följs, och att korrigerande åtgärder vidtas vid behov.
- (b) Att särskild utbildning anordnas när det förväntas komma förändringar som påverkar driften eller personalens arbetsuppgifter.
- (c) Att det antas lämpliga åtgärder efter olyckor och tillbud.

5.1.2 Syfte

Sökanden ska visa att man har relevanta processer på plats för att hantera operativa risker genom säkerhetsstyrningssystemet, vilket inbegriper att se till att de anställda förstår sina roller, de operativa risker de ställs inför och vilka kontrollåtgärderna är, samt att de har lämplig kompetens och utbildning för att hantera dessa i enlighet med dokumentationen i säkerhetsstyrningssystemet.

Sökanden ska säkerställa att fordonen eller infrastrukturen drivs på ett säkert sätt i enlighet med de tillämpliga kraven under olika driftsförhållanden (normala, försämrade och akuta), vilket också inbegriper användningen av tillgångar för teständamål (t.ex. provning av fordons körbeteenden innan tillstånd beviljats) och vid exceptionella omständigheter (t.ex. exceptionella leveranser såsom transport av kärnämne eller stora odelbara bitar som inte kan transporteras med andra transportmedel, som betongbalkar/bågar för broar etc.).

5.1.3 Förklarande anmärkningar

I direktiv (EU) 2016/798 föreskrivs att järnvägsföretag och infrastrukturförvaltare ska införa ett säkerhetsstyrningssystem för att hantera säkerhetsriskerna i deras järnvägsverksamheter. Den allmänna uppfattningen när det gäller säkerhetsstyrning är att säkerhet bör integreras i normala verksamhetsprocesser så mycket som möjligt. Anledningen till detta är att företaget då fokuserar lika mycket på säkerhet som på alla andra processer, vilket minskar konflikterna mellan olika processer.

ISO förklarar i stödbilagan SL till sitt vägledande dokument (N360) att avsikten med paragraf 8 (drift) är att ange de element som måste genomföras inom organisationens verksamhet för att säkerställa att kraven på styrningssystemen är uppfyllda, samt att se till att prioriterade risker och möjligheter hanteras. Dessutom anges det att ytterligare krav (disciplinspecifika) relaterade till operativ planering och styrning kan föreskrivas, särskilt att de inte är skadliga för företagets affärsverksamhet men ger en tillräcklig ram för att kontrollera hur viktiga säkerhetsfrågor hanteras inom organisationens affärsprocesser.

Explicita länkar har lagts till mellan operativa krav och andra styrningssystemkrav (vilket liknar förhållningssättet i bilaga III till förordningen för enheter som ansvarar för underhåll) för att tydliggöra att särskilda operativa krav ska beaktas i förhållande till de relevanta styrningssystemkraven (för järnvägsföretag är t.ex. planering av rutten en verksamhet som bör vara föremål för riskbedömning). Detta tillvägagångssätt är inte avsett att vara uttömmande utan syftar till att identifiera särskilda frågor som myndigheterna anser är betydande (baserat på deras erfarenhet) och som därför bör undersökas vid deras bedömning eller tillsynsverksamhet. Järnvägsföretag och infrastrukturförvaltare bör inte bara fokusera på dessa specifika krav när de utvecklar och implementerar sina säkerhetsstyrningssystem (och till exempel bortse från andra säkerhetsrisker). Under alla omständigheter måste järnvägsföretag och infrastrukturförvaltare tillämpa säkerhetsstyrningssystemkrav (gällande t.ex. riskbedömning, övervakning, kompetens, information och kommunikation) för alla sina relevanta verksamhetsprocesser för att visa att alla säkerhetsrisker kontrolleras på ett tillfredsställande sätt.

Integreringen av säkerhetsstyrningssystemet i verksamhetsprocesserna/de operativa processerna är av avgörande betydelse, och för att uppnå detta mål måste organisationen efterleva tillämpliga TSD:er (**5.1.2**), såsom TSD drift och trafikledning, och anmälda nationella regler när gränssnittskraven inte omfattas fullt ut av TSD:erna. Godtagbara sätt att uppfylla kraven på kan också offentliggöras av medlemsstaten eller dess myndighet, för att underlätta efterlevnaden av de nationella reglerna. Som ett minimum bör följande operativa processer beaktas i de fall det är relevant:

- *Infrastruktur i drift (kontrollera infrastrukturens linjer och utrustning, godkänna fordonsrörelser vid alla förhållanden och säkerställa underhåll: spår och trafikstyrning samt signalsystem).*
- *Tåg i drift (utveckling av rutten och relevanta tidtabeller, hantering av iordningställande av tåg, säkerställande av tågfärd, medföljande, testning, underhåll och reparation av vagnar).*
- *Växlingstjänster (flytt av vagnar för att koppla ihop eller koppla isär ett tåg).*

TSD drift och trafikledning är nyckeln här eftersom det är där de grundläggande driftsprinciperna fastställs, vilka bör återspeglas i de relevanta delarna av säkerhetsstyrningssystemet. Överensstämmelse med TSD drift och trafikledning kan därför användas för att visa att ovannämnda säkerhetsstyrningssystemkrav uppfylls.

Utbytet av information om underhåll av fordon för operativa ändamål (**5.1.3 a**) med enheter som ansvarar för underhåll definieras i artikel 5.3 i förordningen för enheter som ansvarar för underhåll. Den omfattar underhållsplaner och driftsbegränsningar utfärdade av enheter som ansvarar för underhåll under underhållsarbetet (planering på kort sikt).

Där hänvisning görs till utvecklingen och implementering av tidtabeller (**5.1.3 b**), innebär detta att sökanden bör visa hur man genom riskbedömning har hanterat riskerna med verksamheten inom sin

organisation och vid gränssnitten för operativa förbindelser med andra aktörer. De har till exempel tagit hänsyn till följande:

- *Trafikledningspersonalens utökade arbetsbörda när antalet tåg vid vissa tidpunkter ökar.*
- *De lämpliga operativa avtalen med relevant(a) infrastrukturförvaltare för att stoppa trafik, återställande, utbyte av information och alla andra tjänster som anses nödvändiga.*
- *Hantering av de risker som är kopplade till spårunderhåll när tågen körs 24 timmar om dygnet.*

Ny tågtrafik **(5.1.3 b)** kan inbegripa transport av nya typer av varor.

Fordonsrörelser **(5.1.3 d)** har en bredare betydelse än tågrörelser (dvs. planerad förflyttning av fordon) och tillstånd som utfärdats före tågavgång. Begreppet kan också omfatta bärgning av trasiga tåg, underhållsfordons rörelser eller oplanerade utbyten av skadade vagnar i ett tåg före tågets avgång.

I enlighet med UIC-normblad 502-1, artikel 1.1, föreslås följande definition av begreppet "exceptionella leveranser" **(5.1.5)**: *"En leverans anses vara exceptionell om dess mått, dess vikt eller dess egenskaper i förhållande till den fasta utrustningen eller vagnen som innehas av ett järnvägsföretag som är involverat i transporten orsakar särskilda svårigheter, och därför endast kan godtas under särskilda tekniska eller operativa förutsättningar."*

Infrastrukturförvaltaren ska identifiera och tillhandahålla villkor och åtgärder för att använda ett fordon för prov på nätet inom en given tidsram i enlighet med i artikel 21.3 och 21.5 i direktiv (EU) 2016/797 **(5.1.2)**.

Uppgifter om kontroller av ruttkompabiliteten som inkluderar att egenskaperna hos fordonet/tåget överensstämmer med den sträcka som tåget avses trafikera, inklusive avvikande färdväg som identifierats av infrastrukturförvaltaren (TSD Drift och trafikledning (EU) 2015/995 4.2.2.5).

Rutters egenskaper baserat på infrastrukturförvaltarens register (RINF) och/eller informationen som tagits fram av infrastrukturförvaltaren.

I de fall problem identifieras ska dessa lösas gemensamt av järnvägsföretaget och infrastrukturförvaltaren.

Mänskliga och organisatoriska faktorer ska beaktas vid operativ planering i fråga om exempelvis arbetsscheman, hantering av utmattning, stress, arbetsmiljö (fysisk och psykosocial), arbetsplatser och arbetsprocesser etc.

Planering och kontroll av driften har utvecklats för kontinuerlig förbättring av säkerhetskulturen. Säkerhetskulturen ska beaktas i samband med exempelvis arbetsbelastning, arbetsmiljö (fysisk och psykosocial), processer etc. Detta syftar till att säkerställa att konsekvenserna av förändringar eller åtgärder inte har en negativ inverkan på de mänskliga prestationerna eller den organisatoriska säkerheten.

5.1.4 Bevis

- *Information som anger att man vid planering, utveckling, implementering och uppföljning av operativa processer avser att uppnå säkerhetsmålen, utför riskbedömning, mäter och övervakar resultaten, inklusive lämpliga angivelser till var ytterligare information om förfaranden kan hittas. **(5.1.1 a–c)***
- *Bevis på att organisationen är medveten om och faktiskt implementerar alla kategorier av obligatoriska säkerhetskrav som gäller för dess verksamhet och beskriver hur säkerhetsstyrningssystemet överensstämmer med dem.*
- *Information om att sökanden ser till att dess operativa arrangemang är kompatibla med tillämpliga krav (lagstiftning, standarder etc.). **(5.1.2)***

- *Inom ramen för fordonets typgodkännande och/eller fordonets tillstånd för utsläppande på marknaden, kan infrastrukturförvaltaren identifiera och tillhandahålla **(5.1.2)***
 - *de operativa villkor som ska tillämpas vid användningen av fordonet för prover på nätet, baserat på den information som sökanden tillhandahållit för godkännandet,*
 - *alla nödvändiga åtgärder som måste vidtas på infrastruktursidan för att säkerställa en säker och pålitlig drift under testerna på nätet, och/eller*
 - *alla åtgärder i infrastrukturinstallationerna som är nödvändiga för att utföra prover på nätet.*
- *Kontroller före användande av ett godkänt fordon (omarbetat Interoperabilitetsdirektiv (IOD) artikel 23.1) och särskilt ruttkompabiliteten (IOD artikel 23.1 (a), (b) att järnvägsföretagets SMS har förmågan att identifiera och ta fram bevis (5.1.3 (a)) CSM Krav på säkerhetsstyrningssystem) på att fordonet är kompatibelt med rutten som det är avsett att trafikera och att det är på rätt sätt integrerat i tågets sammansättning (se också TSD Drift och trafikledning (2015/995 4.2.2.5)).*
- *Bevis på att driftdokumentation överensstämmer med kraven för att hantera drift (och underhåll) vid organisatoriska och fysiska gränser, t.ex. organisatoriska, tekniska och operativa gränssnitt med angränsande infrastruktur, gränsstationer, interaktioner med andra järnvägsföretag eller infrastrukturförvaltare etc. **(5.1.2)***
- *Information om hur riskerna med driftverksamhet hanteras genom riskbedömningsprocessen. De element som anges i kraven ovan omfattas. **(5.1.3 a, c-f)***
- *Bevis på att artikel 14.2 i direktiv (EU) 2016/798 efterlevs av enheten som ansvarar för underhåll. **(5.1.3 f)***
- *Information om hur ansvarsområdena inklusive riskhantering i fråga om utmattning hanteras för en säker operativ verksamhet. **(5.1.4)***
- *Information om hur organisationen hanterar information och kommunikation för en säker operativ verksamhet. **(5.1.5)***
- *Information om kompetensstyrningssystem och tillhörande rutiner och hur dessa länkar till specifika arbets- eller uppgiftsinstruktioner för att upprätthålla en säker operativ verksamhet. **(5.1.6)***
- *Bevis på att driftdokumentation (förfaranden, arbetsinstruktioner etc.) är uppdaterad när och där det behövs. **(se även 4.5.3)***

5.1.5 Exempel på bevis

En lista över de obligatoriska kraven (inklusive TSD:er) och hur de efterlevs **(se också 2)**.

En förklaring av hur operativa risker hanteras genom riskbedömningsprocessen och hur det säkerställs att de operativa säkerhetsmålen uppfylls. Länkar finns till relevanta förfaranden.

En redogörelse för hur kompetensstyrningssystemet bidrar till kontrollen av operativa risker och hur informations- och kommunikationsflödet hanteras för att säkerställa att riskerna kontrolleras på ett korrekt sätt.

Uppgifter om dess underhållssystem för rullande materiel inklusive länkar till detaljerad dokumentation som stöder detta (där det inte finns något system med enheter som ansvarar för underhåll eller något certifieringssystem).

Uppgifter om befintliga kontroller före avgång (TSD drift och trafikledning) för att säkerställa att överensstämmelse kontrolleras gällande

- *bromsprestanda (förberedelse av uppgift till förare),*
- *tågsammansättning,*
- *främre och bakre signaler,*

- *last och dragna fordons skick.*

En kopia av processen för att identifiera fall av icke-överensstämmelse och hur det säkerställs att alla nödvändiga åtgärder vidtas, t.ex. sådana som leder till att fordonet tas ur drift, att trasiga/defekta komponenter/delar i utrustning/fordon ersätts eller att operativa begränsningar införs .

Ett dokument som anger vilka typer av fordon som ska användas på varje specifik rutt och typen av verksamhet som ska bedrivas, och i synnerhet alla

- *operativa begränsningar på grund av särskilda typer av fordon,*
- *restriktioner på grund av driften av specifika fordonstyper på specifika rutter ,*
- *ytterligare underhållskrav för specifika rutter (se även 5.2).*

Ett dokument som beskriver eventuella ytterligare krav för att hantera försämrade förhållanden (t.ex. incidenter med ett fordon) för det eller de nät som är berörda av området för driften.

Det finns en process för hantering av utmattning tillämplig på anställda med oregelbundna arbetstider. Processen utgår från faktabaserade metoder och professionell expertis. Processen tar hänsyn till att en rad faktorer måste beaktas för en övergripande strategi för riskhantering avseende utmattning. Processen för att hantera utmattning ska inbegripa planering och kontroll av arbetsmiljön och arbetsuppgifterna, för att så långt det är praktiskt möjligt minimera effekterna av utmattning på personalens vaksamhet och prestationer, på ett sätt som står i proportion till nivån för riskexponering och typen av verksamhet.

När det gäller efterlevnaden av de grundläggande driftsprinciperna i TSD drift och trafikledning tillhandahålls bevis som visar att järnvägsföretaget kan säkerställa följande (endast i illustrativt syfte):

- *Ett tåg får bara vara i drift på linjen om tågsammansättningen är kompatibel med infrastrukturen (grundläggande driftsprinciper 3).*

Detta är kopplat till bekräftelse av att tåget är kompatibelt med infrastrukturen på den linje där driften planeras, innan dess rörelse är godkänd. Kompatibilitet mellan ett tåg och infrastruktur påverkas främst av ett fordonets dimensioner och all lasten på fordonet , avstånden mellan tåg och infrastruktur eller till tåg på intilliggande spår (mätning/spårvidd), minimikravet för tågets bromsprestanda, tågets vikt och längd samt infrastrukturens kapacitet och förmåga.

Det finns bevis för att följande villkor uppfylls:

- *Kontroller sker före avgång för att säkerställa att tåget, innan det påbörjar eller fortsätter sin resa, och dess passagerare, personal och varor transporteras säkert (grundläggande driftsprinciper 4).*

Detta gäller iordningsställande av tåg . Det inkluderar exempelvis tågets bromsprestanda , den hastighet som tåget är tillåtet att färdas i, sammansättning av tåget, identifiering, lastning och säkring av gods, tillhandahållande av adekvat information för att utbilda operativ personal. Syftet är att förhindra kollisioner och urspårningar på grund av ett antal risker.

5.1.6 Referenser och standarder

- *ISO N360 JTCG konceptdokument till stöd för bilaga SL*
- *UIC-normblad 502-1:*
- [RID](#)
- *Vägledning om TSD drift och trafikledning*

5.1.7 Tillsynsfrågor

Tillsyn av operativ verksamhet bör genomföras med fokus på skilda områden och genom att dessa undersöks i detalj för att se hur de återspeglas i organisationens säkerhetsstyrningssystem, och om organisationen har rätt personal på rätt plats som gör rätt saker. Detta möjliggör för de nationella säkerhetsmyndigheterna att se om verksamheten omfattas av säkerhetsstyrningssystemet som en sammanhängande helhet eller om olika delar hanteras separat, med svaga länkar till säkerhetsmålen och den övergripande strategin.

Vid tillsyn bör särskilt följande kontrolleras:

- *Hur säkerhetsstyrningssystemets dokumentation överensstämmer med de lokala operativa bestämmelser som tagits fram för att hantera risker i verksamheten.*
- *Hanteringen av nödsituationer eller icke-rutinmässiga situationer.*
- *Hur gränserna för driften hanteras, inbegripet de operativa gränssnitten med andra parter.*
- *Rutiner för trötthetshantering.*
- *Hantering av farliga ämnen.*
- *Rutiner för transport av farligt gods, inklusive utbildning, roller och ansvar för organisationens personal, i enlighet med kapitel 1.3 och 1.4 i RID.*
- *Efterlevnad av de grundläggande driftsprinciper som anges i TSD drift och trafikledning.*

5.2 Styrning och kontroll av (operativa) tillgångar

5.2.1 Reglerande krav

5.2.1	Organisationen ska hantera säkerhetsrisker kopplade till fysiska tillgångar genom hela deras livscykel (se 3.1.1 Riskbedömning), från konstruktion till bortskaffande, och uppfylla kraven avseende mänskliga faktorer under hela livscykeln.
5.2.2	Organisationen ska: <ul style="list-style-type: none">(a) säkerställa att tillgångarna används för avsett syfte och hålla dem i säkert och driftdugligt skick, i enlighet med artikel 14.2 i direktiv (EU) 2016/798 i tillämpliga fall, samt på förväntad prestandanivå,(a) säkerställa att tillgångarna används för avsett syfte och hålla dem i säkert och driftdugligt skick samt på förväntad prestandanivå,(b) styra och kontrollera tillgångarna vid normal driftsförhållanden och vid störning,(c) så snart som praktiskt möjligt, upptäcka fall av bristande efterlevnad av driftskraven innan eller under det att tillgången används, inbegripet att vid behov tillämpa begränsningar av användning för att säkerställa ett driftdugligt skick för tillgången (se 6.1 Övervakning).
5.2.3	Organisationen ska säkerställa att dess planer och rutiner för förvaltning av tillgångar, i tillämpliga fall, uppfyller alla de grundläggande kraven i relevanta tekniska specifikationer för driftskompatibilitet och alla andra relevanta krav (se 1 Organisationens förutsättningar).
5.2.4	För att hålla risker under kontroll, när detta är relevant för underhåll (se 3.1.1 Riskbedömning), ska hänsyn tas till minst följande: <ul style="list-style-type: none">(a) Identifiering av underhållsbehovet för att hålla tillgången i ett säkert och driftdugligt skick, fastställt på grundval av den planerade och faktiska användningen av tillgången och på grundval av dess konstruktionsegenskaper.(a) Identifiering av underhållsbehovet för att hålla tillgången i ett säkert och driftdugligt skick, fastställt på grundval av den planerade och faktiska användningen av infrastrukturen och dess utformning.(b) Hanteringen när tillgången tas ur drift för underhåll, när defekter har konstaterats eller när tillgångens skick försämrats i en sådan grad att den inte längre befinner sig inom gränserna för ett säkert och driftdugligt skick för drift enligt punkt a.(c) Hanteringen när tillgången återtas i drift, med eventuella begränsningar för användning, efter det att underhåll har utförts i syfte att säkerställa att tillgången befinner sig i säkert och driftdugligt skick.(d) Styrning och kontroll av övervaknings- och mätutrustning för att säkerställa att den är i det skick som krävs för att kunna användas för avsett ändamål.
5.2.5	För att utöva kontroll över information och kommunikation, när detta är relevant för en säker styrning och kontroll av tillgångar (se 4.4 Information och kommunikation), ska organisationen ta hänsyn till <ul style="list-style-type: none">(a) utbytet av relevant information inom organisationen eller med underhållsansvarig enhet utanför organisationen (se 5.3 Entreprenörer, partner och leverantörer), i synnerhet om säkerhetsrelaterade fel, olyckor, tillbud samt om eventuella begränsningar för användning av tillgången,

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.

- (b) spårbarheten vad gäller all nödvändig information, inklusive information enligt punkt a (se 4.4 Information och kommunikation och 4.5.3 Kontroll över dokumenterad information),
- (c) upprättande och underhåll av dokumentation inbegripet hantering av alla sådana ändringar som påverkar tillgångarna i säkerhetshänseende (se 5.4 Hantering av ändringar).

5.2.2 Syfte

Sökanden bör visa hur tillgångarna förvaltas under livscykeln, från konstruktion till avyttring, genom de förfaranden och rutiner som anges i säkerhetsstyrningssystemet. Sökanden bör visa att en människocentrerad metod tillämpas i varje skede av livscykeln. Sökanden bör ange när förvaltningen av tillgångarna knyter an till olika delar av säkerhetsstyrningsprogrammet, till exempel kompetensförvaltning, verksamhetsplanering och övervakning. Sökanden bör inrikta sig på att visa att den har ett stabilt system för tillgångsförvaltning, som avspeglar riskerna i samband med verksamheternas typ och omfattning.

5.2.3 Förklarande anmärkningar

Med tillgång **(5.2)** menas all utrustning (fast eller rörlig), struktur, programvaror eller andra komponenter som kräver underhåll över tiden och tillhandahålls för järnvägsdrift. Tillgångarna delas i sin tur upp i tillgångar som förvaltas av järnvägsföretaget (främst fordon) och tillgångar som förvaltas av infrastrukturförvaltare (alla infrastrukturkomponenter, som spår, utrustning för trafiklednings-/signalsystem, spårbyten, kraftförsörjning, plankorsningar och anläggningar som broar, viadukter, tunnlar, plattformar, hissar, rulltrappor etc. En fullständig förteckning finns i bilaga I till direktiv 2012/34/EU).

