

## Veileder

### *Krav til sikkerhetsstyringssystem for sikkerhetssertifisering eller sikkerhetsgodkjenning*

	<i>Utarbeidet av</i>	<i>Validert av</i>	<i>Godkjent av</i>
<i>Navn</i>	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
<i>Stilling</i>	Prosjektleder	Prosjektleder	Enhetsleder
<i>Dato</i>	04/09/2018	04/09/2018	04/09/2018
<i>Underskrift</i>			

#### *Dokumenthistorikk*

<i>Versjon</i>	<i>Dato</i>	<i>Kommentar</i>
1.0	29/6/2018	Endelig versjon for publisering
1.1	10/7/2018	Figur 2 oppdatert, bildetekst lagt til i figur 3
1.2	04/9/2018	Figur 2 oppdatert

*Dette dokumentet er en ikke-juridisk bindende veiledning fra Den europeiske unions jernbanebyrå. Det berører ikke beslutningsprosessene som er fastsatt i gjeldende EU-lovgivning. Videre er en bindende tolkning av EU-loven den eneste kompetansen til EU-domstolen.*

## 0 Innledning

En som søker om et felles sikkerhetssertifikat eller en sikkerhetsgodkjenning skal dokumentere samsvar med de relevante kravene til sikkerhetsstyringssystemer som er fastsatt i Kommisjonens delegerede forordning (EU)

The NSA NO 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.

2018/762 [Forskrift om felles sikkerhetsmetode for sikkerhetsstyringssystemer (CSM SMS)]. Det skal legges frem dokumentasjon på at det er opprettet et sikkerhetsstyringssystem (SMS) som er i samsvar med artikkel 9 i Direktiv (EU) 2016/798 (sikkerhetsdirektivet). Dokumentasjonen skal legges frem for den nasjonale sikkerhetsmyndigheten eller, når det er relevant, Den europeiske unions jernbanebyrå (heretter kalt «Byrået»).

Denne veilederen er utarbeidet i samarbeid med nasjonale sikkerhetsmyndigheter og bransjen. Veilederen er et levende dokument som vil bli oppdatert fortløpende som følge av tilbakemeldinger fra brukere og erfaringer fra implementeringen av Direktiv (EU) 2016/798, relaterte felles sikkerhetsmetoder (CSM) og andre relevante EU-forordninger.

## 0.1 Formålet med veilederen

Denne veilederen viser:

- *Formålet med kravene i vedlegg I og II i CSM SMS, samt forklarende merknader til forskriftskravet*
- *Dokumentasjon som kan legges fram for å vise samsvar med CSM SMS*
- *Sjekkpunkter til det enkelte krav (en liste over eksempler på dokumentasjon). Denne kan brukes både når en virksomhet søker om et felles sikkerhetssertifikat eller sikkerhetstillatelse, og den kan brukes ved vurdering av søknad.*
- *Referanser og standarder som kan brukes til å vurdere, utvikle, implementere eller kontinuerlig forbedre et sikkerhetsstyringssystem*
- *Eksempler på problemstillinger som kan bli vurdert av en nasjonal sikkerhetsmyndighet under tilsyn av jernbanevirksomhet eller infrastrukturforvalter*

Merk: for søknad om sikkerhetssertifikat inkludert farlig gods, kan den nasjonale sikkerhetsmyndigheten ha en direkte rolle som den riktige myndighet for å vurdere relevante deler av søknaden. Alternativt kan det være at den nasjonale sikkerhetsmyndighet har en koordinerende rolle, og at nasjonal sikkerhetsmyndighet da ber om veiledning fra en annen relevant myndighet for farlig gods for vurdering ved behov.

## 0.2 Hvem er denne veilederen rettet mot?

Dette dokumentet er rettet mot:

- *Nasjonal sikkerhetsmyndighet og Byrået når de vurderer om jernbanevirksomheters sikkerhetsstyringssystem overholder de relevante SMS-kravene og for nasjonale sikkerhetsmyndigheter ved gjennomføring av tilsyn*
- *Nasjonal sikkerhetsmyndighet når de vurderer om infrastrukturforvalternes sikkerhetsstyringssystem overholder de relevante SMS-kravene og ved gjennomføring av tilsyn etter utstedelse av sikkerhetstillatelse*
- *Jernbanevirksomhetene (også kalt «Søker») for å bistå dem med å utvikle, implementere, vedlikeholde og kontinuerlig forbedre sikkerhetsstyringssystemet sitt i samsvar med de relevante SMS-kravene (og andre gjeldende sikkerhetskrav), og for å kjenne til hva som kan forventes under tilsyn*