Tillgångars livscykel består av följande faser:

- a) *Utformning.*
- b) *Genomförande (konstruktion/tillverkning, installation, provning och idrifttagande).*
- c) *Drift och underhåll.*
- d) *Reparation, ändringar och eftermontering, vilket omfattar hantering av förändringar.*
- e) *Modernisering, avveckling och bortskaffande.*

Det är viktigt för en organisation att visa hur den fångar och underhåller (system och) säkerhetskrav för tillgångar, och hur dessa kommer att bli verifierade, validerade och spårade.

Om underhåll kontrakteras till en tredje part, är det organisationens ansvar att specificera och övervaka att tillgångens prestanda uppfyller organisationens etablerade standarder.

Så snart processer är igång för att hantera risken som följer av säkerhetskritiska tillgångar, bör organisationen övervaka tillgångsprestandan med avseende på dessa risker och organisationens egna förväntningar.

När tillgångar troligen förnyas, avvecklas, eller kasseras, etablerar och dokumenterar organisationen processer för att hantera risker förknippade med sådana aktiviteter.

Dessa processer är bara relevanta för organisationer som utför sådana aktiviteter, eller som troligen kommer att utföra.

Vid ersättning av en tillgång som närmar sig slutet av sin livscykel försäkras sig organisationen att ersättningstillgången uppfyller etablerade kriterier för säkerhetsprestanda. Som en del av den här processen görs en genomgång av alla säkerhetsanalyser.

Kraven avseende underhåll **(5.2.4)** kommer från förordningen om ett certifieringssystem för enheter som ansvarar för underhåll av godsvagnar (ECM-förordningen). Godsvagnar är en tillgång som järnvägsföretaget och eventuellt infrastrukturförvaltaren bör förvalta. Kraven i ECM-förordningen är mer specifika och

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.

föreskrivande, medan de ovanstående kraven främst handlar om hur järnvägsföretagets och infrastrukturförvaltarens säkerhetsstyrningssystem samverkar med ECM:s underhållssystem, med målet att säkerställa att driften och underhållet av tillgångarna sker på ett säkert sätt. Säkerhetspåverkan av eventuella byten i samband med underhåll (som ingår i den berörda tillgångens livscykel) bör också finnas med i riskbedömningen enligt direktiv (EU) 2016/797 och relevanta specifikationer för driftskompatibilitet (TSD).

Alla tillgångar regleras inte av TSD (5.2.3), och även om en TSD gäller (t.ex. TSD INF) regleras endast det som krävs för driftskompatibilitet, vilket innebär att andra säkerhetskrav ändå kan behövas. Vid byte, modernisering eller uppgradering ska efterlevnaden av de väsentliga kraven i relevanta TDS upprätthållas (dvs. inte bara säkerhetskrav) enligt bestämmelserna i direktiv (EU) 2016/797.

Begreppet "driftsäkerhet" (5.2.4 a) betyder att tillgången ska användas inom säkra gränser. Gränserna för säker användning kan utvecklas under systemets livstid, men ska fastställas enligt parametrarna för driftskompatibilitet. Defekter kan upptäckas (5.2.4 b), och gränserna för säker användning kan anpassas efter detta. För fordon definieras driftsäkerhet i artikel 14.2 i direktiv (EU) 2016/798.

Konfigurationsstyrning (5.2.5 c) omfattar en unik identifiering av tillgångarna, var de finns, eventuellt utfört underhåll etc. (alltså inte bara konfigurationsstyrning av förändringar). Konfigurationsstyrningen av (tekniska) förändringar gäller för byten.

En enhet som har ansvar för underhåll ska utses i enlighet med artikel 14.1 i direktiv (EU) 2016/798 för att säkerställa att alla fordon som enheten har underhållsansvar för är driftsäkra. Det behövs ingen detaljerad beskrivning av de verksamheter som bedrivs av en enhet som har ansvar för underhåll som är certifierad enligt förordning (EU) nr 445/2011. Däremot är det nödvändigt att ange vilka faktorer och aspekter som omfattas av ECM-certifikatet och hur kontakterna med enheten som ansvarar för underhållet fungerar, särskilt vilken information som utbyts mellan sökanden och enheten och hur det går till.

När det gäller fordon som underhålls av ej certifierade enheter som ansvarar för underhåll (dvs. enheter som inte är certifierade enligt förordning (EU) nr 445/2011), är det sökandens ansvar att se till att fordon som den brukar är i ett säkert skick genom att övervaka att enheten har utformat och effektivt genomför sitt underhållssystem enligt artikel 14.2 och 14.3 samt bilaga III till direktiv (EU) 2016/798. Om de icke-certifierade enheterna som ansvarar för underhåll inte ingår i sökandens organisation bör fullgörandet av rättsliga skyldigheter säkerställas i form av avtalsvillkor.

Om järnvägsföretagen arbetar i partnerskap är varje järnvägsföretag fullständigt ansvarigt för en säker drift och för att kontrollera risker i samband med verksamheten, bland annat fordonsunderhållet. Om ett järnvägsföretag använder en partners säkerhetscertifikat för att kontrollera risker i samband med underhållet är detta inte tillräckligt om det inte ges stöd i form av avtalsvillkor med de andra järnvägsföretagen i partnerskapet. Dessa avtalsvillkor måste utformas gemensamt och övervakas av varje partner, och ingår även i varje partners säkerhetsstyrningssystem, vilket i sin tur innebär att de övervakas av de respektive nationella säkerhetsmyndigheterna. De respektive nationella säkerhetsmyndigheterna bör samordna sitt arbete för att hantera eventuella gränsöverskridande gränssnitt som kan ha skapats av de upphandlande enheterna.

5.2.4 Bevis

- *Information om tillgångsförvaltningssystemet inom organisationens säkerhetsstyrningssystem, inklusive relevanta kopplingar till andra områden, såsom riskbedömning, verksamhetsplanering, hantering av förändringar etc. (5.2.1, 5.2.2, 5.2.5 a och b):*

Planeringsfasen

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.

- Bevis för processer och samråd för att fastställa kraven avseende tillgångar.
- Bevis för riskhanteringsstrategier för upphandling och idrifttagande av nya eller ändrade tillgångar.
- Dokumentation om alla relevanta processer för konstruktion och leverans av tillgångar.
- Processer för att hantera risker under planeringsfasen.
- Bevis för de verktyg som används för att garantera säkerheten.
- Uppgifter om standarder eller annan säkerhetsinformation som används som grund för konstruktionen och underhållet av tillgången samt eventuella provningar för att bekräfta efterlevnaden.
- En handbok eller liknande som beskriver processerna för att bruka och underhålla tillgångarna och hur riskerna i drifts- och underhållsfasen hanteras.

Genomförandefasen

- Bevis för hantering av säkerhetsrisker, provning och validering av processer för konstruktion/tillverkning och idrifttagande av tillgången och tillgångens operativa beredskap.

Drift och underhåll

- Bevis för att standarder och processer följs och för att identifierade risker hanteras.
- Planer och rutiner för underhåll av tillgångarna.
- Bevis för hur organisationen identifierar och eliminerar risker.
- Bevis för processer för att rapportera och hantera problem med säkerhetsprestanda samt korrigerande åtgärder.
- Bevis för hur trender i prestanda övervakas mot tillgångens förväntade strategiska livslängd i syfte att följa upp prestanda och planera för moderniseringar.
- Processer för att identifiera fel och störningar och vidta korrigerande åtgärder.
- Hantering av nödsituationer eller icke-rutinmässiga situationer som kan påverka tillgångarnas säkerhet.
- Bevis för hur styrning och kontroll av tillgångar beaktas i samband med händelser som ska rapporteras samt hanteringen av gemensamma risker vid gränssnitten (**se även 3.1**).

Modernisering, avveckling och bortskaffande

- Bevis för processerna för att hantera risker i samband med modernisering, avveckling och bortskaffande av tillgångar i förhållande till organisationens omfattning och karaktär.
- Bevis för en systematisk strategi för att hantera mänskliga och organisatoriska faktorer i tillgångsförvaltningens alla livscykelstadier. **(5.2.1)**
- Bevis på att driftdokumentation överensstämmer med kraven för att hantera (drift och) underhåll vid organisatoriska och fysiska gränser, t.ex. organisatoriska, tekniska och operativa gränssnitt med angränsande infrastruktur, gränsstationer, interaktioner med andra järnvägsföretag eller infrastrukturförvaltare etc. **(5.2.3)**
- Information som visar att sökandens underhållsrutiner följer de tillämpliga kraven (lagstiftning, standarder etc.). **(5.2.3)**
- För fordon: en kopia av ECM-certifikatet eller bevis för att den enhet som ansvarar för underhållet följer artikel 14.2 och 14.3 samt bilaga III till direktiv (EU) 2016/798. **(5.2.4 a–d)**

I händelse av partnerskap mellan järnvägsföretag där det är partnern som står för underhållet av fordonet:

Bevis för parterna har enats om avtalsvillkor om detta, bland annat följande:

- Informationsutbyte enligt artikel 5 i förordning (EU) nr 445/2011.
- Tekniskt stöd vid behov, särskilt för kvarvarande system för trafikstyrning och signalering.

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.

- *Kontroll av att de underhållsverkstäder som anlitas har kapacitet för att tillhandahålla det underhåll som krävs.*
- *Övervakning av fordon och utbyte av relevant information om övervakningen. (se även 6.1)*
- *Vad gäller tillgångar för vilka det krävs intyg om överensstämmelse enligt EU-lagstiftningen eller nationella regler, en kopia av intyget tillsammans med en förklaring av i hur stor utsträckning säkerhetsstyrningssystemet bygger på dessa. (5.2.4 a–d)*
- *Information om hur dokumenthanteringsdelen i säkerhetsstyrningsplanen fungerar i förhållande till tillgångsförvaltningen, inbegripet bevis för att underhållsdokumentationen (förfaranden, arbetsinstruktioner etc.) uppdateras när så är nödvändigt. (5.2.5 a–c)*
- *Bevis för konfigurationshantering av tillgångarna under deras livscykel, inklusive eventuella processer för hantering av förändringar i samband med grundläggande omstruktureringar. (5.2.5 c)*

5.2.5 Exempel på bevis

Planeringsfasen

Organisationen dokumenterar alla relevanta säkerhetsrelaterade processer och uppgifter om konstruktion och leverans av tillgångarna genom konfigurationshanteringsprocesser (eller ett konfigurationsstyrningssystem). Dessa processer beskriver de tekniska och organisatoriska åtgärderna för att kontrollera tillgången under dess livscykel.

Organisationen inför och dokumenterar en process för att hantera risker i samband med utformningen av hanteringen av tillgångar genom att

- *fastställa krav för alla nya och/eller ändrade tillgångar (se även 1) och diskutera dem med berörda aktörer (se även 2.4),*
- *hantera risker i samband med genomförandet av sådana förändringar (se även 3.1), och*
- *hantera risker i samband med upphandling och kontraktsförvaltning i förekommande fall (se även 3.1 och 5.3).*

Detta bör omfatta analyser av säkerhetsrisker för att identifiera områden där risken för fel är som störst, vilket granskas mot organisationens risklogg. Detta kan åstadkommas genom att identifiera säkerhetskritiska system och införa centrala resultatmål med hjälp av lämpliga riskidentifieringstekniker, såsom

- *en analys av tillförlitlighet, funktionssannolikhet, driftsäkerhet, tillgänglighet, underhållsmässighet och säkerhet i fråga om tillgångarnas konstruktion (om centrala resultatkriterier kommuniceras till konstruktörerna för att säkerställa att tillgången är ändamålsenlig), och*
- *FMECA-analys (Failure Mode, Effects and Criticality Analysis) och/eller underhåll för att säkerställa tillförlitlighet (Reliability Centred Maintenance, RCM) så att risker under konstruktionsfasen kan hanteras och som underlag för en underhållsplan.*

Dessa krav kontrolleras mot särskilda standarder och processer för konstruktion, underhåll och drift av järnvägsinfrastruktur och rullande materiel enligt organisationens prioriteringar. Organisationen visar att

- *säkerhetskritiska system utformas enligt funktionella specifikationer,*
- *det finns en testplan för validering och idrifttagande för att bekräfta att tillgången är ändamålsenlig och säker att använda och underhålla, och*
- *drifts- och underhållsdokumentation har utarbetats, som beskriver processerna för uppdatering, granskning och underhåll av tillgångarna (se även 4.5).*

Organisationen ska visa att den använder lämpliga processer för systemteknik och säkerhetssäkring (t.ex. EN50126/8/9 för komplexa system) i sin strategi för konstruktion och upphandling. Detta kan åstadkommas

genom att organisationen upprättar en systemteknisk förvaltningsplan, som föreskriver förfarandet för att identifiera och registrera berörda aktörer, systemkrav och säkerhetsbehov.

Genomförandefasen

För att säkerställa att tillgången används på ett ändamålsenligt och säkert sätt inför organisationen processer för att hantera riskerna i samband med konstruktion, provning och idrifttagande av tillgången i linje med processerna i säkerhetsstyrningsplanen.

Organisationen ska även ha en process för

- *provning, kontroll och validering av tillgångens system- och säkerhetskrav, vilket kan åstadkommas med hjälp av en ledningsplan för provning och idrifttagande eller motsvarande, och*
- *tillgångens operativa beredskap, vilket kan åstadkommas med hjälp av en checklista för operativ beredskap.*

Drift och underhåll

Organisationen har utformat dokumentation om driften och underhållet av tillgången, som beskriver de säkerhetsstyrningsprocesser som organisationen använder för att uppdatera, granska och underhålla sina tillgångar. Den beskriver även verksamhetens omfattning, och vid behov, de riskhanteringsstrategier som organisationen har för att täcka alla relevanta verksamheter.

Syftet med denna dokumentation är att

- *säkerställa att tillgången brukas och underhålls på rätt sätt,*
- *identifiera och inbegripa alla säkerhetsrelaterade villkor som anger eventuella begränsningar av användningen av tillgången samt användningsvillkor, och*
- *ange de kontinuerliga kontroller som ska göras.*

Processen för att konfigurera konstruktion och leverans av föreslagna tillgångar (detta beskrivs i konstruktionsfasen) utvidgas till att omfatta tillgångens hela livscykel genom att organisationen gör följande:

- *Upprättar och underhåller ett register över alla tillgångar. Registret bör bland annat innehålla information om tillgångarnas unika identifiering, var de finns, eventuellt underhåll etc.*
- *Hanterar dokument och information om tillgångarna enligt organisationens säkerhetsstyrningssystem (se även 4.4 and 4.5).*
- *Fastställer hur kritiska tillgångarna är baserat på resultaten från en säkerhetsriskbedömning. Säkerhetskritiska tillgångar identifieras i tillgångsregistret.*

Organisationen visar hur informationen om tillgångarna skapas, underhålls och integreras i deras risklogg.

Organisationen övervakar löpande efterlevnad av valda standarder och processer för att säkerställa att järnvägsdriften är säker och effektiv. I detta syfte inför organisationen processer för att säkerställa att

- *tillgångarna brukas och underhålls enligt relevanta anvisningar,*
- *tillgångarnas skick övervakas,*
- *utrustning som behövs för att testa eller inspektera tillgångarna kontrolleras, kalibreras och underhålls på lämpligt sätt,*
- *eventuella risker i samband med driften och underhållet av tillgångarna hanteras enligt riskhanteringsprocesserna samt alla tillämpliga arbetsmiljölagar, och*
- *reservdelar finns tillgängliga för underhåll, särskilt för säkerhetskritiska tillgångar. Detta kan åstadkommas genom att organisationen fastställer behoven av reservdelar utifrån hur kritiska tillgångarna är, vilket i sin tur identifieras med hjälp av RCM.*

Organisationen visar att den har planerat underhållet av tillgångarna för att

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.

- uppfylla kompetens-, kapacitets- och resurskrav,
- tillgodose behoven av informationshantering och registrering,
- ta fram detaljerade planer utifrån en riskbaserad process, där de olika underhållsnivåerna fastställs och organisationens etablerade standardstrukturer, förfaranden och ansvar för underhållet anges, och
- se till att de verktyg och den utrustning som används för underhållet är kalibrerade.

Detta kan innefatta

- en teknisk underhållsplan, och
- arbetsinstruktioner som har tagits fram utifrån och granskats mot den tekniska underhållsplanen.

Planeringen ska dokumenteras och kontrolleras med hjälp av ett datoriserat system för underhållsstyrning (se även 4.5).

När fordon eller utrustning anvisas för en uppgift

- ska organisationen ha processer för att
 - se till att uppgiften/arbetet slutförs (t.ex. att varje typ av rullande materiel är tekniskt kompatibel med tåglinjerna, vilket ska kontrolleras enligt tjänstgöringsschemat och före avgång,
 - underhållet av säkerhetskritiska komponenter sker enligt planen (tidpunkter för förebyggande underhåll samt typ av underhåll),
 - underhållsåtgärderna fastställs när defekter upptäcks eller när gränserna för säker användning överskrids (korrigerande underhåll), om inte driftsbegränsningar införs,
 - nödvändiga åtgärder vidtas så snabbt som möjligt när det finns behov av förändringar, t.ex. att rullande materiel tas ur drift eller att driftsbegränsningar införs,
- arbetsinstruktioner finns tillgängliga för alla säkerhetskritiska verksamheter,
- kontroller görs av att alla uppgifter slutförs,
- dokumentationen om utfört underhåll kontrolleras (se även 4.5), och
- kompetensbaserad utbildning om alla säkerhetskritiska system finns tillgänglig (se även 4.1).

Det finns en process/rutiner för att säkerställa att driftsbegränsningar, vare sig de är tillfälliga eller permanenta (t.ex. en viss fordonstyp eller vissa linjer), ska införas.

- Processen eller rutinerna ska beaktas när fordon eller utrustning anvisas för en uppgift/ett arbete.
- Den personal som driver fordonet eller utrustningen ska informeras om detta i god tid (t.ex. lokförare, ombordansvarig).

Organisationen ska visa att den

- vet hur de säkerhetskritiska tillgångarna presterar genom att fastställa vad som behöver övervakas, mätas och rapporteras,
- har infört och registrerat metoder för övervakning, mätning, analys och utvärdering av säkerhetskritiska tillgångar och hur ofta detta bör göras,
- övervakar trender i prestanda mot tillgångens förväntade strategiska livslängd (se även 6.1),
- rapporterar om prestandaproblem baserat på säkerhetsriskens nivå och prioriterar säkerhetsrelaterade prestandaproblem så att de hanteras på lämpligt sätt,
- vid behov justerar underhållsplanen baserat på övervakningsresultaten,
- inrättar kanaler för att kommunicera resultat (se även 4.4),
- förbättrar prestandan hos säkerhetskritiska tillgångar genom att
 - se över drifts- och underhållskontroller och bedöma risken med tillgångar som inte uppfyller de fastställda standarderna,
 - identifierar grundorsakerna till säkerhetsproblem, och

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.

- fastställer nödvändiga åtgärder för att tillgångarna ska bli driftsäkra igen,
- ständigt förbättrar säkerhetsstyrningssystemet genom att identifiera eventuella risker och vidta korrigerande åtgärder (**se även 7.2**), och
- dokumenterar möjligheter att begränsa eller eliminera risker och hur detta uppnåddes.

Organisationen har processer för att identifiera eventuella fel eller störningar som kan uppstå hos tillgångarna och säkerställer att lämpliga korrigerande åtgärder vidtas. Dessa åtgärder vidtas enligt underhållsprogrammen eller planerna, och

- säkerställer att störningar och korrigerande åtgärder registreras,
- hanterar säkerhetskritiska fel,
- säkerställer lämplig rapportering av händelser, och
- samordnar icke schemalagda reparationer av säkerhetsrelaterade tillgångar.

Organisationen

- dokumenterar processerna för att hantera störningar,
- använder lämpliga analystekniker för säkerhetskritiska funktioner, såsom orsaksanalyser,
- registrerar störningar, vilket kan innebära felkoder, fellägen, effekter, kritikalitet och korrigerande åtgärder,
- utvecklar rutiner för att hantera gemensamma reparationer, och
- inför en återkopplingsprocess för de tekniska teamen för att granska och förbättra system och minimera risken för framtida fel.

Detta kan åstadkommas med hjälp av rapportering och analys av fel och korrigerande åtgärder, vilket omfattar följande:

- Registrera fel som upptäckts under provning och idrifttagande samt eventuella fel som uppstått under drift eller underhåll.
- Planera korrigerande åtgärder för att avhjälpa felen.

Organisationen dokumenterar alla fel och korrigerande åtgärder som kräver att en tekniskt kunnig person kontrollerar eventuella icke schemalagda reparationer.

Det finns en process/rutin som styr hanteringen av försämringar eller nödlägen i tillgångsförvaltningen.

Organisationen har infört processer för att hantera eventuella risker i gränssnitten som kan uppstå under driften och underhållet av tillgångarna (**se även 3.1.1**). Detta omfattar gränssnitt mellan tillgångarna och mellan de aktörer som använder dem.

Fasen för modernisering, avveckling och bortskaffande

Organisationen bör ha kontroll över tillgångarnas skick och ersätta eller underhålla tillgångar som har försämrats.

En testplan för validering och idrifttagande har upprättats för att bekräfta att den nya tillgången är ändamålsenlig och säker att använda och underhålla. Om organisationen förlänger en befintlig tillgångs livslängd bör den kontrollera relevant säkerhetsinformation, såsom historiska data, för att se till att den är säker att använda.

Organisationen bör övervaka trender mot förväntad prestanda (se drifts- och underhållsfasen).

När organisationen bortskaffar järnvägsinfrastruktur eller rullande materiel är det viktigt att riskerna i samband med att tillgången tas ur drift hanteras på lämpligt sätt.

Hantera ändringar av säkerhetskritiska tillgångar

I situationer där organisationen vill ändra den grundläggande konfigurationen hos säkerhetskritiska tillgångar genomför den en förändringshanteringsprocess för att säkerställa effektiv hantering av säkerhetsrisker och fastställa grundläggande konfigurationer för alla säkerhetskritiska tillgångar samt relaterad programvara (vare sig programvaran är inbyggd i befintliga system eller består av fristående program). Om en operatör ändrar den grundläggande konfigurationen för säkerhetskritiska tillgångar bör den, i möjligaste mån

- hantera de risker som uppstår i samband med ändringarna av tillgångarna,
- spåra serie- och modellnummer,
- validera funktionskrav mot specifikationer och riskkontrollåtgärder,
- kontrollera att den nya konfigurationen fungerar, och
- se till att de tillgångar som omfattas av konfigurationsstyrningen har aktuell status.

Organisationens ändringar av etablerade utgångsvärden, driftsförhållanden eller underhållsschemat för säkerhetskritiska tillgångar får inte på något sätt påverka säkerheten i järnvägsdriften.

Gemensamma säkerhetsmetoder

Det finns en process/rutin som enheterna som ansvarar för underhåll (t.ex. ECM) använder för att kontrollera att den gemensamma säkerhetsmetoden i riskbedömningen och övervakningen har tillämpats på lämpligt sätt (dvs. antingen enligt lag och/eller avtalsvillkor).

Integration av den mänskliga faktorn

Det finns en systematisk process för att integrera den mänskliga faktorn i systemens livscykel. Det tas till exempel hänsyn i utformning av arbetsuppgifter, arbetsrutiner, arbetsmiljö och det finns tillräckliga resurser i relation till tillgången, för att säkerställa att mänskliga och organisatoriska faktorer hanteras på lämpligt sätt.

Organisationens process bör innehålla en ram för hur identifierade problem i detta sammanhang identifieras och kontrolleras för att gemensamt enas om lösningar under konstruktions- eller förändringshanteringsprocessen. Processen anger dessutom förhållandet till andra parter som deltar i konstruktionsarbetet eller i genomförandet av ändringar.

Information om användningen av informationsverktyget för säkerhetsvarningar (SAIT) (se 5.4.3).

5.2.6 Referenser och standarder

- [Guide for the application of the Art 14 \(a\) of the Safety Directive and Commission Regulation \(EU\) No 445/2011 on a system of certification of entities in charge of maintenance for freight wagons](#)
- Cenelec – EN50126 Järnvägsanläggningar – Specifikation av tillförlitlighet, funktionssannolikhet, driftsäkerhet, tillgänglighet, underhållsmässighet och säkerhet (RAMS) – Del 1: Grundläggande fordringar och generell process.
- Office of the National Rail Safety Regulator – Asset management guideline (2015).

5.2.7 Tillsynsfrågor

När det gäller tillsynen är det viktigt att den koncentreras på förvaltningen av tillgångarna under deras livscykel, från konstruktion till bortskaffande, och inte på individuella fel i förvaltningen om de inte har direkta följder för säkerheten.

Tillsyn bör se till hur befintliga tillgångar som anskaffades före de rådande standarderna förvaltas och underhålls.

Tillsyn bör se till om och hur organisationen använder SAIT.

5.3 Entreprenörer, partner och leverantörer

5.3.1 Reglerande krav

5.3.1	Organisationen ska identifiera och hålla under kontroll säkerhetsrisker som uppstår på grund av att verksamhet lagts ut på entreprenad, inklusive drift eller samarbete med entreprenörer, partner och leverantörer.
5.3.2	För att hålla de säkerhetsrisker som avses i 5.3.1. under kontroll ska organisationen definiera kriterier för urval av entreprenörer, partner och leverantörer och de avtalsvillkor dessa måste uppfylla, däribland <ul style="list-style-type: none">(a) rättsliga och andra säkerhetsrelaterade krav (se 1. Organisationens förutsättningar),(b) den kompetensnivå som krävs för att utföra de uppgifter som anges i avtalet (se 4.2 Kompetens),(c) ansvaret för de arbetsuppgifter som ska utföras,(d) den förväntade säkerhetsnivå som ska upprätthållas under avtalets löptid,(e) skyldigheterna vad gäller utbytet av säkerhetsrelaterad information (se 4.4 Information och kommunikation),(f) spårbarheten vad gäller säkerhetsrelaterade dokument (se 4.5 Dokumenterad information).
5.3.3	I enlighet med den process som anges i artikel 3 i förordning (EU) nr 1078/2012 ska organisationen övervaka <ul style="list-style-type: none">(a) säkerhetsnivån inom alla aktiviteter och all verksamhet som utförs av entreprenörer, partner och leverantörer, för att säkerställa att de uppfyller de krav som anges i avtalet,(b) entreprenörers, partner och leverantörers medvetande om de säkerhetsrisker som de ger upphov till i organisationens verksamhet.

5.3.2 Syfte

Sökanden ska visa att den kan identifiera, bedöma och kontrollera risker i samband med de verksamheter som bedrivs av entreprenörer och andra leverantörer som sökanden har en arbetsförbindelse till. Detta handlar inte bara om riskbedömning, och det är inte heller nödvändigt att ange alla risker eller relevanta riskkategorier, utan sökandena ska visa hur deras system och rutiner i stort är utformade och organiserade för att göra det lättare att identifiera, bedöma och kontrollera riskerna. Detta inkluderar behovet att avtalet beskriver hur säkerhetsrelaterad information utbyts. Väl utformade avtal är ett allmänt vedertaget sätt att hantera risker. Det främsta ansvaret för att hantera entreprenörer och kontrollera att de uppfyller de fastställda riskerna ligger dock hos organisationen. Att organisationen anlitar entreprenörer eller underentreprenörer innebär dock inte att järnvägsföretaget/infrastrukturförvaltaren delegerar sitt ansvar för att se till att de kontrakterade tjänsterna utförs enligt överenskomna standarder.

Sökanden bör visa att den har processer för att kontrollera entreprenörers och andra leverantörers kompetens och bedöma deras säkerhetsnivå som ett led i upphandlingsprocessen.

Varje organisation ansvarar för att genomföra den övervakningsprocess som anges i den gemensamma säkerhetsmetoden och att genom avtalsvillkor säkerställa att de kontrollåtgärder som vidtas av entreprenörerna också övervakas enligt systemet. Om organisationerna identifierar relevanta säkerhetsrisker i samband med defekter eller fel i den tekniska utrustningen är de enligt den gemensamma säkerhetsmetoden skyldiga att rapportera dessa risker till övriga berörda parter så att de kan vidta eventuella nödvändiga korrigerande åtgärder för att säkerställa systemsäkerhet.

5.3.3 Förklarande anmärkningar

Ytterligare information om avtalsvillkor och partnerskap finns i bilaga 3.

5.3.4 Bevis

- *Bevis för att organisationens säkerhetsstyrningssystem är kopplat till entreprenörernas och leverantörernas riskhanteringssystem. (5.3.1)*
- *Bevis för att avtalsvillkoren utformas på grundval av riskbedömningar. (5.3.1) (se även 3.1)*
- *Bevis för att det finns processer som anger hur mänskliga och organisatoriska faktorer bör hanteras och kommuniceras till underentreprenörer samt hantering av underentreprenörer. (5.3.1)*
- *Bevis för hur organisationen hanterar dokumentation av entreprenörer och leverantörer. (5.3.2 a–d)*
- *Bevis för hur organisationen väljer entreprenörer och leverantörer för att säkerställa att de är kompetenta och att säkerhetsriskerna hanteras på lämpligt sätt. (5.3.2 a–e)*
- *Bevis för att organisationen har en process för att se till att viktig säkerhetsinformation förmedlas till eller rapporteras av entreprenörer och leverantörer. (5.3.2 d)*
- *Bevis för att organisationen har en process eller rutin för att säkerställa att de underentreprenörer och leverantörer den samarbetar med kan hantera de risker de ställs inför. (5.3.3 a och b)*
- *Bevis för att entreprenörer, partner eller leverantörer regelbundet övervakas enligt den gemensamma säkerhetsmetoden för övervakning (förordning (EU) nr 1078/2012), för att säkerställa att produkterna och tjänsterna uppfyller angivna krav och säkerhetsmål. (5.3.3 a) (se även 6.1)*

5.3.5 Exempel på bevis

Det finns ett förfarandet för att välja och övervaka entreprenörer, partner och leverantörer. Att förfarandet klagör att de standarder som entreprenörerna ska tillämpa är samma standarder som gäller för direkt anställd personal, samt vilka roller och ansvar entreprenörerna har. Att förfarandet dokumenterar det informationsutbyte som krävs mellan säkerhetsstyrningssystemen till sökanden och underentreprenörer, partner eller leverantörer.

Det finns bevis på de säkerhetsmål som entreprenörer, partner och leverantörer förväntas uppfylla och de indikatorer som kommer att användas för att mäta hur de uppfylls.

Strategin för mänskliga och organisatoriska faktorer visar hur dessa frågor hanteras med entreprenörer och underleverantörer.

Dokumenthanteringsrutinen för de standarder som ska tillämpas av entreprenörer, partner och leverantörer (se även 4.5.1.1 e, Dokumenterad information).

En förteckning/översikt av sökandens entreprenörer, partner och leverantörer för internt eller externt bruk, med angivelse av de produkter och/eller tjänster som de tillhandahåller **(se även 4.5.1.1 d och e)**, tillsammans med information om vilka följder detta får för säkerheten och vilka åtgärder som vidtas för att kontrollera de identifierade riskerna (t.ex. informationsutbyte, förtydligande av ansvar, utbildning) **(se även 3.1.1.1 a)**.

Sökandens system för att säkerställa personalens kompetens, kopplat till det system som tillämpas av entreprenörer, partner och leverantörer.

Att sökandens process/rutin för att hantera entreprenörer, partner och leverantörer omfattar åtgärder för att hantera gränssnittsrisker som uppstår i samband med deras verksamhet, att denna information utbyts vid behov, hur detta är integrerat i avtalsvillkoren och hur utbytet av information är integrerat i säkerhetsstyrningssystemet.

Att sökanden har en lämplig revisions-/inspektionsplaneringsprocess för sina entreprenörer, partner och leverantörer och att deras verksamheter i detta sammanhang registreras, till exempel i form av revisions-/inspektionsrapporter.

En process eller rutin för att identifiera relevanta krav som entreprenörer, partner och leverantörer omfattas av och informera dem om detta, och i förekommande fall om dessa krav anges i avtalsvillkoren. Detta bör ingå i dokumenthanteringssystemet för att se till att informationen går att spåra.

Sökandens dokumenthanteringssystem för att hantera intyg, tillstånd eller andra typer av bevis som visar att kraven för entreprenörer, partner och leverantörer uppfylls samt kontinuerlig kontroll av giltigheten (t.ex. genom övervakning).

5.3.6 Tillsynsfrågor

För att få en fullständig bild av omfattningen av kontroll- och övervakningsåtgärderna kan det vara nödvändigt att även låta tillsynen omfatta entreprenörer eller leverantörer som arbetar för organisationen. Det kan även vara nödvändigt att få tillgång till den dokumentation som entreprenören eller leverantören arbetar efter och undersöka hur den relaterar till de förfaranden som anges i organisationens säkerhetsstyrningsplan.

Rutiner för att se till att underentreprenörers och leverantörers säkerhetsnivå utgör en integrerad del av upphandlingsprocessen.

5.4 Hantering av förändringar

5.4.1 Reglerande krav

5.4.1 Organisationen ska genomföra och hantera ändringar i säkerhetsstyrningssystemet för att upprätthålla eller förbättra säkerhetsnivån. Detta ska omfatta beslut i de olika stadierna i ändringshanteringen och den efterföljande översynen med avseende på säkerhetsrisker (se 3.1.1 Riskbedömning).

5.4.2 Syfte

Det är viktigt att sökanden kan identifiera och bemöta nya risker som kan uppstå i verksamheten, genom att i förekommande fall tillämpa kraven i fråga om förändringshantering i direktiv (EU) 2016/798 och den gemensamma säkerhetsmetoden för riskvärdering och riskbedömning (kommissionens genomförandeförordning (EU) 402/2015). Sökanden bör visa att den gemensamma säkerhetsmetoden omfattar förfaranden för att utvärdera dessa risker och vid behov vidta nya riskkontrollåtgärder. Detta bör inbegripa alla typer och nivåer av förändringar, både större och mindre, permanenta och tillfälliga, omedelbara och långsiktiga. Det bör gälla förändringar av

- typ av verksamhet,
- utrustning,
- förfaranden,
- organisation,
- personal,
- gränssnitt.

Processen bör göra det möjligt att bedöma alla risker på ett proportionerligt och robust sätt, vid behov med hänsyn till mänskliga faktorer, och att vidta rimliga kontrollåtgärder.

Ändringar i roller, ansvar, verktyg och utrustning, arbetsmiljö, processer och förfaranden stöds av en analys av mänskliga och organisatoriska faktorer för att identifiera möjliga säkerhetsrisker relaterade till förändringen. Metoder som används kan till exempel vara uppgiftsanalys, analys av användbarhet, simulering, riskbedömning, HAZOP och säkerhetsenkät. Det finns exempel på förändring som föregås av riskbedömning med ett tillvägagångssätt som inbegriper mänskliga och organisatoriska faktorer. Det här är särskilt relevant vid förändring av arbetsrutiner till följd av ändrad utrustning, ändrat arbetsschema eller omfördelning av ansvar.

5.4.3 Förklarande anmärkningar

Alla förändringar omfattas inte av riskbedömningen (**5.4.1**). Förändringar som aktivt hanteras genom andra processer i säkerhetsstyrningssystemet, t.ex. den dagliga driften, bör inte betraktas som förändringar som ska hanteras via den formella förändringsprocessen.

De roller, ansvar och befogenheter som ska fastställas (**se även 2.3**) omfattar styrning av förändringar (**5.4.1**), t.ex. att fördela uppgifter till en kontrollansvarig avdelning.

Personalen bör rådfrågas under förändringshanteringsprocessen (**se även 2.4**).

Förändringar av roller, ansvar, verktyg och processer föregås av en säkerhetsanalys av den aktuella förändringen för att identifiera eventuella säkerhetsrisker. Säkerhetsrisker i samband med nedskärningar, förändringar i ledningen eller utläggande på entreprenad, bland annat verksamheter eller samarbete med entreprenörer, partner och leverantörer, bör hanteras och prioriteras på samma sätt som interna risker.

5.4.4 Bevis

- *En beskrivning av processen för att styra förändringar. (5.4.1)*
- *En beskrivning av de förfaranden och metoder som används för att utvärdera nya eller förändrade risker och införa nya förfaranden eller metoder. (5.4.1)*
- *Kontrollåtgärder, inklusive angivelser av var de detaljerade processerna kan hittas. (5.4.1)*
- *Information om hur organisationen identifierar väsentliga förändringar och fattar beslut om när processerna i de gemensamma säkerhetsmetoderna ska tillämpas eller när riskbedömningar ska utföras enligt förfarandena i säkerhetsstyrningssystemet. (5.4.1)*
- *Information om vilka rutiner som organisationen har infört inom ramen för hanteringen av förändringar för att hantera fordonstillstånd och ändringar av det gemensamma säkerhetsintyget eller säkerhetstillståndet. (5.4.1)*
- *Information om processen för anmälan av förändringar till den berörda nationella säkerhetsmyndigheten innan nya järnvägsverksamheter inleds. (5.4.2)*

5.4.5 Exempel på bevis

En kopia av förfarandet för hantering av förändringar som bifogas ansökan. Detta dokument omfattar kraven för riskbedömning av alla förändringar enligt olika rättsliga krav. Organisationens visar exempel på en problem- och antagandelogg, som regelbundet ses över allteftersom förändringen genomförs. Förfarandet omfattar även processen för anmälan av förändringar till den nationella säkerhetsmyndigheten.

Processen för hantering av förändringar refererar till användandet av riskbedömningsprocessen och resultaten beaktas när operativa processer utformas, genomförs och ses över.

5.4.6 Tillsynsfrågor

För att fastställa om rutinerna för hantering av förändringar i den gemensamma säkerhetsmetoden är tillräckligt robusta är det nödvändigt att följa ett antal förändringar av olika typer under processens gång för att se om de a) har hanterats på lämpligt sätt och om de risker som kan uppstå till följd av den aktuella förändringen har beaktats, och b) om eventuella lärdomar har integrerats i översynerna av förfarandena i den gemensamma säkerhetsmetoden.

Bedöma om förfarandena för hantering av förändringar överensstämmer med den gemensamma säkerhetsmetoden om riskbedömning.

Organisationen har processer för att genomföra och kontinuerligt övervaka relevanta TSD, nationella regler och andra standarder, och vid behov kan visa hur dessa tillämpas under utrustningens eller verksamhetens livscykel.

5.5 Hantering av nödsituationer

5.5.1 Reglerande krav

5.5.1	Organisationen ska identifiera nödsituationer och de därtill hörande åtgärder som ska vidtas i tid för att hantera dem (se 3.1.1 Riskbedömning) och för att återgå till normala driftsförhållanden i enlighet med förordning (EU) 2015/995 (1).
5.5.2	Organisationen ska, för varje identifierad typ av nödsituation, säkerställa att a) larmtjänster omgående kan kontaktas, b) larmtjänsterna får all relevant information, både i förväg med tanke på förberedelserna inför larmutryckningen, och vid själva nödsituationen, c) första hjälpen tillhandahålls internt.
5.5.3	Organisationen ska identifiera och dokumentera roller och ansvarsområden för alla parter i enlighet med förordning (EU) 2015/995.
5.5.4	Organisationen ska ha planer för insats, larm och information i händelse av en nödsituation, inklusive rutiner för att: (a) larma all personal med ansvar för hantering av nödsituationer, (b) <i>sprida information till alla parter (t.ex. infrastrukturförvaltare, entreprenörer, myndigheter, larmtjänster), inklusive nödlägesinstruktioner för passagerare</i> c) fatta de beslut som krävs utifrån den nödsituation som föreligger.
5.5.5	Organisationen ska beskriva hur resurser och medel för hantering av nödsituationer har fördelats (se 4.1 Resurser) och hur utbildningskraven har fastställts (se 4.2 Kompetens).
5.5.6	Planer och rutiner för nödsituationer ska testas regelbundet i samarbete med andra berörda parter och uppdateras vid behov.
5.5.7	Organisationen ska säkerställa att kompetent ansvarig personal, med erforderliga språkkunskaper, kan kontaktas enkelt och utan dröjsmål av infrastrukturförvaltaren och att denna personal kan förse infrastrukturförvaltaren med information på relevant nivå.
5.5.7	<i>Organisationen ska samordna planer för nödsituationer med alla järnvägsföretag som använder organisationens infrastruktur, med larmtjänster, så att de snabbt kan ingripa, och med alla andra parter som skulle kunna bli involverade i en nödsituation.</i>
5.5.8	Organisationen ska ha ett förfarande för att kontakta den underhållsansvariga enheten eller fordonsinnehavaren vid en nödsituation.
5.5.8	<i>Organisationen ska ha planer och rutiner för att vid behov omgående kunna stoppa driften och järnvägstrafiken samt informera alla berörda parter om de åtgärder som har vidtagits.</i>
5.5.9	<i>När det gäller gränsöverskridande infrastruktur ska samarbete mellan relevanta infrastrukturförvaltare underlätta den nödvändiga samordningen av och beredskapen hos de behöriga larmtjänsterna på båda sidor om gränsen.</i>

5.5.2 Syfte

Robusta system för planering i händelse av nödsituationer är av grundläggande vikt för alla ansvariga och bör omfatta den information som bör lämnas till räddningstjänsterna så att de kan utforma sina planer för åtgärder vid allvarigare incidenter. De aspekter av den gemensamma säkerhetsmetoden som är direkt relevanta för rutiner för att hantera nödsituationer är också viktiga, t.ex. övningar och testning av beredskapsplaner.

5.5.3 Förklarande anmärkningar

Nödsituationer **(5.5.1)** har samband med resultaten av organisationens riskbedömning, även om TSD Drift och trafikledning (se punkt 4.2.3.7) innehåller en icke uttömmande förteckning över nödsituationer.

Notera att 5.5.7 och 5.5.8 i det reglerande kravet ovan har olika lydelse för järnvägsföretag respektive infrastrukturförvaltare. 5.5.9 avser endast infrastrukturförvaltare.