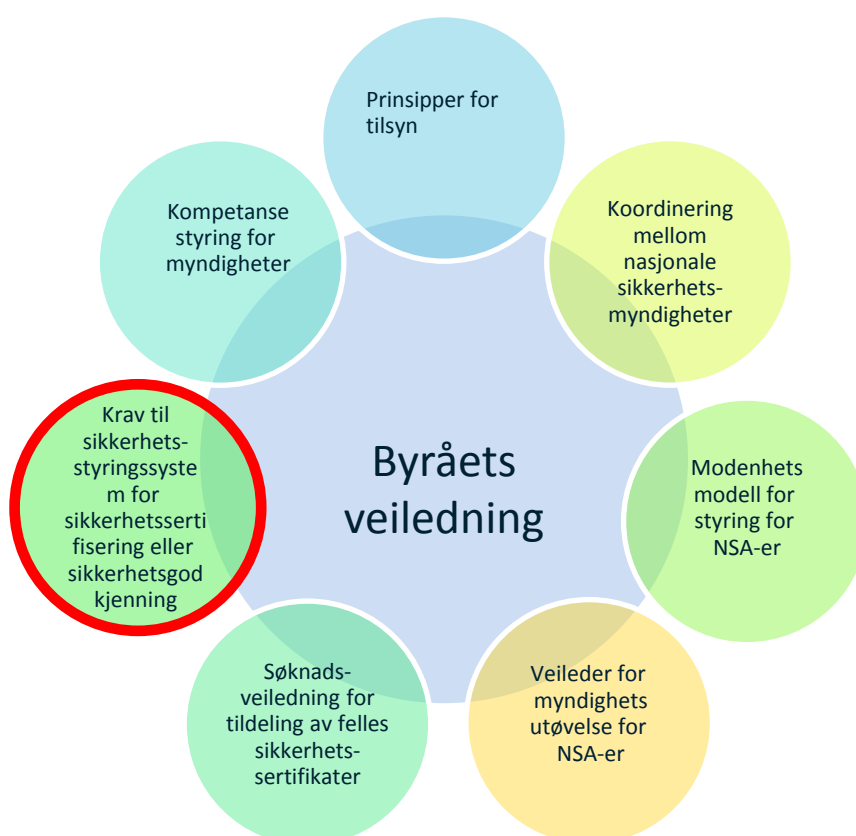
## 0.3 Omfang

Denne veilederen gir ikke fastsatt fremgangsmåte for innholdet i en virksomhets sikkerhetsstyringssystem, og gir ikke den endelige fasit over hvilken dokumentasjon som skal fremlegges av søker. Årsaken til dette er at

hver virksomhets SMS skal skreddersys for de spesifikke risikoene som virksomheten må ha kontroll på. Veilederen gir kun eksempler på dokumentasjon som skal fremvises av søkeren.

## 0.4 Veilederens struktur

Dette dokumentet er en av flere veiledere til jernbanevirksomhetene, nasjonale sikkerhetsmyndigheter og Byrådet. Veilederen skal være en hjelp til forståelse av roller og gjennomføring av oppgaver i samsvar med Direktiv (EU) 2016/798 (sikkerhetsdirektivet).



Figur 1: Byråets veiledningssamling

Informasjonen i denne veilederen skal suppleres med spesifikk veiledning fra nasjonale sikkerhetsmyndigheter. Den nasjonale veilederen beskriver og forklarer notifiserte nasjonale regler som gjelder for det tiltenkte driftsområdet, samt dokumentene som skal sendes sammen med søknaden om et felles sikkerhetssertifikat (se også *Byråets søknadsveiledning for utstedelse av felles sikkerhetssertifikater*). Den nasjonale veilederen skal også omfatte nasjonale krav som gjelder for infrastrukturforvalter ved søknad om sikkerhetstillatelse. Notifiserte nasjonale regler er kun de reglene som er notifisert av en medlemsstat til Kommisjonen. Det forventes at antall notifiserte nasjonale regler vil komme til å reduseres over tid. Disse vil enten bli erstattet av tiltak som er skissert i Tekniske spesifikasjoner for interoperabilitet (TSI), andre EU-forordninger eller virksomhetenes bestemmelser. Virksomhetenes bestemmelser eller standarder vil bli vurdert som hensiktsmessige gjennom etterlevelse av TSI-OPE (Forskrift om gjennomføring av TSI-drift og trafikkstyring på det nasjonale jernbanenettet). Etterlevelse av TSI-OPE vil reflekteres gjennom kravene til sikkerhetsstyringssystemet som er forklart i denne veilederen.