5.5.4 Bevis

Sökanden förväntas lämna en översikt av följande:

- *De typer av nödsituationer som omfattas, även driftsförsämringar och de åtgärder som vidtas för att hantera detta. **(5.5.1)***
- *Den information som sökanden lämnar till räddningstjänsterna så att de ska kunna planera sina insatser vid större järnvägsolyckor, i förekommande fall med hänvisning till skyldigheter enligt tillämplig EU-lagstiftning och eventuella gränsöverskridande arrangemang. **(5.5.2 a och b)***
- *Planer, roller och ansvar (även för personer med särskild kompetens som avdelas att assistera infrastrukturförvaltaren eller tvärtom), utbildning och åtgärder för att behålla kompetens samt rutiner för effektiv kommunikation med räddningstjänsterna och relevant personal och information till personer som drabbas av olyckor, såsom passagerare eller berörda tredje parter (detta bör visas i form av ett dokument som anger alla parter roller och ansvar, hur resurser och medel fördelas och vilka utbildningsbehov som har identifierats samt rutiner för att återgå till normal drift efter en nödsituation. **(5.5.1), (5.5.3), (5.5.4 a–c), (5.5.5), (5.5.7) (5.5.8 och 5.5.9, endast från krav som gäller infrastrukturförvaltare)***
- *Särskilda aspekter av säkerhetsstyrningssystemet som är direkt relevanta för rutiner för att hantera nödsituationer, t.ex. övningar och testning av beredskapsplaner för att identifiera eventuella svagheter. **(5.5.6)***
- *Förfarandet för att kontakta den enhet som ansvarar för underhållet eller fordonsinnehavaren vid en eventuell nödsituation som påverkar deras fordon. **(5.5.8, endast från rättsliga krav för järnvägsföretag)***

5.5.5 Exempel på bevis

En kopia av förfaranden och planer för hantering av nödsituationer (t.ex. återhämtningsrutiner). Förfarandet omfattar hela det trafikerade nätet, med särskilda rutiner för tunnlar och andra platser som medför hög risk, och gränsöverskridande samarbete, personal, roller och ansvar, med kopplingar till infrastrukturförvaltarens rutiner för nödsituationer och hur andra berörda parter bör kontaktas, t.ex. enheter som ansvarar för underhåll. När området för verksamheten för ett järnvägsföretag omfattar flera infrastrukturförvaltare, bör järnvägsföretaget ta i beaktan infrastrukturförvaltarens olika arrangemang (och användaröverenskommelser) för nödsituationer.

Förfarandet innehåller en hänvisning till den gemensamma säkerhetsmetodens krav för personal som rycker in vid nödsituationer. Extern personal måste uppfylla samma standarder.

Förfarandet vid nödsituationer inbegriper även en process för att informera olycksoffer och deras anhöriga om klagomålsförfaranden.

Förfarandet omfattar (i förekommande fall) information om vad som sker vid en nödsituation där farligt gods är inblandat, och organisationen (järnvägsföretaget) har en process för att säkerställa att

- *det är lätt att komma i kontakt med lastaren, tankvagnsägaren om vagnen är privatägd, ägaren eller innehavaren och operatören om det rör sig om en tankcontainer, mottagaren etc.,*
- *infrastrukturförvaltaren så snabbt som möjligt får relevant information (t.ex. vagnarnas registreringsnummer, vagnarnas placering i tågsättet, UN-nummer, RID-klassificeringskod och riskidentifieringsnummer för det farliga godset enligt RID-bestämmelserna),*
- *organisationen (infrastrukturförvaltaren) har en process för att se till att myndigheterna (t.ex. räddningstjänster, polisen, andra larmtjänster och myndigheter) får relevant information om farligt gods (se exemplen ovan).*

5.5.6 Tillsynsfrågor

För bedömningen av säkerhetsstyrningssystemets förfaranden för att hantera nödsituationer kan det vara nödvändigt att dubbelkontrollera dem mot relevanta gränssnittsaktörers förfaranden, särskilt förhållandet mellan centrala aktörer såsom järnvägsföretaget, infrastrukturförvaltaren och räddningstjänsten, för att se till att rutinerna för att hantera tillbud är enhetliga.

Kontrollera att det finns förfaranden för alla förutsägbara nödsituationer.

Rutiner för att testa beredskapsplaner och samordnade förfaranden med räddningstjänster, som inte är begränsade till teoretiska övningar.

Gränssnittsförfaranden med andra berörda parter finns och omfattar kontroller av tester samt kommunikation, samordning och kompetens.

6 Utvärdering

6.1 Övervakning

6.1.1 Reglerande krav

- 6.6.1. Organisationen ska utföra övervakning i enlighet med förordning (EU) nr 1078/2012 i syfte att
- (a) kontrollera att alla processer och förfaranden i säkerhetsstyrningssystemet, inbegripet de driftsmässiga, organisatoriska och tekniska säkerhetsåtgärderna, tillämpas korrekt och att de är ändamålsenliga,
 - (b) kontrollera att säkerhetsstyrningssystemet tillämpas korrekt som en helhet och huruvida det uppnår de förväntade resultaten,
 - (c) undersöka om säkerhetsstyrningssystemet uppfyller kraven i denna förordning,
 - (d) fastställa och genomföra korrigerande åtgärder och utvärdera åtgärdernas ändamålsenlighet (se 7.2 Kontinuerlig förbättring), vid behov, om eventuell bristande efterlevnad av punkterna a, b och c upptäcks.
- 6.6.2. Organisationen ska regelbundet övervaka hur säkerhetsrelaterade arbetsuppgifter utförs inom organisationen, på alla nivåer, och ingripa om dessa uppgifter inte utförs ordentligt.

6.1.2 Syfte

Organisationen bör visa att den har en process för att övervaka tillämpningen av och effektiviteten hos säkerhetsstyrningssystemet, och att processen är lämplig för verksamhetens omfattning och typ. Organisationen bör även visa att det med hjälp av processen är möjligt att identifiera, utvärdera och korrigera eventuella brister i säkerhetsstyrningssystemets funktion.

6.1.3 Förklarande anmärkningar

Kontrollåtgärdernas effektivitet innebär att organisationen har en process för att kontrollera att riskbedömningar och de åtgärder som vidtas till följd av dessa granskas efter en viss period för att säkerställa att åtgärderna har lett till att säkerhetsrisken har minskat som förväntat (6.1.1 d).

Övervakningen bör omfatta en analys av hur strategin för mänskliga och organisatoriska faktorer har fungerat.

Säkerhetsnivån bedöms systematiskt mot strategin för förbättring av säkerhetskulturen. Det betyder att organisationen bör se till hur förbättringar i säkerhetskulturen passar med och är del av målet med förbättrad säkerhet.

Självkritiska och objektiva bedömningar av organisationens program, metoder och resultat på säkerhetsområdet ska genomföras rutinmässigt. Säkerhetsinformation, till exempel från program för korrigerande åtgärder, personalprestationer, incident- och olycksanalyser, undersökningar och relevant intern och extern erfarenhet av driften, ska systematiskt samlas in och utvärderas för att identifiera trender och se till att både organisationen och personalen håller sig till fastställda rutiner.

Sådana bedömningar ger en tydlig bild av hur organisationens säkerhetskultur påverkar säkerheten och kan därför bidra till att förbättra säkerheten. Syftet med en sådan bedömning är att identifiera starka och svaga punkter i säkerhetskulturen genom en jämförelse av hur den är jämfört med hur den är tänkt att vara. Detta ger organisationen möjlighet att prioritera områden som kan förbättras och göra ändringar, till exempel av processen, utbildningen och beteendet. Säkerhetsbedömningar är ett sätt att arbeta proaktivt för att förbättra säkerheten och höja säkerhetsmarginalerna. Oberoende bedömningar av säkerhetskulturen

rekommenderas vart tredje till femte år, medan organisatoriska egenbedömningar bör genomföras varje eller vartannat år.

6.1.4 Bevis

- *Information om hur sökanden har genomfört den gemensamma säkerhetsmetoden om övervakning. (6.1.1 a)*
- *Information om hur övervakningsprocessen identifierar om de förväntade säkerhetsmålen har uppnåtts eller ej. (6.1.1 b)*
- *Bevis för att säkerhetsstyrningssystemet har ändrats till följd av att åtgärder har vidtagits för att korrigera brister som upptäckts under övervakningen. (6.1.1 c)*
- *Organisationen bör ha en process för att fastställa resultatstandarder och resultatindikatorer för övervakningen av operativa processer och genomförda ändringar. Det bör finnas ett program för kontinuerlig bedömning av processer som har samband med mänskliga och organisatoriska faktorer, till exempel hur personalen följer etablerade förfaranden och i fråga om användning av ny utrustning. (6.1.2)*

6.1.5 Exempel på bevis

En förklaring om att den gemensamma säkerhetsmetoden om övervakning tillämpas och att det finns ett förfarande som täcker denna verksamhet. Förfarandet anger hur uppfyllandet av säkerhetsmålen mäts och korrigeras inom ramen för hanteringen av förändringar och riskbedömningsprocessen samt hur brister i säkerhetsstyrningssystemet kommer att korrigeras.

Organisationen har processer och förfaranden för att systematiskt kontrollera att alla rutiner för att inbegripa mänskliga och organisatoriska faktorer är lämpliga och att resultaten överensstämmer med prestandaindikatorerna.

Organisationen ska ha processer och rutiner för att systematiskt utvärdera hur personalen utför säkerhetskritiska arbetsuppgifter. Dessa processer baseras på en proaktiv strategi, med standarder för prestanda och systematisk utvärdering. Faktabaserade metoder används, till exempel personalresursledning.

6.1.6 Tillsynsfrågor

Granskningar av övervakningsprocessen och de resultat och åtgärder som den leder till är avgörande för att fastställa huruvida säkerhetsstyrningssystemet är ett "levande" dokument som utvecklas allteftersom erfarenheterna skapar förbättringar, eller om den är ett fastställt dokument som inte förändras över tiden.

En annan avgörande faktor är att granska ett antal viktiga riskområden och kontroller för att se om de tillämpas korrekt och är effektiva i säkerhetsstyrningssystemet, så att de nationella tillsynsmyndigheterna kan fastställa att de gemensamma säkerhetsmetoderna för övervakning efterlevs.

6.2 Internrevision

6.2.1 Reglerande krav

- 6.2.1. Organisationen ska utföra internrevisioner på ett oberoende, opartiskt och öppet sätt för att samla in och analysera information för sina övervakningsaktiviteter (se 6.1 Övervakning), vari följande ska ingå:
- (a) En tidsplan över planerade internrevisioner, som kan ses över med hänsyn till resultaten från tidigare revisioner och övervakning.
 - (b) Identifiering och urval av behöriga revisorer (se 4.2 Kompetens).
 - (c) Analys och utvärdering av revisionsresultaten.
 - (d) Fastställande av om det behövs korrigerande eller förbättrande åtgärder.
 - (e) Kontroll av om åtgärderna har slutförts och om de är ändamålsenliga.
 - (f) Dokumentation rörande genomförandet och resultaten av revisioner.
 - (g) Rapportering av revisionsresultaten till högsta ledningen.

6.2.2 Syfte

Sökande ska visa att de har ett internt revisionssystem med kompetent personal som ger meningsfulla resultat som ledningen tar hänsyn till och som säkerställer att säkerhetsstyrningssystemet uppfyller de rättsliga bestämmelserna.

6.2.3 Förklarande anmärkningar

Interna revisioner **(6.2.1)** betraktas som övervakningsverktyg inom ramen för den gemensamma säkerhetsmetoden om övervakning. Även om detta är ett separat krav är syftet att bidra till att uppnå övervakningsmålen enligt den gemensamma säkerhetsmetoden om övervakning.

Syftet med interna revisioner **(6.2.1)** är att få information om huruvida säkerhetsstyrningssystemet överensstämmer med de tillämpliga kraven **(6.1.1 c)** och om det genomförs och upprätthålls på ett effektivt sätt **(6.1.1 a, b och d)**. Tillämpliga krav avser kraven i bilagorna I och II till den gemensamma säkerhetsmetoden om bedömning av överensstämmelse, och därmed alla andra krav som organisationen tillämpar **(se även 1.1)**.

Revisorerna har ansvaret för att kontrollera att de korrigerande åtgärder eller förbättringsåtgärder som vidtas till följd av revisionsresultaten är fullständiga och effektiva **(6.2.1 c)**.

6.2.4 Bevis

- Organisationen ska visa att det finns en internrevisionsprocess eller ram för planerade revisioner och kompletterande riktade revisioner på grundval av säkerhetsinformation. **(6.2.1 a)**
- Bevis för ett kompetensförvaltningssystem med verktyg för att kontrollera interna revisorers kompetens. **(6.2.1 b)**
- Bevis för både interna och externa revisionsresultat som har föranlett åtgärder. **(6.2.1 c–f)**
- Bevis för att revisionsresultaten har diskuterats på högsta ledningsnivå och att relevanta åtgärder har vidtagits till följd av detta. **(6.2.1 g)**

6.2.5 Exempel på bevis

Det finns ett internt revisionsförfarande för planerade och kompletterande revisioner, inbegripet diskussioner om resultaten på hög ledningsnivå.

Exempel på revisionsrapporter och register över resultaten från interna revisioner, som anger vilka åtgärder som har vidtagits med anledning av resultaten.

Resultat av revisioner som har genomförts inom organisationen samlas in, analyseras och fungerar som underlag för rekommendationer för de regelbundna genomgångarna av ledningen.

Förfarandet innehåller hänvisningar till kompetensförvaltningssystemet. Den gemensamma säkerhetsmetoden visar att revisorerna har genomgått lämplig utbildning i revisionsfrågor (t.ex. ISO).

6.2.6 Referenser och standarder

- *ISO 19011:2011 – Vägledning för revision av ledningssystem*

6.2.7 Tillsynsfrågor

Granskning av planering av revisioner och revisionsresultat är en viktig del av tillsynen. Granskningen visar om revisionen inriktas på rätt områden, om resultaten är rimliga och om revisionspersonalen är kompetent och oberoende.

Kontrollera att de områden som väljs ut för revision överensstämmer med organisationens riskprofil.

Det finns en mekanism för att genomföra ej planerade revisioner, som aktiveras genom att ett antal exempel granskas.

6.3 Ledningens genomgång

6.3.1 Reglerande krav

6.3.1	Högsta ledningen ska regelbundet granska säkerhetsstyrningssystemets fortsatta lämplighet och ändamålsenlighet med beaktande av minst följande: <ul style="list-style-type: none">(a) En beskrivning av framstegen med att hantera ännu ej slutförda åtgärder från tidigare ledningsgenomgångar.(b) Förändrade interna och externa förhållanden (se 1. Organisationens förutsättningar),(c) Organisationens säkerhetsnivå med avseende på<ul style="list-style-type: none">i) uppfyllandet av säkerhetsmålen,ii) resultaten från dess övervakningsaktiviteter, inklusive resultat från internrevisioner, och från interna utredningar rörande olyckor/tillbud samt status vad gäller åtgärderna på respektive område,iii) relevanta resultat från tillsynsverksamhet som utförts av den nationella säkerhetsmyndigheten.(d) Rekommendationer till förbättringar.
6.3.2	Baserat på resultaten av ledningens genomgång ska den högsta ledningen ta det övergripande ansvaret för planeringen och genomförandet av nödvändiga ändringar av säkerhetsstyrningssystemet.

6.3.2 Syfte

Starkt ledarskap från ledningen är avgörande för att organisationens säkerhetsstyrningssystem ska fungera effektivt och ändamålsenligt och utvecklas över tiden. Organisationen bör visa att ledningen aktivt deltar i granskningen av säkerhetsstyrningssystemets prestanda och utvecklar det inför framtiden.

6.3.3 Bevis

- *Processer för ledningsmöten om granskningen av säkerhetsstyrningssystemet och framstegen med interna rekommendationer från revisioner och granskningar. (6.3.1 a–d)*
- *Uppgifter om organisationens resultat jämfört med säkerhetsmålen. (6.3.1 c i)*
- *Bevis för att rekommendationerna från den berörda nationella säkerhetsmyndigheten har beaktats i säkerhetsstyrningssystemet. (6.3.1 c iii)*
- *Organisationen kan visa att den har processer för att ta fram och sätta upp mål som är förenliga med typen och omfattningen av relevanta risker, att den regelbundet bedömer resultaten mot målen, följer tillämpliga förfaranden och använder säkerhetsuppgifter för att övervaka, granska och genomföra ändringar av de operativa rutinerna. (6.3.1)*
- *Bevis för att ledningen spelar en aktiv roll i planeringen och genomförandet av nödvändiga förändringar av säkerhetsstyrningssystemet. (6.3.2)*
- *Det finns processer och verktyg för att systematiskt rapportera alla typer av identifierade risker, fel, tillbud, tillkortakommanden och händelser, liksom för att kategorisera och analysera det som rapporterats med hänsyn till mänskliga och organisatoriska faktorer, för att hitta rotorsaker och effektiva åtgärder.*
- *Experter på mänskliga och organisatoriska faktorer används i processen för olycksutredning.*
- *Det finns systematiska processer för att återföra lärdomar gällande mänskliga och organisatoriska faktorer till utbildning och design.*
- *Lärdomar från olycks- och tillbudsutredningar kommuniceras till anställda i organisationen och återförs i utbildning, design och andra områden för att minska sannolikheten för en upprepning.*

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.

- *Resultat från olycksutredningar tas upp på ledningsmöten och ses som ett viktigt redskap för lärande och förbättring.*
- *Det finns en process för att säkerställa kvaliteten på olycksutredningar.*

6.3.4 Exempel på bevis

Förfarandet för granskning av och åtgärder till följd av interna rekommendationer från revisioner och granskningar som utförts av den högsta ledningen, tillsammans med protokoll från utvalda möten.

En problemlogg som visar vilka rekommendationer som har gjorts och framstegen med att korrigera brister som har fastställts av ledningen.

Förfarandet för ledningens granskning av resultaten från interna olycksundersökningar samt relevanta resultat från den nationella säkerhetsmyndighetens tillsyn.

Information tillhandahålls gällande vilka indikatorer som följs upp av ledningen och hur frekvent detta görs.

6.3.5 Tillsynsfrågor

När det gäller tillsynen är det viktigt att processen för att säkerställa att ledningen granskar säkerhetsstyrningssystemet leder till verkliga förändringar på operativ nivå.

Ledningen måste följa föränderliga interna och externa omständigheter. Tillämpar ledningen till exempel framtidsanalys eller andra tekniker såsom PESTLE-principen (*Political, Economic, Social, Technical, Legal, Environmental*) för att informera om utvecklingen av säkerhetsstyrningssystemet?

Länken mellan resultaten av ledningens genomgång och hur dessa resultat blir ett underlag till den årliga säkerhetsrapporten.

7 Förbättringar

7.1 Lärdomar av olyckor och tillbud

7.1.1 Reglerande krav

- 7.1.1. Olyckor och tillbud som har anknytning till organisationens järnvägsverksamhet ska:
- (a) rapporteras, registreras, utredas och analyseras för fastställande av de bakomliggande orsakerna,
 - (b) rapporteras till nationella organ, i tillämpliga fall.
- 7.1.2. Organisationen ska säkerställa att:
- (a) rekommendationerna från den nationella säkerhetsmyndigheten, det nationella utredningsorganet och från branschledda/interna utredningar utvärderas och genomförs om detta är tillämpligt eller förordnas,
 - (b) relevanta rapporter/uppgifter från andra berörda parter som järnvägsföretag, infrastrukturförvaltare, underhållsansvarig enhet och fordonsinnehavare övervägs och beaktas.
- 7.1.3. Organisationen ska använda information som har samband med utredningen för att se över riskbedömningen (se 3.1.1 Riskbedömning) för att dra lärdomar, i syfte att förbättra säkerheten och, vid behov, anta korrigerande åtgärder och/eller förbättrande åtgärder (se 5.4 Hantering av ändringar).

7.1.2 Syfte

Organisationen bör visa att den utreder olyckor och tillbud för att lära av erfarenheten och förbättra riskkontrollerna, att den personal som ansvarar för detta har rätt kompetens för att genomföra utredningar, även av personal- och organisationsrelaterade problem, att olyckor rapporteras till berörda myndigheter, att rekommendationer och rapporter tas fram och att ledningen agerar enligt dessa.

Analysen av oönskade händelser bör inte inriktas på att hitta skyldiga eller att en avdelning är mer ansvarig än en annan, utan det handlar om att förstå och förbättra de organisatoriska svagheter som föranledde sådana händelser. Den största utmaningen i analysen av händelser är att även förhindra "relaterade" händelser. Om analysen inte går längre än att hitta de omedelbara orsakerna blir det endast möjligt att förhindra att liknande händelser inträffar. Om analysen däremot gör det möjligt att identifiera tekniska och organisatoriska "grundorsaker" bidrar förbättringsåtgärderna till att förebygga andra typer av olyckor som föranleds av samma mekanismer. Om analysen exempelvis visar att ett förfarande inte har uppdaterats och den korrigerande åtgärden endast syftar till att rätta till detta blir effekten begränsad. Om analysen däremot går längre och identifierar brister i processen för att uppdatera förfarandena blir den positiva effekten av en förbättringsåtgärd mycket större.

Organisationen tillämpar dessutom "dubbelriktat lärande", vilket innebär att lärandet inte bara inriktas på själva händelsen, utan även på organisationens förmåga till förbättring, genom att inrikta sig på de faktorer som antingen främjar eller hindrar kunskaps- och informationsöverföringen inom organisationen.

Rapportering av farliga situationer och överhängande risk för tillbud uppmuntras och underlättas. Vid behov finns mekanismer för anonym rapportering. Om rapporteringen är personlig hjälper den personal eller avdelning som har skickat rapporten till med analysen och kommer med förslag om kortsiktiga åtgärder. Gruppdiskussioner organiseras och berörd personal eller hela organisationen informeras om vidtagna åtgärder.

Analyserna av farliga händelser analyseras i ett helhetsperspektiv med hjälp av olika kompetenser och med hänsyn till alla berörda parter (vid behov även externa parter).

En "rättvissekultur" främjas och positiva säkerhetsinitiativ uppmuntras och förstärks (incidentrapportering, personalens deltagande i analysarbete och insatser för ständig förbättring, stöd till kollegor etc.). Rättvisekulturen bör syfta till att ingen är rädd för att få skulden, genom en allmänt accepterad gräns för vad som är tillåtet eller ej. Alla ska kunna göra misstag.

7.1.3 Förklarande anmärkningar

Begreppen "händelser som kunde ha lett till olyckor" och "andra farliga händelser" ingår i definitionen av "tillbud" enligt direktiv (EU) 2016/798. Det är lika viktigt att utreda händelser som kunde ha lett till olyckor och andra farliga händelser för att proaktivt hantera säkerhetsfrågor.

Erfarenheter från olyckor och tillbud bör bidra till informationsutbytet med andra berörda parter (infrastrukturförvaltare, andra järnvägsföretag, enheter som ansvarar för underhåll, för att utveckla samarbetet och främja en övergripande förbättring av säkerhetsstyrningssystemets resultat).

För utredningar som kräver ett mänskligt och organisatoriskt perspektiv bör utredarna antingen vara utbildade i detta eller ha tillgång till lämplig sakkunskap för att kunna undersöka problemen i fråga.

7.1.4 Bevis

- *Information om rapporteringsprocessen för olyckor/tillbud, hur grundorsaker identifieras och analyseras, rapportering inom organisationen och till behöriga myndigheter och andra parter. **(7.1.1)***
- *Information om organisationens utredningsmetoder, inklusive mänskliga och organisatoriska faktorer, för att granska riskanalysen och utvärderingsprocessen efter en olycka. **(7.1.3)***
- *Bevis för att organisationen har vidtagit åtgärder till följd av de berörda myndigheternas rekommendationer utifrån rapporter om olyckor och tillbud och att eventuella nödvändiga förändringar har genomförts. **(7.1.2 a och b)***
- *Granska tidigare tillbud för att identifiera faktorer som är relevanta för nuvarande tillbud. Bevis för att organisationen lär sig mer allmänt från tillbud och andra erfarenheter, både nationellt och internationellt. **(7.1.3)***

7.1.5 Exempel på bevis

Förfarandet för utredning av olyckor som innehåller beskrivningar av utredningsmetoder och hänvisningar till kompetenshanteringskraven för olycks- och tillbudsutredare.

Exempel på olycks- och tillbudsrapporter av olika typer, som visar vilka utredningar som har gjorts av respektive behöriga personer. Resultaten är evidensbaserade, och rekommendationer efterlevs.

En kopia av förfarandet/processen för att spåra de korrigerande/riskreducerande åtgärder som identifieras efter en olycka/ett tillbud.

Information tillhandahålls gällande användandet av SAIT för att ha kontroll på sådant som rör specifika tillgångar och informera andra organisationer.

Protokoll från styrelsemöten som visar att resultaten av olyckor/tillbud och relaterade rekommendationer (dvs. korrigerande åtgärder och/eller förbättringsåtgärder) rapporteras tillbaka till ledningen, och hur de fungerar som underlag för riskstyrningssystemet **(se även 6.3)**.

Mänskliga och organisatoriska faktorer beaktas i utredningar av olyckor och tillbud. Undersökningarna har ett systematiskt perspektiv, dvs. de inriktas inte bara på de mänskliga tekniska och organisatoriska aspekterna i sig, utan betonar även samspelet mellan aktörerna. Om en tågförare till exempel har varit inblandad i ett tillbud med passerad stoppsignal bör undersökningen omfatta relevanta problem, t.ex. trötthet, kognitiv överbelastning, kompetens etc. (mänskliga faktorer), teknikens inverkan på arbetsprestationen, såsom gränssnitt mellan maskin och människa, utformning, signalernas placering (teknik), organisationens inflytande över arbetsprestationerna, såsom utbildning, säkerhetsstyrningssystemet, organisatoriska prioriteringar (organisation) samt samspelet mellan dessa tre områden, exempelvis hur upphandlingar påverkar utformningen eller hanteringen av förändringar i och med att ny design införs.

7.1.6 Referenser och standarder

- IAEA (2002) – *Safety culture in nuclear installations: Guidance for use in the enhancement of safety culture*. IAEA TECDOC-1529. Internationella atomenergiorganet, Wien (2002).
- Mathis, T.L. & Galloway, S.M. (2013) – *Steps to safety culture excellence*.
- Kecklund, L., Lavin, M. & Lindvall, J. (2016) – *Safety culture: A requirement for new business models. Lessons learned from other High-Risk Industries*. Pågående, presenterades vid den internationella konferensen på temat Human and Organisational Aspects of Assuring Nuclear Safety – Exploring 30 Years of Safety Culture, Wien, 22–26 februari 2016.
- RSSB (2015) – *Safety Culture and behavioural development: Common factors for creating a culture of continuous development* (www.sparkrail.org)

7.1.7 Tillsynsfrågor

Kompetensen hos olycks-/tillbudsutredare är avgörande för att ta fram meningsfulla rekommendationer och vidta lämpliga förebyggande åtgärder. De personer som ansvarar för tillsynen bör undersöka hur ledningen har påverkat resultaten av olycks- och tillbudsrapporter och hur detta i så fall har påverkat kvaliteten på rapporterna och eventuella relaterade åtgärder.

Organisationen har dragit lärdom av resultaten av interna utredningar, och detta framgår av dokument, rapporter eller andra informationskanaler (t.ex. intranät, personaltidningar etc.).

Organisationens kultur för rapportering av tillbud och händelser som kunde ha lett till olyckor.

7.2 Kontinuerlig förbättring

7.2.1 Reglerande krav

7.2.1.	Organisationen ska kontinuerligt förbättra säkerhetsstyrningssystemets lämplighet och ändamålsenlighet, med beaktande av den ram som anges i förordning (EU) nr 1078/2012 och minst resultaten av följande verksamhet: (a) Övervakning (se 6.1 Övervakning). (b) Internrevision (se 6.2 Internrevision). (c) Ledningens genomgång (se 6.3 Ledningens genomgång). (d) Lärdomar av olyckor och tillbud (se 7.1 Lärdomar av olyckor och tillbud).
7.2.2.	Organisationen ska, som ett led i det organisatoriska lärandet, tillhandahålla medel för att motivera personal och andra berörda parter att ta aktiv del i arbetet för att förbättra säkerheten.
7.2.3.	Organisationen ska tillhandahålla en strategi för att kontinuerligt förbättra sin säkerhetskultur, vilken ska vara baserad på användning av sakkunskap och erkända metoder för att identifiera beteenderelaterade frågor som påverkar olika delar av säkerhetsstyrningssystemet och för att införa åtgärder för att hantera dessa.

7.2.2 Syfte

Ständig förbättring är ett viktigt inslag i en effektiv säkerhetsstyrningsmetod. Syftet med detta krav är att de sökande ska visa hur de arbetar för förbättringar och att säkerhetsstyrningssystemet stöder dessa insatser.

Högsta ledningen bidrar genom en kollektiv reflektion till att kontinuerligt förbättra säkerhetskulturen i organisationen.

Denna kollektiva reflektion tar sin form i en strategi som behandlar kulturella aspekter som har en betydande inverkan på säkerhetsnivån och som behöver uppvärderas eller förändras.

7.2.3 Förklarande anmärkningar

Ständig förbättring (**7.2.1**) fokuserar på de utvärderingar som görs inom ramen för säkerhetsstyrningssystemet och de förbättringsåtgärder som blir resultatet, men inte på de områden som redan är under förbättringeftersom de redan omfattas av övervakningen.

Organisatoriskt lärande (**7.2.2**) avser processen för förbättringsåtgärder genom ökad kunskap och förbättrad förståelse.

Säkerhetskultur (**7.2.3**) avser här definitionen i punkt 2.1.1 j och den förklarande anmärkningen till denna punkt. En positiv säkerhetskultur motiverar och gör det möjligt för organisationer och individer att sträva efter att förbättra säkerheten och effektiviteten. Resultaten blir att personalen trivs med arbetet och stannar kvar, och ger dessutom kostnadsfördelar. En säkerhetskultur kan även bidra till att uppfylla lagstadgade krav, eftersom säkerhets- och tillsynsmyndigheter blir alltmer medvetna om den viktiga roll som säkerhetskulturen spelar för en effektiv hantering av säkerhetsfrågor. Mer specifikt kan en säkerhetskultur ge följande fördelar:

- *En minskning av den operativa risken genom mer omfattande riskbedömningar och förbättrad förståelse för risker hos personalen.*
- *En minskning av antalet personalolyckor genom undanröjande av faror som konstaterats via ökad rapportering av händelser som kunde ha lett till olyckor.*
- *En minskning av osäkra handlingar och förhållanden genom ökat personaldeltagande och ledarskapsutveckling.*
- *Minskade kostnader med anknytning till personalolyckor, osäkra handlingar och förhållanden.*

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.

- *Förbättrad effektivitet genom stärkt personalutbildning, ökat engagemang och minskade skador, osäkra handlingar och osäkra förhållanden.*
- *Förbättrat och mer effektivt säkerhetsstyrningssystem, med förfaranden och regler som bättre stämmer överens med verkligheten.*

De fundamentala egenskaperna i en kultur formas dagligen genom interaktion och är därför svåra att förändra. Till följd av detta bör strategin för säkerhetskultur ses som långsiktig och något som ägs av och uppmuntras av den högsta ledningen.

Det finns många sätt att förbättra säkerhetskulturen. Nedan följer några exempel:

- *Utarbetande av ett enkelt system för att dela med sig av betänkligheter rörande säkerheten. Detta kan bero på organisationens mognadsgrad. Det bör vara möjligt att vara anonym, men organisationen bör främja ökat förtroende och vara öppen och tillgänglig för alla. Det är viktigt att återkoppling matas in i systemet för att se till att personalen är delaktig och känner tillhörighet.*
- *Ändra upphandlings- och avtalsvillkor för att främja en god säkerhetskultur för leverantörer. Säkerhetskultur kan vara ett kriterium för att välja leverantörer.*
- *Tydligt belöna säkert beteende. Belöningarna kan vara olika, från ökad årslön i form av bonusar till veckovisa säkerhetspriser för utmärkta insatser.*
- *Införa särskilda mål för chefer om ledarskap i säkerhetsfrågor, till exempel att uppmuntra ledningen att spela en synligare roll genom att föregå med gott exempel.*

Säkerhetskulturen bör bedömas ur flera aspekter. Datainsamlingsmetoderna bör baseras på samhällsvetenskaplig forskning. Detta innebär att uppgifterna samlas in av en grupp av granskare som går igenom hela organisationen, med hjälp av tekniker såsom iakttagelser, dokumentanalys och intervjuer.

Bedömningsresultaten bör kommuniceras på alla nivåer i organisationen. De bör föranleda åtgärder för att främja och upprätthålla en positiv säkerhetskultur, förbättra ledarskapet i säkerhetsfrågor och främja en positiv inställning till lärande inom organisationen.

Identifiering och val av relevanta kulturella egenskaper är ofta en komplex uppgift¹ som bör utföras noggrant. Den här uppgiften bör verkligen innefatta personal på alla nivåer i organisationen och ofta utanför (till exempel entreprenörer).

Även om uppfattningar och värderingar hos personalen kan samlas in genom enkäter, bedöms en sådan metod ofta otillräcklig för att fastställa kulturella värderingar som påverkar säkerhet. Resultatet av undersökningen kan möjligen ge experter en vägledning, för att sedan kunna utföra observationer, individuella intervjuer och använda fokusgrupper, för att mer precist kunna ställa en diagnos på organisationens säkerhetskultur.

Notera: En fokusgrupp samlar ett mindre antal personer (vanligtvis mellan 4 och 15) med en moderator för att fokusera på ett specifikt ämne. Fokusgrupper uppmanar till diskussion istället för individuella svar på formella frågor och producerar därför kvalitativ data.

Baserat på diagnosen kan en handlingsplan tas fram och stödjas av den högsta ledningen, med syftet att värdera upp eller ändra kulturella egenskaper. Den högsta ledningen övervakar implementeringen av de identifierade åtgärderna och reviderar den följaktligen.

¹ Spridningen av aktiviteter och organisationens storlek är enkla exempel på parametrar som bidrar till komplexiteten för den här uppgiften.

För att säkerställa att strategin håller i längden, bör diagnosen revideras var 2-5 år med samma tillvägagångssätt. Frekvensen beror på resultatet från den ursprungliga övningen.

I flera högriskindustrier ställs ofta den här diagnosen inom en *säkerhetskulturbedömning* som leder till en handlingsplan.

Följande gäller vid en säkerhetskulturbedömning:

Bedömning av säkerhetskultur kan utföras av en oberoende part eller genom egenbedömning. Fördelen med en oberoende bedömning är att organisationen får en mer objektiv bild av säkerhetskulturen, men risken finns att organisationen blir missförstådd eller har problem att acceptera slutsatserna. Fördelen med egenbedömning är att den utförs med organisationens egen personal som har en djupgående kännedom om organisationen. Nackdelen är att status och hierarkier kan komma i vägen. Några karaktäristiska moment i en säkerhetskulturbedömning:

- *Inkluderar en 2/3-veckors bedömningsprocess och ett förberedelsestadium,*
- *Involverar ett revisionsteam med kompetens inom olika områden,*
- *Datainsamling vilar på samhällsvetenskapliga metoder (inklusive intervjuer, fokusgrupper, observationer),*
- *Bedömningens omfattning är hela organisationen och dess gränssnitt,*
- *Baserad på en säkerhetskulturmodell eller ramverk,*
- *Högsta ledningen är engagerad och ser bedömningen som en möjlighet till lärande,*
- *Resultaten sprids i hela organisationen,*
- *Resultaten tas om hand för att skapa/ändra en strategi för att löpande förbättra de valda egenskaperna inom säkerhetskultur.*

Förbättringar av strategin för mänskliga och organisatoriska faktorer och processer är en integrerad del av den ständiga förbättringen av säkerhetsstyrningssystemet.

En systematisk strategi definieras som en stegvis process för att lösa problem i samband med säkerhetskulturen. Organisationen kan till exempel ha en process för riskövervakning, tillbuds- och olycksrapportering och hur informationen används, samt dra nytta av lärdomar för ständig förbättring.

Mer information om säkerhetskultur återfinns i bilaga 4.

7.2.4 Bevis

- *Information om processen för att samla in bevis för att visa att säkerhetshanteringsmetoden ständigt förbättras. (7.2.1)*
- *Förfaranden som visar hur organisationen tar hänsyn till resultaten från övervakning, interna revisioner, granskning av ledningen och lärande från olyckor och tillbud för att förbättra säkerhetshanteringsmetoden. (7.2.1)*
- *Information om hur organisationen arbetar för att engagera personalen och andra för att förbättra säkerhetsstyrningssystemet. (7.2.2)*
- *Sökanden bör i form av en strategi ange hur säkerhetskulturen utvecklas så att de risker som kan härröras till säkerhetskultur beaktas inom säkerhetsstyrningssystemets relevanta processer. I detta sammanhang bör sökanden ange var närmare uppgifter om relevanta förfaranden finns. (7.2.3)*
- *Säkerhetskulturen bedöms löpande för att identifiera förbättringar (7.2.3)*
- *Förbättringar inom säkerhetskulturen appliceras genom PGKA-cykeln (planera, genomföra, kontrollera, agera) för att säkerställa att åtgärderna har en inverkan. Lärdomar implementeras och inverkan av implementeringen utvärderas löpande (7.2.3).*

7.2.5 Exempel på bevis

Förfarandet för övervakning, internrevision, granskningar av ledningen och olycks- och tillbudsutredningar, särskilt de delar som inriktas på relevanta lärdomar som kan inbegripas i säkerhetsstyrningssystemet.

Initiativet "Close Call" inom järnvägsnätet (www.safety.networkrail.co.uk/alerts-and-campaign/close-call), där personalen uppmuntras att aktivt informera organisationen om brister/luckor eller situationer som medför säkerhets- eller hälsorisker.

Exempel på protokoll från regelbundna fackförenings-/ledningsmöten om arbetsmiljön, som visar att situationer som bedöms vara ovissa/osäkra eller behöver övervägas närmare har diskuterats.

Resultaten från olycksutredningar rapporteras vid ledningsmöten och ses som ett viktigt verktyg för lärande och förbättring.

En kopia av strategin för förbättring av säkerhetskulturen och hur den är kopplad till de olika delarna av säkerhetsstyrningssystemet.

Strategin visar att personalen har lämplig yrkeskompetens och vid behov utbildning och erfarenhet inom de säkerhetsfrågor som ligger till grund för strategin.

Den typ av utbildning och kompetens som krävs handlar bland annat om att personalen förstår vad en säkerhetskultur innebär, hur säkerhetsresultaten mäts och arbetar för ständig förbättring. Den kritiska aspekten är att det råder en förståelse om att säkerhetskulturen är ett heltäckande koncept som påverkar alla delar av säkerhetsstyrningssystemet, och att den inte kan behandlas som en fristående faktor.

Det finns en process för att kontinuerligt utvärdera säkerhetshöjande åtgärder. Effekterna av de säkerhetshöjande åtgärderna är identifierade och praktiskt tillämpade så att de är möjliga att utvärdera.

7.2.6 Tillsynsfrågor

Inom ramen för översynen bör ledningens åtagande om ständig förbättring av säkerhetsstyrningssystemet testas genom intervjuer och dokumentanalys. Finns det en riskbaserad metod för att identifiera förbättringar, som är kopplad till känsliga och kritiska kontroller?

Om organisationen använder mognadsmodeller för att utvärdera resultaten av säkerhetsstyrningssystemet bör dessa granskas.

Bilaga 1 – Jämförelsetabeller

Nedanstående tabeller ger en direkt jämförelse mellan bedömningskraven i bilaga II till de tidigare förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010 och i bilagorna I och II till kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*]. Syftet är att underlätta övergången från det gamla säkerhetscertifieringssystemet enligt direktiv 2004/49/EG till det nya system som införs genom direktiv (EU) 2016/798.

Detta motsvarar kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] men utgör inte ett bevis på järnvägsföretagens eller infrastrukturförvaltarnas förmåga att uppfylla de relevanta kraven i säkerhetsstyrningssystemet enligt artikel 9 i direktiv (EU) 2016/798. Detaljnivån i de tidigare och de nya bedömningskraven kan fortfarande variera, även om de i viss del bygger på gemensamma principer. Alla bedömningskrav i bilagorna I och II till kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] motsvarar inte heller de tidigare förordningarna. Detta innebär att järnvägsföretag och infrastrukturförvaltare måste visa att de uppfyller de nya kraven (eller delar av dem) på andra sätt.

De krav enligt säkerhetsstyrningssystemet i bilagorna I och II till kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*] som inte motsvarar kraven i förordning (EU) nr 1158/2010 och/eller förordning (EU) nr 1169/2010 ska anses utgöra nya krav. I detta avseende ska sökanden lämna ytterligare bevis för att dessa krav uppfylls. I de flesta fall finns det inga exakta motsvarigheter mellan kriterierna i de tidigare förordningarna och kraven i den nya förordningen om gemensamma säkerhetsmetoder. I dessa fall baseras jämförelsen på syftet med kraven. Kraven kan också ha gjorts mer uttryckliga i kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*], samtidigt som syftet är detsamma. I sådana fall ska kraven i den förordningen inte anses utgöra nya krav, utan kan användas av de olika parterna som hjälp för att förstå vilka bevis som sökanden förväntas lämna.

Järnvägsföretag och infrastrukturförvaltare som vill utveckla ett integrerat ledningssystem kan också få information om motsvarigheten till ISO:s högnivåstruktur (HLS).² Att ett ledningssystem är certifierat enligt någon av systemstandarderna (t.ex. ISO 9001, ISO 14001 eller ISO 45001) utgör inte heller ett bevis på järnvägsföretagens eller infrastrukturförvaltarnas förmåga att uppfylla de relevanta kraven i säkerhetsstyrningssystemet enligt artikel 9 i direktiv (EU) 2016/798.

Tabell 1: Direkt jämförelse – Bedömningskriterier/krav som är gemensamma för järnvägsföretag/infrastrukturförvaltare

<i>Förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) nr 2018/762 Krav</i>	<i>ISO HLS Avsnitt nr</i>	<i>Kommentar</i>
A.1	3.1.1.1	6.1	
A.2	3.1.1.1	6.1	

² ISO-/IEC-direktiv, del 1, konsoliderat supplement 2016, bilaga SL tillägg 2.

<i>Förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) nr 2018/762 Krav</i>	<i>ISO HLS Avsnitt nr</i>	<i>Kommentar</i>
A.3	6.1.1	9.1	
A.4	3.1.1.1 (e)	Ej tillämpligt	
A.5	4.4 4.5.1.1	7.4	
A.6	6.1.1 5.4.1	9.1 8.1	
B.1	5.2.4	Ej tillämpligt	Underhåll är en fas i tillgångens livscykel.
B.2	5.2.4	Ej tillämpligt	Underhåll är en fas i tillgångens livscykel.
B.3	2.3.1 4.2.1	5.3 7.2	Definition och ansvarsfördelning för underhåll behandlas huvudsakligen i punkt 2.3.1. Den kompetens som krävs för underhåll behandlas huvudsakligen i punkt 4.2.1.
B.4	6.1.1 5.2.5	9.1 7.4	Uppgiftsinsamling (fel, defekter) och analys ingår i övervakningsprocessen. Uppgiftsutbytet mellan de personer som ansvarar för den dagliga driften och dem som ansvarar för underhållet ingår i informations- och kommunikationsprocessen för tillgångsförvaltning.
B.5	6.1.1	Ej tillämpligt	Anges i artikel 4.2 i den gemensamma säkerhetsmetoden om övervakning.
B.6	6.1.1	9.1	Utvärdering av prestationerna och resultaten av underhållet ingår i övervakningsprocessen för underhåll.
C.1	5.3.2 (a) 5.3.3 (a)	8.1	
C.2	5.3.3 (a)	8.1	
C.3	5.3.2 (b)	Ej tillämpligt	
C.4	5.2.5 (b) 5.3.2 (c)	Ej tillämpligt	
C.5	5.3.2 (c) 5.3.3 (a)	Ej tillämpligt	
D.1	3.1.1.1 (a)	Ej tillämpligt	
D.2	3.1.1.1 (c)	Ej tillämpligt	

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.

<i>Förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) nr 2018/762 Krav</i>	<i>ISO HLS Avsnitt nr</i>	<i>Kommentar</i>
D.3	6.1.1	Ej tillämpligt	
E.1	1.1.1 (a) 1.1.1 (b)	4.1	
E.2	4.5.1.1 (a)	4.4	
E.3	4.5.1.1 (c)	7.5.1	
E.4	4.5.1.1 (a) 4.5.1.1 (b)	7.5.1	
F.1	4.5.1.1 (a)	4.4	
F.2	2.3 4.5.1.1 (a)	5.3 4.4	
F.3	2.3.1 2.3.4	Ej tillämpligt	
F.4	4.5.1.1 (a) 4.2.1 2.3.1 2.3.2 2.3.3	4.4 5.3	Definitionen av säkerhetsrelaterade uppgifter ingår i beskrivningen av säkerhetsstyrningssystemet, inklusive ansvarsfördelning. Ansvarsuppgifter definieras för varje relevant roll inom säkerhetsstyrningssystemet.
G.1	4.5.1.1 (a) 2.3.1	4.4 5.3	Definitionen av säkerhetsrelaterade uppgifter ingår i beskrivningen av säkerhetsstyrningssystemet, inklusive ansvarsfördelning. Ansvarsuppgifter definieras för varje relevant roll inom säkerhetsstyrningssystemet.
G.2	6.1.1 6.2.1	9.1 9.2	Syftet med internrevisioner är att kontrollera om organisationen uppfyller de tillämpliga kraven.
G.3	2.1.1 (d)(i) 2.3.2	Ej tillämpligt	
G.4	2.3.1	5.3	
G.5	4.1.1	7.1	Notera att det finns en länk här till kriteriet i 1158/2010 N2(d)
H.1	2.4.1	Ej tillämpligt	
H.2	(struket)	Ej tillämpligt	Personal som arbetar med säkerhetsrelaterade uppgifter bör delta i utformningen, underhållet och förbättringen av säkerhetsstyrningssystemet. Det är organisationen som genomför krav 2.4.1 på ett sådant sätt att efterlevnaden kan kontrolleras.
I	7.2.1	10.1 10.2	

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.

<i>Förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) nr 2018/762 Krav</i>	<i>ISO HLS Avsnitt nr</i>	<i>Kommentar</i>
J	2.2.1	5.2	
K.1	3.2.1 3.2.2 (d)	6.2	
K.2	3.2.2 (a)	6.2	Säkerhetsmålen bör överensstämma med säkerhetspolicyn, som i sin tur bör vara anpassad till järnvägsverksamhetens typ och omfattning.
K.3	3.2.4	6.2	Säkerhetsmålen begränsas inte till de gemensamma säkerhetsmål som fastställs av medlemsstaterna.
K.4	6.1.1 5.4	9.1 8.1	
K.5	3.2.4 (anpassad)	9.1	En hänvisning till övervakningsstrategin och planerna enligt den gemensamma säkerhetsmetoden om övervakning.
L.1	6.1.1 5.4	9.1 8.1	
L.2	4.2 4.4 4.5 5.2.2 (a)	Ej tillämpligt	Kravet att använda kompetent personal, förfaranden, specifika dokument och rullande materiel hanteras inom kompetens, information och kommunikation, dokumenterad information respektive tillgångsförvaltning.
L.3	1.1.1 (e) 6.1.1 6.1.2	4.3 9.2	Efterlevnaden av de tillämpliga kraven behandlas utförligt i punkt 3.1.2.2 (inte specifik för underhåll). Övervakning säkerställer att förfarandena tillämpas på ett korrekt sätt. Internrevision säkerställer att förfarandena överensstämmer med de tillämpliga kraven.
M.1	3.1.2.1 5.4.1	6.1 8.1	Enligt ISO ska förändringar först planeras, vilket inbegriper identifiering och bedömning av risken, och därefter genomföras.
M.2	3.1.2.1	Ej tillämpligt	
M.3	5.4.1	8.1	
N.1	4.2.1	7.2	
N.2	4.5.1.1 (a) 2.3.1 2.3.2 2.3.4 6.1.1	Ej tillämpligt	

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.

<i>Förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) nr 2018/762 Krav</i>	<i>ISO HLS Avsnitt nr</i>	<i>Kommentar</i>
O.1	4.4.1 4.4.2 4.4.3	7.4	
O.2	4.4.3	7.4	
O.3	4.4.1	Ej tillämpligt	
P.1	4.4.3	Ej tillämpligt	
P.2	4.5.2 4.5.3	7.5.2 7.5.3	
P.3	4.5.3	7.5.3	
Q.1	7.1.1	10.1	
Q.2	7.1.2	Ej tillämpligt	
Q.3	7.1.3	10.2	
R.1	5.5.1	Ej tillämpligt	
R.2	5.5.2	Ej tillämpligt	
R.3	5.5.3	Ej tillämpligt	
R.4	5.5.4	Ej tillämpligt	
R.5	5.5.5	Ej tillämpligt	
R.6	5.5.1	Ej tillämpligt	
R.7	5.5.6	Ej tillämpligt	
S.1	6.2.1	9.2	
S.2	6.2.1 (a)	9.2	
S.3	6.2.1 (b)	9.2	
S.4	6.2.1 c–f	9.2	
S.5	6.2.1 (g) 6.3.1	9.3	

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.

<i>Förordningarna (EU) nr 1158/2010 och (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) nr 2018/762 Krav</i>	<i>ISO HLS Avsnitt nr</i>	<i>Kommentar</i>
S.6	6.2.1	9.2	

Nedanstående tabell ger en direkt jämförelse mellan de tidigare bedömningskriterierna och de nya kraven enligt säkerhetsstyrningssystemet som endast gäller järnvägsföretag.

Tabell 2: Direkt jämförelse – Bedömningskriterier/krav som är specifika för järnvägsföretag

<i>Förordning (EU) nr 1158/2010 Kriterium</i>	<i>Förordning (EU) 2018/762 Bilaga I Krav</i>	<i>ISO HLS Avsnitt nr</i>	<i>Kommentar</i>
R.8	5.5.7	Ej tillämpligt	
R.9	5.5.8	Ej tillämpligt	

Nedanstående tabell ger en direkt jämförelse mellan de tidigare bedömningskriterierna och de nya kraven för säkerhetsstyrningssystem som endast gäller infrastrukturförvaltare.

Tabell 3: Direkt jämförelse – Bedömningskriterier/krav som är specifika för infrastrukturförvaltare

<i>Förordning (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) 2018/762 Bilaga II Krav</i>	<i>ISO HLS Ref.nr</i>	<i>Kommentar</i>
R.8	5.5.7	Ej tillämpligt	
R.9	5.5.8	Ej tillämpligt	
T.1	5.2.1	Ej tillämpligt	Säker konstruktion och installation av infrastruktur ingår i tillgångens livscykel.
T.2	3.1.2 5.4.1	Ej tillämpligt	Identifiering av tekniska förändringar av infrastrukturen behandlas huvudsakligen i punkt 3.1.2. Hantering av tekniska förändringar av infrastrukturen behandlas huvudsakligen i punkt 5.4.1.
T.3	3.1.2	Ej tillämpligt	Efterlevnad av tillämpliga regler för konstruktion av infrastruktur behandlas huvudsakligen i punkt 3.1.2.

<i>Förordning (EU) nr 1169/2010 Kriterium</i>	<i>Förordning (EU) 2018/762 Bilaga II Krav</i>	<i>ISO HLS Ref.nr</i>	<i>Kommentar</i>
U.1	5.1.1 5.1.3	Ej tillämpligt	Hantering av infrastrukturens säkerhet behandlas huvudsakligen i punkt 5.1.1.
U.2	5.1.1	Ej tillämpligt	Hantering av säkerheten vid infrastrukturens fysiska och/eller operativa gränser behandlas huvudsakligen i punkt 5.1.1.
U.3	5.1.3 (c) 5.5.7	Ej tillämpligt	Hantering av normal och försämrad drift behandlas huvudsakligen i punkt 5.1.3 c.
U.4	5.1.2 5.2.3	Ej tillämpligt	
V.1	5.2.4 6.1.1	Ej tillämpligt	Underhåll av infrastruktur behandlas huvudsakligen i punkt 5.2.4. Revisioner och inspektioner (i förekommande fall) ingår i övervakningen.
V.2	5.2.4	Ej tillämpligt	Underhåll av infrastruktur behandlas huvudsakligen i punkt 5.2.4.
V.3	5.2.3	Ej tillämpligt	
W.1	5.1.3	Ej tillämpligt	
W.2	5.1.1	Ej tillämpligt	Hantering av säkerheten vid trafikkontroll- och signalsystemens fysiska och/eller operativa gränser behandlas huvudsakligen i punkt 5.1.1.
W.3	5.1.2 5.2.3	Ej tillämpligt	

Nedanstående tabell ger en direkt jämförelse mellan ISO HLS och de nya kraven för säkerhetsstyrningssystem.

Tabell 4: Direkt jämförelse – ISO:s högnivåstruktur

<i>ISO HLS Ref.nr</i>	<i>Förordning (EU) 2018/762 Krav- id</i>	<i>Kommentar</i>
4.1	1.1.1 (a) 1.1.1 (b)	
4.2	1.1.1 (c) 1.1.1 (d)	
4.3	1.1.1 (e) 1.1.1 (f)	
4.4	4.5.1.1 (a)	
5.1	2.1	
5.2	2.2	

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.

<i>ISO HLS Ref.nr</i>	<i>Förordning (EU) 2018/762 Krav- id</i>	<i>Kommentar</i>
5.3	2.3	
6.1	3.1.1 3.1.2	Den gemensamma säkerhetsmetoden om riskbedömning tillämpas för att fastställa om en förändring är säkerhetsrelaterad (eller ej) och om den är betydande (eller ej). Den "virtuella" åtskillnad som ISO gör mellan den strategiska nivån (ISO HLS avsnitt 6) och den taktiska nivån (ISO HLS avsnitt 8) i planeringen omprövas med hänsyn till EU:s regelverk och särskilt tillämpningen av ovanstående gemensamma säkerhetsmetod (oavsett förändringarnas art).
6.2	3.2.1 3.2.2 (a) 3.2.2 (d) 3.2.4	
7.1	4.1	
7.2	4.2	
7.3	4.3	
7.4	4.4	
7.5.1	4.5.1	
7.5.2	4.5.2	
7.5.3	4.5.3	
8.1	5.1 5.2 5.3 5.4 5.5	Enligt ISO:s vägledande dokument (N360) är avsikten med avsnitt 8 i ISO HLS att ange de krav som måste genomföras inom organisationens verksamhet för att säkerställa att kraven på styrningssystemen är uppfyllda och se till att prioriterade risker och möjligheter behandlas. Dessutom anges det att ytterligare krav (disciplinspecifika) relaterade till operativ planering och kontroll kan föreskrivas. I detta avseende överensstämmer kraven i 5.X med ISO:s metod, särskilt att de inte är skadliga för företagets affärsverksamhet men ger en tillräcklig ram för att kontrollera hur viktiga säkerhetsfrågor hanteras inom organisationens affärsprocesser.
9.1	6.1	Begreppet "övervakning" avser den övervakningsram som anges i den gemensamma säkerhetsmetoden om övervakning, och har därför en bredare betydelse än begreppet övervakning, mätning, analys och utvärdering, som definieras i avsnitt 9.1 i ISO HLS.

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.

<i>ISO HLS Ref.nr</i>	<i>Förordning (EU) 2018/762 Krav- id</i>	<i>Kommentar</i>
9.2	6.2	Interna revisioner betraktas som övervakningsverktyg inom ramen för den gemensamma säkerhetsmetoden om övervakning. Även om detta är ett separat krav är syftet att uppnå övervakningsmålen enligt den gemensamma säkerhetsmetoden om övervakning.
9.3	6.3	
10.1	7.1	
10.2	7.2	

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.

Bilaga 2 – Ömsesidigt godkännande av tillstånd, erkännanden eller intyg för produkter eller tjänster som beviljas enligt EU-lagstiftningen

Den myndighet som utfärdar gemensamma säkerhetsintyg eller säkerhetstillstånd kan ta hänsyn till intyg som utfärdats av andra organ, såsom ISO:s organ för bedömning av överensstämmelse, för att undvika dubbla bedömningar och extrakostnader för sökanden. Ansvaret för att fatta det slutliga beslutet ligger alltid hos den utfärdande myndigheten.

När det gäller bedömningar av ansökningar om gemensamma säkerhetsintyg ska den utfärdande myndigheten enligt artikel 3.12 i genomförandeförordning (EU) 2018/763 godta tillstånd, erkännanden eller intyg för produkter eller tjänster som tillhandahålls av järnvägsföretag eller deras entreprenörer, partner eller leverantörer och som beviljats enligt berörd EU-lagstiftning, som bevis på järnvägsföretagets förmåga att uppfylla de motsvarande kraven för säkerhetsstyrningssystemet för den berörda produkt- eller tjänstetypen. Även om det inte finns någon motsvarande bestämmelse i EU-lagstiftningen om bedömning av ansökningar om säkerhetstillstånd, uppmuntras även de nationella säkerhetsmyndigheterna att tillämpa samma princip.

I nedanstående tabell beskrivs de olika fall som finns hittills i EU:s regelverk, med illustrativa exempel på typer av produkter eller tjänster som kan omfattas av varje fall.

Tabell 5: Tillstånd, erkännanden eller intyg för produkter eller tjänster som beviljas enligt EU-lagstiftningen

<i>Fall</i>	<i>Typ av produkt eller tjänst</i>	<i>Tillämplig EU-lagstiftning</i>	<i>Förordning (EU) 2018/762 Krav-id</i>	<i>Kommentar</i>
ECM-certifikat	Underhåll av fordon	Artikel 14.4 i direktiv (EU) 2016/798	5.2 5.3	I de fall som anges i artikel 14.4 i direktiv (EU) 2016/798 utgör intyg från enheter som ansvarar för underhåll och underhållsverkstäder tillräckliga bevis på att järnvägsföretag genom sitt säkerhetsstyrningssystem har förmåga att kontrollera risker i samband med underhåll av godsvagnar, även godsvagnar som används av entreprenörer.

<i>Fall</i>	<i>Typ av produkt eller tjänst</i>	<i>Tillämplig EU-lagstiftning</i>	<i>Förordning (EU) 2018/762 Krav-id</i>	<i>Kommentar</i>
Erkännande	Utbildning av lokförare	Direktiv 2007/59/EG Beslut nr 2011/765/EU	4.2.2	Utbildningscentrum ska erkännas av den behöriga myndigheten för att kunna tillhandahålla utbildningskurser för verksamma och blivande lokförare enligt direktiv 2007/59/EG. Utbildningscentrum spelar en viktig roll för att säkerställa att lokförare har kompetens för de säkerhetsrelaterade uppgifter som de anvisas. I detta avseende bör utbildningscentrumen ha kompetens för den utbildning de tillhandahåller. Erkännande från en behörig myndighet bör i förekommande fall beaktas av säkerhetscertifieringsorganet och den nationella säkerhetsmyndigheten i deras bedömning av kompetenshanteringssystemet.
Förarbevis och kompletterande intyg för lokförare	lokförarnas kompetens och lämplighet	Direktiv 2007/59/EG	4.2.1	Förarbevis och kompletterande intyg som utfärdas enligt direktiv 2007/59/EG utgör ett tillräckligt bevis för lokförarens kompetens och lämplighet. Detta utgör dock inget hinder för organisationen att visa att dess rutiner för kompetens och lämplighet är tillräckliga.

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.

<i>Fall</i>	<i>Typ av produkt eller tjänst</i>	<i>Tillämplig EU-lagstiftning</i>	<i>Förordning (EU) 2018/762 Krav-id</i>	<i>Kommentar</i>
Gemensamt säkerhetsintyg	Underhåll och inspektion av infrastruktur Växling Provning av rullande materiel	Artikel 10 i direktiv (EU) 2016/798	5.3	Infrastrukturförvaltare kan lägga ut underhållet eller inspektionen av infrastrukturen på entreprenad till företag som använder specialfordon på spåren. Växling eller testning av operatörer kan även krävas för att erhålla ett säkerhetsintyg. I ovanstående fall utgör det gemensamma säkerhetsintyget tillräckligt bevis för att järnvägsföretag och infrastrukturförvaltare genom sina säkerhetsstyrningssystem har förmåga att kontrollera riskerna om de anlitar entreprenörer och leverantörer.
Tillstånd för utsläppande på marknaden/godkännande av fordon (typ)	Godkännande av fordon (typ)	Direktiv (EU) 2016/797	5.2	Godkännande av fordon (typ) säkerställer att fordonet genom konstruktion, tillverkning, kontroll och validering överensstämmer med de grundläggande kraven i all tillämplig lagstiftning (inklusive säkerhet), så att fordonet kan användas på ett säkert sätt i alla järnvägsnät som det är avsett för enligt de begränsningar och villkor för användningen som anges i fordonets/fordonstypens tekniska specifikationer.

I specifika fall kan det krävas mer än att inneha ett intyg (eller motsvarande) som beviljats enligt EU-lagstiftningen för att kontrollera alla säkerhetsrisker i samband med de produkter som levereras till eller de tjänster som används av järnvägsföretag eller infrastrukturförvaltare.

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.

Järnvägsföretag i partnerskap behåller till exempel hela ansvaret för en säker drift, och följaktligen för att kontrollera risker i samband med sin verksamhet, inklusive tillhandahållande av underhåll av fordon. Om ett järnvägsföretag använder en partners säkerhetscertifikat för att kontrollera risker i samband med underhållet är detta inte tillräckligt om det inte ges stöd i form av avtalsvillkor med de andra järnvägsföretagen i partnerskapet. Dessa avtalsvillkor måste utformas gemensamt och övervakas av varje partner, och ingår även i varje partners säkerhetsstyrningssystem, vilket i sin tur innebär att de övervakas av de respektive nationella säkerhetsmyndigheterna.

Det gemensamma säkerhetsintyget kan därför användas för att kontrollera riskerna i samband med tillhandahållande av underhåll och för att uppfylla kraven på kontroll av risker i samband med underhåll av fordon när följande tre villkor är uppfyllda:

1. *Det måste finnas gällande avtalsvillkor mellan järnvägsföretagen i partnerskapet som omfattar aspekter i samband med underhåll, såsom följande:*
 - a) *Informationsutbyte enligt artikel 5 i förordning (EU) nr 445/2011.*
 - b) *Tekniskt stöd vid behov, särskilt för kvarvarande system för trafikstyrning och signalering.*
 - c) *Kontroll av att de underhållsverkstäder som anlitas har kapacitet för att tillhandahålla det underhåll som krävs.*
 - d) *Effektiv övervakning av fordon och utbyte av relevant information om övervakningen.*
2. *Avtalsvillkoren utformas på grundval av resultaten av riskbedömningen och måste övervakas regelbundet av varje järnvägsföretag mot den gemensamma säkerhetsmetoden om övervakning (förordning (EU) nr 1078/2012). Övervakningsresultaten utbyts därefter formellt mellan de båda järnvägsföretagen i partnerskapet.*
3. *Båda järnvägsföretagens säkerhetsstyrningssystem innehåller lämpliga processer och förfaranden för att uppfylla villkoren i punkterna 1 och 2 ovan.*

I andra fall kan nationell lagstiftning kräva att ett behörigt organ (t.ex. den nationella säkerhetsmyndigheten) ska utfärda ett nationellt intyg (eller motsvarande) för en viss typ av produkt eller tjänst. Intyget kan även användas som bevis för järnvägsföretagens eller infrastrukturförvaltarnas förmåga att uppfylla de relevanta kraven i kommissionens delegerade förordning (EU) 2018/762 [*gemensamma säkerhetsmetoder för krav på säkerhetsstyrningssystem*]. Nationella intyg som beviljas till enheter som ansvarar för underhåll och/eller underhållsverkstäder för andra fordon än godsvagnar kan även ge rimlig försäkras, liknande intyget för enheter som ansvarar för underhåll, om att de fordon som de ansvarar för att underhålla är driftsäkra.

Bilaga 3 – sidospår, avtalsvillkor och partnerskap

Sidospår

I detta dokument avser "sidospår" järnvägsinfrastruktur som är ansluten till ett järnvägsnät som faller inom en järnvägsförvaltares ansvar (dvs. infrastrukturdelen av järnvägssystem som omfattas av direktiv (EU) 2016/798). Sidospår kan ingå i järnvägsnätet eller inte, beroende på hur varje medlemsstat har införlivat detta direktiv.

Verksamheter som bedrivs på sidospår, till exempel lastning av vagnar, är industriverksamheter som har samband med specifika järnvägsverksamheter, såsom sammansättning, förberedelse och flyttning av fordonssätt som kan fungera som tåg eller användas på tåg. Det kan bland annat handla om att koppla ihop olika fordon så att de bildar fordons- eller tågsätt och sedan flytta dem.

Sidospår kan vara (men är inte begränsade till)

- *infrastruktur som används för att parkera järnvägsfordon när de inte används,*
- *intermodala terminaler,*
- *infrastruktur som används för tjänster på personfordon, såsom rengöring eller lättare underhåll,*
- *infrastruktur som tillhör och förvaltas av en underhållsverkstad för järnvägsfordon,*
- *industriområden eller industrianläggningar för lastning/urlastning av godsvagnar.*

Verksamheter på sidospår utförs av en "sidospårsoperatör". En sidospårsoperatör kan vara ett järnvägsföretag, en infrastrukturförvaltare, en tjänsteleverantör (t.ex. rengöring av personfordon), en industriorganisation (t.ex. en kemisk anläggning som lastar/lastar ur tankvagnar) eller en underleverantör till industriorganisationen. I det första fallet har organisationen fattat ett affärsbeslut att bli ett järnvägsföretag eller är redan detta, som planerar att bedriva verksamhet på sidospår förutom sin befintliga järnvägsverksamhet. I det senare fallet förvaltar infrastrukturförvaltaren sidospåren eller agerar som ett järnvägsföretag enligt sitt säkerhetstillstånd.

"Sidospårsleverantören" kontrollerar arbetsmiljörisker genom sitt arbetsmiljösystem, som har införts enligt internationell och nationell lagstiftning. Om sidospårsoperatören inte är ett järnvägsföretag omfattar förvaltningssystemet de arbetsmiljökrav som gäller för extern personal, särskilt från järnvägsföretag, till exempel när tågförare kör in på sidospåret. Parallellt med detta kontrollerar järnvägsföretaget arbetsmiljörisker genom sitt arbetsmiljösystem, som har införts enligt internationell och nationell lagstiftning.

Fall 1: Sidospårsoperatören är järnvägsföretaget "Y".

Genom sitt säkerhetsstyrningssystem kontrollerar järnvägsföretaget riskerna i samband med sin järnvägsverksamhet i infrastrukturen för sidospår och på järnvägsnätet på infrastrukturförvaltarens ansvar. Kontrollen omfattar risker i samband med skador på fordon som orsakats av någon av de verksamheter som bedrivs på sidospåret, inklusive sammansättning, förberedelse och drift av tåg.

I praktiken är det ibland svårt att avgöra vilket järnvägsföretag som är ansvarigt. Ett tåg som tillhör järnvägsföretaget "X" anländer till exempel till ett sidospår (föraren och lokomotivet är inhyrda), och järnvägsföretaget "Y", som driver sidospåret, tar över som ett nytt tåg (föraren och lokomotivet är inhyrda), samtidigt som sidospårsverksamheter måste genomföras. I sådana fall gäller ovanstående säkerhetsprinciper. Det finns gemensamma gränssnittsrisker som måste beaktas i järnvägsföretag Y:s säkerhetsstyrningssystem (t.ex. skador på fordon till följd av sidospårsverksamheter som lastning). Dessutom måste information utbytas om fordonet från järnvägsföretag X till järnvägsföretag Y. Det handlar bland annat om att det är nödvändigt att kontrollera att fordonet är driftsäkert när järnvägsföretag X överför det till sidospårsoperatören och när det överförs vidare via järnvägsföretag Y. Järnvägsföretag Y, som ansvarar för

sidospårsverksamheten, behåller hela ansvaret för att kontrollera riskerna i samband med underhåll som utförs på sidospåret.

Fall 2: Sidospårsoperatören är inte ett järnvägsföretag

Fyra delfall kan övervägas:

- **Delfall 2.1** – Sidospårsoperatören är infrastrukturförvaltare.
- **Delfallen 2.2 och 2.3** – Sidospårsoperatören är inte en infrastrukturförvaltare och bedriver endast verksamhet på sin egen infrastruktur, men inte på järnvägsnätet på infrastrukturförvaltarens ansvar.
- **Delfall 2.4** omfattar järnvägsverksamhet som bedrivs av en sidospårsoperatör, som inte är infrastrukturförvaltare, på järnvägsnätet på infrastrukturförvaltarens ansvar.

Delfall 2.1: När verksamheterna på sidospår är gemensamma mellan järnvägsföretag och infrastrukturförvaltare (eller en organisation som agerar för dess räkning) måste varje järnvägsföretag informeras om alla säkerhetsrelaterade händelser som har inträffat inom ramen för den verksamhet som infrastrukturförvaltaren bedriver enligt avtal. Detta inkluderar skador, olyckor och tillbud med fordon inblandade.

Avtalsvillkoren förvaltas via varje järnvägsföretags säkerhetsstyrningssystem och infrastrukturförvaltarens säkerhetsstyrningssystem.

Genom sitt säkerhetsstyrningssystem kontrollerar järnvägsföretaget riskerna i samband med den egna verksamheten i förhållande till den information som mottas.

Delfall 2.2: Sammansättningen och förberedelserna av tåget sköts av järnvägsföretaget (hopkoppling, förberedelser) på sidospårsinfrastrukturen. Järnvägsföretaget måste informeras om alla (säkerhets)händelser som har inträffat inom ramen för sidospårsoperatörens verksamhet (t.ex. lastning eller rengöring) genom avtalsvillkor. Detta inkluderar skador, olyckor och tillbud med fordon inblandade.

Avtalsvillkoren förvaltas via järnvägsföretagets säkerhetsstyrningssystem.

Genom sitt säkerhetsstyrningssystem kontrollerar järnvägsföretaget riskerna i samband med sina efterföljande verksamheter i förhållande till den information som mottas.

Delfall 2.3: Sammansättningen av tåget sköts helt/delvis av sidospårsoperatören eller av en organisation som arbetar för sidospårsoperatörens räkning.

När tågsättet har satts samman överförs det till järnvägsföretaget.

Precis som i delfall 2.2 måste järnvägsföretaget informeras om alla (säkerhets)händelser som har inträffat inom ramen för sidospårsoperatörens verksamhet (t.ex. lastning eller rengöring) och under sammansättningen av tågsättet genom avtalsvillkor. Sådana händelser inkluderar skador, olyckor och tillbud med fordon inblandade.

Avtalsvillkoren förvaltas via järnvägsföretagets säkerhetsstyrningssystem.

Genom sitt säkerhetsstyrningssystem kontrollerar järnvägsföretaget riskerna i samband med den egna verksamheten i förhållande till den information som mottas.

Delfall 2.4: Detta delfall kompletterar delfall 2.3. Här beskrivs därför endast järnvägsföretagets ytterligare skyldigheter i detta sammanhang.

Sidospårsoperatören kör tåg eller flyttar fordon i tågsätt från sin järnvägsinfrastruktur till järnvägsnätet på infrastrukturförvaltarens ansvar.

Till exempel:

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.

- *Sidospårsoperatören flyttar tåg eller tågsätt från en servicebangård till plattformarna på en persontågsstation eller till en parkeringsbangård i anslutning till persontågsstationen.*
- *Sidospårsoperatören flyttar tåg eller tågsätt från en industrianläggning till en transiteringspunkt (transiteringssidospår) i anslutning till godsstationen.*

Sidospårsoperatören är varken ett järnvägsföretag eller en infrastrukturförvaltare, men verksamheter som genomförs i en infrastrukturförvaltares nät måste omfattas av ett gemensamt säkerhetsintyg eller ett säkerhetstillstånd.

De järnvägsverksamheter som genomförs av sidospårsoperatören i järnvägsnätet på en infrastrukturförvaltares ansvar omfattas antingen av ett järnvägsföretags gemensamma säkerhetsintyg eller en infrastrukturförvaltares säkerhetstillstånd. Detta innebär att järnvägsföretaget eller infrastrukturförvaltaren måste kontrollera riskerna i samband med de verksamheter som genomförs av sidospårsoperatören, via avtalsvillkoren om underleverantörer enligt deras säkerhetsstyrningssystem.

Järnvägsföretaget och infrastrukturförvaltaren måste noggrant beskriva omfattningen av sina järnvägsverksamheter och verksamheter som gränsar till andra järnvägsverksamheter så att de nationella säkerhetsmyndigheterna kan utöva effektiv tillsyn. För att säkerställa effektivitet i säkerhetsstyrningssystemet och de nationella säkerhetsmyndigheternas tillsyn är det mycket viktigt att järnvägsföretagen och infrastrukturförvaltarna tydligt och utförligt beskriver sina verksamheter och andra verksamheter som gränsar till järnvägsverksamheter.

Avtalsvillkoren för samtliga delfall måste innehålla (men är inte begränsade till) följande:

- *Vad varje part i avtalet ska göra.*
- *Förväntad kvalitet på produkter/tjänster.*
- *Fördelning av roller och ansvarsområden.*
- *Vilken information samt när och hur informationen utbyts mellan parterna i avtalet. Informationen omfattar rapportering av händelser enligt beskrivningen i delfallen och de särskilda egenskaperna hos sidospårsinfrastruktur, såsom hastighetsbegränsningar, viktgränser eller lutningsförhållanden.*
- *Kompetenskrav.*
- *Arbetsmiljökrav (enligt riskbedömningar, nationella krav etc.).*

Avtalsvillkor och partnerskap

Järnvägsföretaget ansvarar för att se till att tåget är driftsäkert genom att samordna och styra järnvägsverksamheten. Avtalsöverenskommelser (som vanligen består av ramavtal, specialavtal och bilagor) utgör grunden för ett effektivt samarbete mellan olika järnvägsföretag, vare sig de är nya eller etablerade, och måste uppfylla lagstiftning på EU-nivå och nationell nivå samt andra tillämpliga krav.

Järnvägsföretaget måste därför kontrollera riskerna i samband med verksamheten, vilket omfattar samarbete med partner och användning av (under)leverantörer. Den nationella säkerhetsmyndigheten kontrollerar därefter att järnvägsföretaget uppfyller sina rättsliga skyldigheter på ett öppet och korrekt sätt.

Järnvägsföretag kan inte delegera sitt säkerhetsansvar för att samordna och säkerställa en säker drift av tågen. Järnvägsföretagen kan dock samarbeta i dessa frågor. Dessa grundläggande principer gäller även för samarbete mellan järnvägsföretagen. Det järnvägsföretag som bär ansvaret för en säker drift av tågen måste tydligt anges i alla avtal mellan parterna, och måste ha ett gemensamt säkerhetsintyg. Järnvägsföretaget förvaltar antingen resurserna (personal, fordon) direkt via sitt säkerhetsstyrningssystem, eller kan besluta att (helt eller delvis) lägga ut användningen av resurserna (t.ex. leasing av fordon, anställning av lokförare) på en annan part. I det senare fallet har järnvägsföretaget enligt [förordning \(EU\) nr 1078/2012](#) fortfarande ansvar

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.

för att övervaka riskerna i samband med användning av (under)leverantörer genom sitt säkerhetsstyrningssystem. Det måste därför kontrollera att resurserna uppfyller rättsliga krav och andra tillämpliga säkerhetskrav (t.ex. att fordonen är driftsäkra, att linjen är kompatibel, personalutbildning, att lokförarna har giltiga licenser och intyg för en viss linje).

Ett gemensamt säkerhetsintyg som ett certifieringsorgan har utfärdat (och som därför övervakas av en nationell säkerhetsmyndighet) till avtalsparten (dvs. antingen partnern eller underleverantören) kan ge det järnvägsföretag som ansvarar för driftsäkerheten tillräcklig försäkran om att säkerhetsstyrningssystemet uppfyller de relevanta kraven. Avtalsvillkoren omfattar överföring av relevant säkerhetsinformation (t.ex. tågförarnas tidigare vilotider) mellan parterna i avtalet.

Principerna för samarbetet mellan järnvägsföretag är desamma, oavsett samarbetsformer, dvs. partnerskap eller utläggande på entreprenad (helt eller delvis) av järnvägsverksamheter eller gränsöverskridande verksamheter. Typen och omfattningen av de åtgärder som järnvägsföretagen ska vidta och i hur stor utsträckning den nationella säkerhetsmyndigheten ska övervaka samarbetet beror dock på graden av järnvägsföretagens samarbetsarrangemang.

Gränsöverskridande samarbete mellan järnvägsföretag (dvs. användning av externa fordon och/eller extern personal) kräver sannolikt mer kontroll än andra samarbetsarrangemang eftersom verksamheten läggs över på ett annat järnvägsföretag som använder andra språk och tillämpar andra regler för driften av rullande materiel, som kan skilja sig mellan medlemsstaterna. Att hyra in externa tågförare eller fordon kräver naturligtvis mindre övervakning, och därför mindre tillsyn från den nationella säkerhetsmyndighetens sida.

Bilaga 4 – Säkerhetskultur

Inledning till säkerhetskultur och strategin för förbättring av säkerhetskultur

En kultur skapas genom samspelet mellan människor i vardagen och bidrar till att fastställa förväntat beteende och samhällsnormer. Kultur är ett komplicerat begrepp med många faktorer, som utvecklas över tiden beroende på omständigheter, förhållanden och nationens, statens, samhällets och/eller organisationens erfarenheter.

Begreppet säkerhetskultur avser de kulturella faktorer som särskilt handlar om säkerhet. Det är visserligen möjligt att beskriva vissa av de faktorer som bidrar till en säkerhetskultur, men det är omöjligt att samla in all information som detta begrepp omfattar. Det finns inget gemensamt vetenskapligt och objektivt sätt att mäta en säkerhetskultur. Det beror på att de bidragande faktorerna varierar, inte bara mellan organisationer, utan även inom dem. Olika avdelningar har olika säkerhetskrav och säkerhetsbehov, till exempel operativa och finansiella, och den rådande säkerhetskulturen utvecklas utifrån dessa. Externa faktorer som rättsliga krav, utbildningsnivå, samhällsstrukturer och den nationella kulturen bidrar också till organisationens säkerhetskultur.

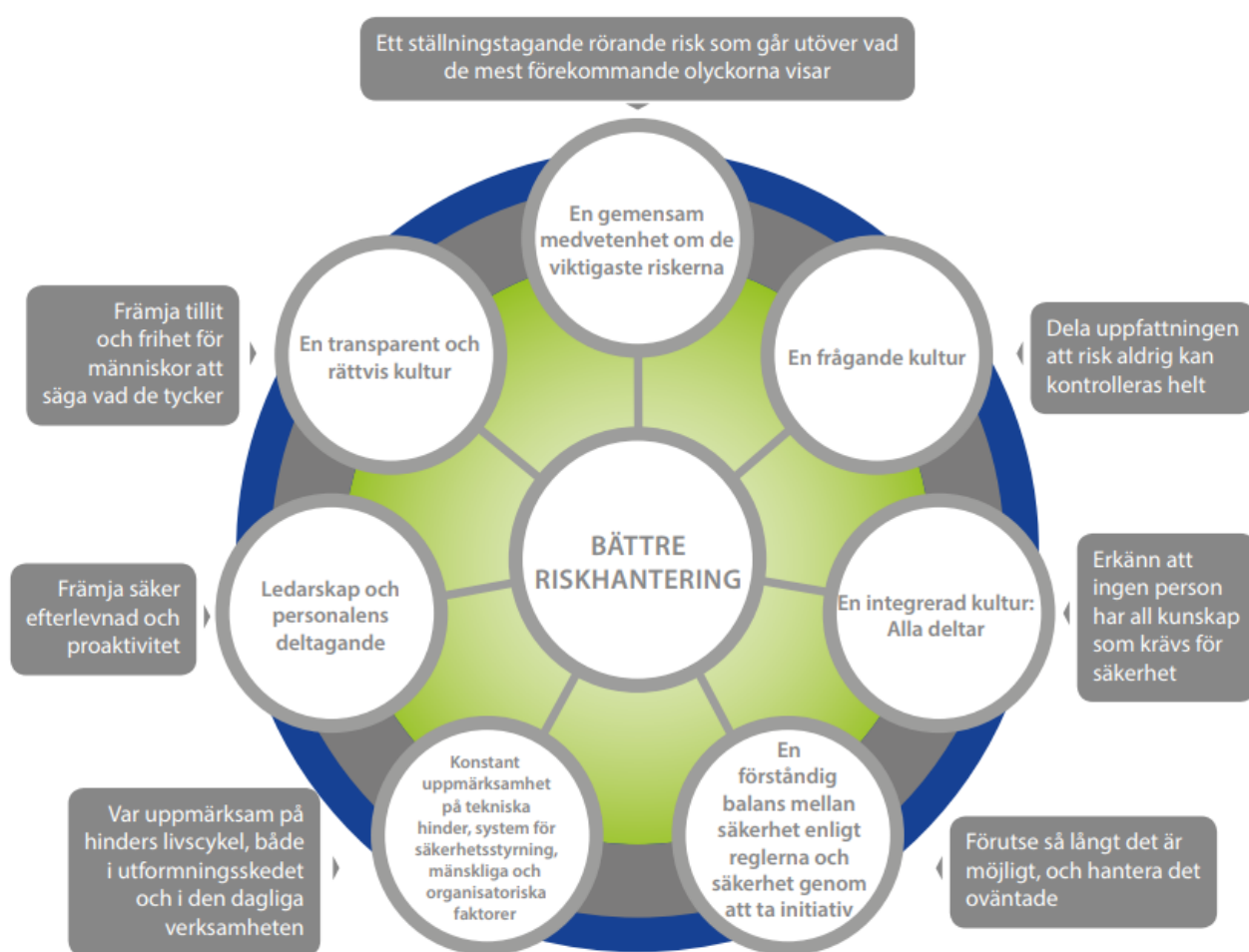
Säkerhetskultur är ett etablerat begrepp, men det finns ingen etablerad definition. Avsaknaden av en definition har lett till att den teoretiska diskussionen och den praktiska tillämpningen i viss mån har glidit isär, och det som främst är en social företeelse har omvandlats till egenskaper hos en god säkerhetskultur.

Ett rakt sätt att beskriva säkerhetskultur är därför att titta på de faktorer som inverkar på beteende. Säkerhetsstyrningssystemet utgör grunden för säkerhetskulturen, eftersom den via riktlinjer och förfaranden definierar och föreskriver vad som krävs. I en utopi skulle säkerhetsstyrningssystemet vara perfekt och följas av ledning och personal. En utopi är dock en utopi, och det som händer är att ledningen och personalen försöker förstå innehållet i säkerhetsstyrningssystemet utifrån sina värderingar, attityder och övertygelser, som de i sin tur har fått från sin personliga erfarenhet av arbetsplatsens och samhällets beteendennormer. Om säkerhetsstyrningssystemet är rimligt och det finns en efterlevnadskultur leder detta till korrekt beteende. Om så inte är fallet görs individuella tolkningar och alternativa lösningar används. Dessa grundas på en individuell riskbedömning som väger faktorer som påverkar de beslut som fattas. Riskbedömningen inriktas inte bara på den faktiska risken, utan omfattar även faktorer som rör bekvämlighet, risken att upptäckas, ledningens uttalanden och åtgärder etc. Det inbördes sambandet mellan säkerhetsstyrningssystemets logik och det resulterande beteendet definierar därför säkerhetskulturen.

För att mäta en säkerhetskultur krävs insikt i dessa tre faktorer och deras inbördes förhållanden. Som sagt finns det inget gemensamt vetenskapligt och objektivt sätt att mäta en säkerhetskultur. Egenskaper som påverkar säkerhetskulturen kan dock analyseras mot bakgrund av dessa tre faktorer.

En riktlinje som "Säkerheten först" kan till exempel följas upp genom att man undersöker vad detta egentligen innebär för de anställda – tror de faktiskt på det, sätter ledningen verkligen handling bakom orden, hur fattas besluten och på vilka grunder, hur reagerar organisationen under press etc. Andra faktorer kan undersökas på liknande sätt, till exempel kontinuerligt lärande och en ifrågasättande inställning. En kombination av analysresultaten ger en bild av kulturens status. Med tiden kan en mer heltäckande bild byggas upp, som möjliggör mer handfasta slutsatser.

För att förstå säkerhetskulturen i en organisation har specialister och forskare utarbetat modeller som vanligtvis inbegriper en uppsättning egenskaper inom en positiv säkerhetskultur. I figur 4 visas ett exempel på en sådan modell, som baseras på det senaste arbetet i Institute for an Industrial Safety Culture (ICSI).



Figur 4: Inslag i en säkerhetskultur

Baserat på ISCI-modellen kan ett samband påvisas mellan de flesta av säkerhetsstyrningssystemets inslag och de dominerande inslagen i en säkerhetskultur, vilket visas i tabell 6.

Tabell 6: Förhållande mellan kraven i säkerhetsstyrningssystemet och inslagen i en säkerhetskultur

Inslag i säkerhetsstyrningssystemet	CSM SMS krav	Inslag i en säkerhetskultur
Ledarskap och åtaganden	2.1	<ul style="list-style-type: none"> • Frågeställande kultur • En transparent och rättvis kultur • Ledarskap och personalens deltagande
Säkerhetspolicy	2.2	Ledarskap och personalens deltagande
Struktur och skyldigheter	2.3	Integrerad kultur (alla är delaktiga)
Personalens och andra parter deltagande	2.4	<ul style="list-style-type: none"> • En transparent och rättvis kultur • Integrerad kultur (alla är delaktiga) • Ledarskap och personalens deltagande

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.

<i>Inslag i säkerhetsstyrningssystemet</i>	<i>CSM SMS krav</i>	<i>Inslag i en säkerhetskultur</i>
Riskbedömning	3.1	<ul style="list-style-type: none"> En gemensam medvetenhet om de viktigaste riskerna Konstant uppmärksamhet på tekniska hinder, system för säkerhetsstyrning, mänskliga och organisatoriska faktorer En förnuftig balans mellan säkerhet enligt reglerna och säkerhet genom att ta initiativ
Säkerhetsmål och planering	3.2	-
Resurser	4.1	Integrerad kultur (alla är delaktiga)
Kompetens	4.2	<ul style="list-style-type: none"> En transparent och rättvis kultur Integrerad kultur (alla är delaktiga)
Medvetenhet	4.3	En gemensam medvetenhet om de viktigaste riskerna
Information och kommunikation	4.4	En transparent och rättvis kultur
Dokumenterad information/dokumentation över säkerhetsstyrningssystemet	4.5	Konstant uppmärksamhet på tekniska hinder, system för säkerhetsledning, mänskliga och organisatoriska faktorer
Integration av mänskliga och organisatoriska faktorer (HOF)	4.6	-
Operativ verksamhet	5.1	<ul style="list-style-type: none"> En gemensam medvetenhet om de viktigaste riskerna Frågeställande kultur En förnuftig balans mellan säkerhet enligt reglerna och säkerhet genom att ta initiativ
Förvaltning av tillgångar	5.2	En gemensam medvetenhet om de viktigaste riskerna
Entreprenörer, partner och leverantörer	5.3	<ul style="list-style-type: none"> En transparent och rättvis kultur Integrerad kultur (alla är delaktiga)
Förändringshantering	5.4	-
Hantering av nödsituationer	5.5	En förnuftig balans mellan säkerhet enligt reglerna och säkerhet genom att ta initiativ
Övervakning	6.1	Frågeställande kultur
Internrevision	6.2	-
Ledningens granskning	6.3	-
Förbättring/Lära från olyckor och tillbud	7.1	<ul style="list-style-type: none"> Frågeställande kultur En transparent och rättvis kultur
Ständig förbättring	7.2	<ul style="list-style-type: none"> Frågeställande kultur En transparent och rättvis kultur

För mer information om ISCI-modellen hänvisas till institutets webbplats (<http://www.icsi.eu.org>).

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.

Ett exempel på en strategi för att förbättra säkerhetskulturen i ett större företag inom järnvägen: PRISME-programmet implementerat hos SNCF, Frankrike

Efter en rad allvarliga järnvägsolyckor och på varandra följande arbetsplatsolyckor gjorde SNCF 2014 en storskalig enkätundersökning, med stöd av den verkställande direktören, med målet att förstå hur personalen uppfattade säkerhet.

”Frågeformuläret utformades efter konsultation med 20 fokusgrupper mellan april och maj 2014. Alla aktiviteter och alla nivåer i organisationen har tagits i beaktan.

”...För att garantera konfidentialitet har enkätundersökningen genomförts av ett oberoende institut. Undersökningen följde normen ISO 20252, var baserad på CAWI (en intervjuteknik som är datorbaserad och genomförs via ett internetformulär) och tillgänglig via privat dator, smarttelefon eller platta.”

”Fokusgrupperna gav väldigt värdefull information. Särskilt behovet att förenkla dokumentationen identifierades genom fokusgrupperna.”

Det här initiativet visade sig vara framgångsrikt då fler än 53 000 av 150 000 anställda svarade på undersökningen.

En samstämmig bild växte fram ur undersökningen som betonade behovet av att arbeta för dialog och främja rapportering från alla anställda. En nödvändig faktor identifierades för att löpande kunna förbättra säkerhet: en djup kulturell förändring som stödjer proaktiva attityder på alla nivåer i företaget, till skillnad från ett reaktivt förhållningssätt till individuella händelser.

Som en följd av detta förband sig högsta ledningen till att implementera en övergripande företagspolicy för säkerhet. Policyn siktar på att nå den högsta säkerhetsnivån och visar att säkerhet står högst på listan av företagsvärderingar samtidigt som den belyser att säkerhet är ett oundgängligt medel för att uppnå de bästa resultaten i verksamheten.

En arbetsgrupp på styrelsenivå skapade en ambitiös handlingsplan som baserades på undersökningen och en ytterligare så kallad benchmarking. Handlingsplanen benämndes PRISME som bestod av sex element. En undersökning som gjordes i november 2015 visade att dessa element hade identifierats som ”viktigt” eller ”mycket viktigt” av 93% av personalen.

Elementen är följande:

- *Utveckla ett proaktivt (Proactive) beteende för att lära från fel och problem,*
- *upprätta ett system baserat på riskanalys (Risk) som förväntar, identifierar och prioriterar åtgärder,*
- *ha kontroll över gränssnitten (Interfaces) för att undvika att endast se till sin egen avdelning och därmed samarbeta bättre,*
- *förenkla (Simplify) processerna, dokumentationen och driftlägen och anpassa dem till arbetet i praktiken för att skapa större effektivitet,*
- *skapa en gynnsam miljö för ledningen (Managerial) så att alla blir personligen engagerade för att reducera olycksrisken till den lägsta möjliga nivån,*

- *införskaffa verktyg och innovativ utrustning (Equipment) för att tillhandahålla moderna arbetsmetoder till alla, en säker miljö och ett säkert nätverk.*

Inom PRISME har följande konkreta åtgärder implementerats:

- *Endagars utbildning i mänskliga och organisatoriska faktorer för 8000 ledare,*
- *utveckling och främjande av en opartisk och rättvis kultur,*
- *förstärkning av verktyg för kommunikation och spridning av information (2 månaders säkerhet, indikatorer, säkerhetsnotiser),*
- *revision av säkerhetsstyrningssystemet och säkerhetsregler,*
- *förbättring av riskanalys för att bättre fånga systemaspekter.*

Programmets effektivitet håller för närvarande på att utvärderas, men flera fördelar har redan identifierats:

- *Förbättrad kvalitet på olycksutredningar med hänsyn på organisationsfaktorer,*
- *förbättrad rapportering av tillbud och problem från de anställda,*
- *förbättrad kommunikation,*
- *ledningens beteende uppfattas som mer stödjande och proaktiv av de anställda.*

Bilaga 5 – Integrering av mänskliga och organisatoriska faktorer

Introduktion till mänskliga och organisatoriska faktorer

Mänskliga och organisatoriska faktorer (HOF) är ett tvärvetenskapligt område som inriktas på åtgärder för att höja säkerheten, förbättra resultaten och öka kundnöjdheten. Det är en användarcentrerad strategi, vilket innebär att den utformas utifrån en uttrycklig förståelse av användare, arbetsuppgifter och förhållanden. Utgångspunkten är alltid användarens förmågor och begränsningar och hur dessa påverkas av och samverkar med de system som användaren använder i arbetet. Målet är att ta reda på det bästa sättet att utföra en uppgift på ett säkert och effektivt sätt. Betoningen ligger på användarvänlighet. Mänskliga och organisatoriska faktorer är ett proaktivt sätt att säkerställa bra konstruktionsprocesser och ett reaktivt sätt att identifiera de viktigaste problemen när något går fel.

Vid konstruktion av nya fordon är det till exempel inte tillräckligt att bara tillämpa konstruktionsstandarder. Förare, ombordpersonal och underhållspersonal bör göras delaktiga så att de kan tillföra sin erfarenhet och förståelse av hur uppgifterna kan utföras på ett säkert och effektivt sätt. Det kan till exempel handla om problem med vissa stationer eller linjer, tillgänglighet och tillträde för underhållsarbete, uppgiftsprioriteringar i förarhytten, kommunikationskrav eller passagerarnas beteende på stationerna.

Det effektivaste sättet att införliva olika operatörers kunskap och erfarenhet är genom en återkommande process där användarna kontinuerligt utvärderar tågets konstruktion och utveckling under arbetets gång. Detta bidrar till att förebygga ett vanligt fel i konstruktionsprocessen, nämligen att fokusera på människans samspel med individuella system i stället för arbetsuppgiften i allmänhet. Leverantörerna har till exempel olika idéer om hur larm bör prioriteras, och utan ett heltäckande perspektiv blir användaren ofta överöst med information med begränsad relevans för den uppgift som ska utföras. Att den tekniska konstruktionen gör det möjligt att visa informationen innebär inte att användaren har användning för den. En analys av mänskliga och organisatoriska faktorer bidrar till att göra åtskillnad mellan behovet av kunskap och sådant som bara är trevligt att ha.

Detta tillvägagångssätt omfattar ett systematiskt perspektiv, dvs. det inriktas inte bara på de mänskliga tekniska och organisatoriska aspekterna i sig, utan betonar även samspelet mellan de olika aktörerna. Om en tågförare till exempel har varit inblandad i en incident med passerad stoppsignal, bör undersökningen bland annat omfatta (ej uttömmande lista) trötthet, kognitiv överbelastning, kompetens etc. (mänskliga faktorer), teknikens inverkan på arbetsprestationen, såsom gränssnitt mellan maskin och människa, utformning, signalernas placering (teknik), organisationens inflytande över arbetsprestationerna, såsom utbildning, säkerhetsstyrningssystemet, organisatoriska prioriteringar (organisation) samt samspelet mellan dessa tre områden, exempelvis hur upphandlingar påverkar utformningen eller hanteringen av förändringar i och med att ny utformning införs.

Metoderna kommer från många olika områden, till exempel experimentell psykologi, industriteknik, organisationspsykologi, sociologi, ledningsvetenskap, kognitiv teknik, ergonomi, datavetenskap och säkerhetsteknik. Eftersom analysen av mänskliga och organisatoriska faktorer inriktas på användaren, är uppgiftsanalys en vanlig metod. En uppgiftsanalys hjälper konstruktören att förstå de uppgifter som ska utföras och hur de anknyter till de system som användaren samverkar med och de organisatoriska förhållanden som påverkar arbetsresultaten. Baserat på uppgiftsanalysen kan ytterligare analyser göras, till exempel av samspelet mellan människa och maskin, arbetsbelastning, människans tillförlitlighet, antropometri och biometrisk analys. Det viktigaste är att säkerställa att användaren har bästa möjliga förhållanden för ett säkert och effektivt arbete.

Följande litteraturhänvisningar ger ytterligare information om mänskliga och organisatoriska faktorer:

- *Salvendy, G. (2012). Handbook of Human Factors and Ergonomics. New Jersey: Wiley & Sons. ISBN-13: 978-0470528389*

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.

- *Wickens, C.D., Lee, J.D., Liu, Y & Gordon Becker, S.E (2004). An Introduction to Human Factors Engineering. New Jersey: Pearson Education. ISBN-13: 978-0131837362*

Strategi för att stödja integreringen av mänskliga och organisatoriska faktorer i säkerhetsstyrningssystemet

Organisationen bör ha en strategi för att säkerställa att kunskap om mänskliga faktorer, metoder och en människocentrerad metod systematiskt och konsekvent tillämpas på alla relevanta processer i organisationen. Detta innebär att man först överväger människornas behov, förmågor och beteenden och att utformningen därefter anpassas till dessa behov, förmågor och beteenden.

Strategin för mänskliga och organisatoriska faktorer kan innehålla följande:

Ledarskap

- *Ledarskap och åtaganden*
 - *Ledningens åtagande gentemot strategin för mänskliga och organisatoriska faktorer anges tydligt i riktlinjer och mål.*
 - *Det finns en process/riktlinjer som visar hur mänskliga och organisatoriska faktorer bör tillämpas i projekt.*
 - *Strategin för mänskliga och organisatoriska faktorer är en integrerad del av konstruktionsprocessen och projektledningen.*
- *Säkerhetspolicy*
 - *Säkerhetspolicyn anger tydligt att ett perspektiv med mänskliga och organisatoriska faktorer bör tillämpas i alla säkerhetsrelaterade processer.*
- *Organisatoriska roller, skyldigheter, ansvarsområden och befogenheter*
 - *Tydligt definierade roller, ansvar- och redovisningsskyldigheter för den person som ansvarar för strategin för mänskliga och organisatoriska faktorer.*
 - *Det finns riktlinjer för HOF-experters regelbundna deltagande i projekt och processer.*

Planering

- *Åtgärder för riskhantering*
 - *En beskrivning av hur mänskliga och organisatoriska faktorer övervägs i riskanalyser.*
 - *HOF-experters deltar i riskanalyser.*

Stöd

- *Resurser och kompetens*
 - *En systematisk metod för att säkerställa att det finns kompetens på området mänskliga och organisatoriska faktorer inom relevanta roller, baserat på en behovsanalys.*
 - *Tid och resurser anslås för att se till att kraven angående mänskliga och organisatoriska faktorer uppfylls.*
- *Medvetenhet*
 - *Allmän kunskap inom organisationen om den systematiska metoden för att säkerställa kompetens i mänskliga och organisatoriska faktorer i relevanta roller.*

Drift

- *Operativ planering och kontroll*
 - *Mänskliga och organisatoriska faktorer beaktas i verksamhetsplaneringen.*
- *Förvaltning av tillgångar*
 - *Organisationen har riktlinjer för att tillämpa en människocentrerad strategi i alla skeden av tillgångens livscykel.*
- *Beskrivning av förändringen*

- *Mänskliga och organisatoriska faktorer ska alltid bedömas som ett led i processen för hantering av förändringar.*

Resultatutvärdering

- *Övervakning*
 - *Säkerhetsnivån bedöms systematiskt mot säkerhetsstrategin.*

Förbättring

- *Lära från olyckor och tillbud*
 - *Kunskap om och metoder för mänskliga och organisatoriska faktorer används i olycksutredningar.*
 - *Det finns en metod för att genomföra undersökningar baserat på kunskap om och metoder för mänskliga och organisatoriska faktorer.*
 - *Det finns ett utbildningsprogram för olycks- och tillbudsutredare som omfattar mänskliga och organisatoriska faktorer.*
- *Ständig förbättring*
 - *En process för ständig förbättring av organisationens processer för att hantera mänskliga och organisatoriska faktorer.*

Bilaga 6 – Definitioner

Användningen av ord eller begrepp som ”måste”, ”bör” eller ”ska” i dokumentet anger att det finns rättsliga krav, som ska följas.

Olycka	En oönskad eller ouppståtlig plötslig händelse, eller en viss följd av sådana händelser, som får skadliga följder; olyckor indelas i följande kategorier: kollisioner, urspårningar, plankorsningsolyckor, personolyckor som inbegriper rullande materiel i rörelse, bränder och övriga olyckor (direktiv (EU) 2016/798).
Område för verksamheten	Ett eller flera nät i en eller flera medlemsstater där ett järnvägsföretag avser att bedriva trafik (direktiv (EU) 2016/798).
Förvaltning av tillgångar	Det tillvägagångssätt som organisationen använder för att säkerställa att fysiska tillgångar är säkra, ändamålsenliga och kommersiellt användbara, från design och konstruktion, genom tillgångens livscykel och fram till bortskaffande.
Revision	Systematisk, oberoende och dokumenterad process för att erhålla bevis och utvärdera dem objektivt för att fastställa i vilken utsträckning kraven har uppfyllts (ISO 9000).
Typ av verksamhet	Karakteriseringen av verksamheten genom dess omfattning, inklusive design och konstruktion av infrastruktur, underhåll av infrastruktur, trafikplanering, trafikstyrning och kontroll samt användningen av järnvägsinfrastrukturen, inklusive konventionella linjer eller höghastighetslinjer, passagerar- eller godstransport.
Kompetens	Förmåga att tillämpa kunskap och färdigheter för att uppnå de avsedda resultaten (ISO 9000).
Ständig förbättring	Återkommande verksamhet för att förbättra resultaten (dvs. mätbara resultat) (ISO 9000).
Dokumenthantering	Process (eller förfarande) för att identifiera, skapa, underhålla, hantera, lagra och behålla dokumenterad information.
Verksamhetens omfattning	Den omfattning som kännetecknas av passagerarantal och/eller godsvolym samt uppskattad storlek på ett järnvägsföretag efter antalet anställda inom järnvägssektorn (dvs. som mikroföretag, små företag, medelstora företag eller stora företag) (direktiv (EU) 2016/798). När det gäller järnvägsverksamhet som bedrivs av infrastrukturförvaltare, den omfattning som kännetecknas av längden på järnvägsspåren och infrastrukturförvaltarens uppskattade storlek räknat i antalet anställda inom järnvägssektorn (förordning (EU) 2018/762 [<i>gemensamma säkerhetsmetoder för säkerhetsstyrningssystem</i>]).
Fara	Ett förhållande som kan leda till en olycka (förordning (EU) nr 402/2013).
Mänskliga och organisatoriska faktorer	Alla egenskaper hos människors prestationer och organisatoriska aspekter som måste övervägas för att säkerställa att systemet eller organisationen alltid är säkra och effektiva.
Människocentrerat synsätt	Ett synsätt där man tar hänsyn till människornas behov, förmågor och beteenden och utformningen därefter anpassas till dessa behov, förmågor och beteenden.

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.

Tillbud	Händelse som inte utgör en olycka eller allvarlig olycka men som påverkar eller kan påverka järnvägsdriftens säkerhet (direktiv (EU) 2016/798). Detta omfattar händelser som kunde ha lett till olyckor.
Infrastrukturförvaltare	Varje organ eller företag som särskilt ansvarar för att anlägga, förvalta och underhålla järnvägsinfrastruktur, inklusive trafikledning, trafikstyrning och signalering. Infrastrukturförvaltarens uppgifter med avseende på järnvägsnät eller del av ett järnvägsnät får tilldelas olika organ eller företag (direktiv 2012/34/EU).
Berörd part	Person eller organisation som kan påverka, påverkas av eller uppleva att de blir påverkade av ett beslut eller en aktivitet (ISO 9000) i samband med säkerhetsstyrningssystemet.
Utredning	En process som genomförs i syfte att förebygga olyckor och tillbud och som omfattar insamling och analys av information, slutsatser, däribland fastställande av orsaker och, i förekommande fall, utformning av säkerhetsrekommendationer (direktiv (EU) 2016/798).
Ledningssystem	En uppsättning sammanhängande eller interagerande element i en organisation som anger riktlinjer och mål och en strategi för att nå de målen (ISO 9000).
Övervakning	De rutiner som införs av järnvägsföretag, infrastrukturförvaltare eller enheter som ansvarar för underhåll för att kontrollera att deras ledningssystem tillämpas korrekt och är effektiva (förordning (EU) nr 1078/2012).
Nationella regler	Alla bindande regler som antagits i en medlemsstat, oavsett vilket organ som har utfärdat dem, och som innehåller andra järnvägssäkerhetsrelaterade eller tekniska krav än dem som anges i unionsbestämmelser eller internationella regler, vilka i den medlemsstaten är tillämpliga på järnvägsföretag, infrastrukturförvaltare eller tredje parter (direktiv (EU) 2016/798).
Process	En uppsättning sammanhängande eller interagerande element som omvandlar tillförda faktorer (input) till en resulterande verkan (output) (ISO 9000).
Järnvägsinfrastruktur	Utrustning som är nödvändig för att en järnväg ska fungera, bland annat <ul style="list-style-type: none"> • järnvägsspår och spårstrukturer, • servicevägar, signalsystem, kommunikationssystem, rullande materiel, • kontrollsystem, tågkontrollsystem och datahanteringssystem, • meddelanden och skyltar, • elförsörjning och elektriska framdrivningssystem, • byggnader, verkstäder, depåer och bangårdar, och • anläggningar, maskiner och utrustning.

Järnvägsföretag	<p>Ett järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, samt andra offentliga eller privata företag vars verksamhet består i att tillhandahålla gods- och/eller persontrafik på järnväg med krav på att företaget måste tillhandahålla dragkraft; här innefattas även företag som endast tillhandahåller dragkraft (direktiv (EU) 2016/798).</p> <p>Varje offentligt eller privat företag med tillstånd i enlighet med detta direktiv vars huvudsakliga verksamhet består i att tillhandahålla tjänster för transport av gods och/eller passagerare på järnväg med kravet att företaget måste tillhandahålla dragkraft; detta gäller även företag som endast tillhandahåller dragkraft (direktiv 2012/34/EU).</p>
Risk	Frekvensen av olyckor och tillbud som vållar skada (orsakad av en riskkälla) och graden av allvar hos denna skada (förordning (EU) nr 402/2013).
Riskanalys	Systematisk användning av all tillgänglig information för att identifiera riskkällor och uppskatta risken (förordning (EU) nr 402/2013).
Riskbedömning	Den övergripande process som innefattar en riskanalys och en riskvärdering (förordning (EU) nr 402/2013).
Riskvärdering	Ett förfarande utgående från riskanalys för att fastställa om en godtagbar risknivå har uppnåtts (förordning (EU) nr 402/2013).
Riskhantering	Systematisk användning av strategier, förfaranden och metoder för att analysera, utvärdera och kontrollera risker (förordning (EU) nr 402/2013).
Säkerhetskultur	En säkerhetskultur syftar på samspelet mellan systemet för säkerhetsledning, hur människor tolkar det baserat på sina attityder, värderingar och övertygelser, och vad de faktiskt gör, vilket visar sig i beslut och beteenden. En positiv säkerhetskultur karaktäriseras av ett kollektivt åtagande av ledare och enskilda att alltid agera på ett säkert sätt, i synnerhet när de ställs inför konkurrerande mål (förordning (EU) 2018/762 [<i>gemensamma säkerhetsmetoder för säkerhetsstyrningssystem</i>]).
Mål	<p>Resultat som ska uppnås.</p> <p>Säkerhetsmål ska vara specifika, mätbara, uppnåbara, realistiska och tidsbaserade. De måste också fastställas för relevanta funktioner och nivåer inom organisationen.</p>
Partner	En kommersiell enhet som en annan kommersiell enhet har någon form av allians med. Förhållandet kan vara avtalsbaserat, dvs. ett bindande åtagande där båda parter förbinder sig att inte gå ihop med tredje parter.
Partnerskap	Ett arrangemang där parterna, som kallas partner, kommer överens om att samarbeta till nytta för sina gemensamma intressen.
Säkerhetsstyrningssystem	Organisation, åtgärder och förfaranden som införts av en infrastrukturförvaltare eller ett järnvägsföretag för att trygga en säker verksamhet (direktiv (EU) 2016/798).
Verkställande ledning	Person eller grupp av personer som leder och kontrollerar en organisation på högsta nivå (ISO 9000).

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.

Verksamhetstyp	Den typ som kännetecknas av persontrafik, inklusive eller exklusive höghastighetstrafik, godstrafik, inklusive eller exklusive trafik med farligt gods, samt enbart växlingstjänster (direktiv (EU) 2016/798).
----------------	--