The NSA NO 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.

Denne veilederen er bygget opp etter samme struktur som vedlegg I og vedlegg II i CSM SMS. I de følgende kapitlene er hvert av kravene vist i en gul ramme som en referanse. Der det er forskjeller mellom kravene som gjelder for jernbaneforetak og kravene som gjelder for infrastrukturforvaltere, vises den relevante teksten for sistnevnte i parentes i blått.

En sammenstilling av vurderingskriteriene i tidligere Forordning (EU) 1158/2010 og (EU) 1169/2010, og kravene i Kommisjonens delegerede forordning (EU) 2018/762 [CSM SMS] er beskrevet i Vedlegg 1 til denne veilederen. Tabellene inneholder også kryssreferanser til klausulene i ISO High Level Structure der det er aktuelt. Disse er tatt med for å hjelpe søkerne til å vise at sikkerhetsstyringssystemene deres samsvarer med de nye kravene, særlig i tilfeller der søkeren allerede har fått et sikkerhetssertifikat eller sikkerhetstillatelse og/eller der søkeren allerede anvender et annet ISO-styringssystem (for eksempel ISO 9001, 14001 eller 45001) (slik at de kan integreres). Tabellene kan også brukes til hjelp ved utvikling av et sikkerhetsstyringssystem. Bruk av denne tabellen sikrer ikke automatisk etterlevelse av kravene i CSM SMS for virksomheter som er ISO-sertifisert. Ytterligere forklaringer og eksempler finnes i Vedlegg 2.

## 0.5 ISO-standarder

Den internasjonale standardiseringskomiteen (ISO) har utviklet prosedyrer som skal følges når man utvikler og opprettholder en internasjonal standard. I vedlegg SL, tillegg 2 i [ISO/IEC-direktivene del 1 og konsolidert ISO-tillegg](#) finner man en høynivåstruktur (HLS) for bruk av kjernetekst i hver enkelt styringssystemstandard.

Vedlegg I og vedlegg II i CSM SMS legger til rette for en struktur som er i samsvar med HLS. CSM SMS legger også til rette for integrering av ulike styringssystemer der det måtte være aktuelt, der styringssystemene deler de samme organisatoriske kjerneprinsippene og kravene. I et styringssystem må det også sikres etterlevelse av lovkrav som er relevant for ulike fagområder (for eksempel sikkerhet, miljø, kvalitet). I tillegg må risiko som er spesifikk for de ulike fagområder identifiseres og håndteres.

ISO-standardene og relevant veiledning kan hjelpe jernbanevirksomheter til å utvikle sine egne sikkerhetsstyringssystemer (ISO 31000 er for eksempel et generelt dokument for bedre forståelse av risikostyring, ISO 31010 inneholder informasjon om valg og anvendelse av risikovurderingsteknikker som FMECA, FTA, ETA, HAZOP, og ISO 55000 inneholder krav til forvaltning av eiendeler). Disse er imidlertid bare til hjelp hvis man har kompetanse innen jernbanerelatert risiko.

Selv om styringssystemet til en virksomhet er bygget opp etter ISO-standarder, vurderes søknader om felles sikkerhetssertifikat og sikkerhetstillatelser etter kravene i CSM SMS. For å avklare: - ISO-standardene er basert på frivillig sertifisering, men enkelte juridiske rammeverk åpner for muligheten til å anta at de er i overensstemmelse med gjeldende regler som gjelder for et bestemt fagområde. Det foreligger ingen bestemmelser som automatisk gir ISO-standardene samsvar med kravene i sikkerhetsdirektivet eller med CSM SMS.

Klausul 4 til 10.2 som er hentet fra ISO/IEC-direktiver del 1 og konsolidert tillegg 2016, vedlegg SL, tillegg 2, er gjengitt eller tilpasset med tillatelse fra ISO. Vennligst se kildedokumentet for den originale teksten. Dette dokumentet kan lastes ned fra [nettstedet til ISO Central Secretariat](#). Opphavsretten forblir hos ISO.

## 0.6 Formålet med sikkerhetsstyringssystemet

Formålet med sikkerhetsstyringssystemet er å sikre at virksomheten har kontroll på risiko som oppstår på grunn av virksomhetens aktivitet og i tråd med relevante sikkerhetsrelaterte krav.

En systematisk oppbygging av sikkerhetsstyringssystemet gjør det mulig å identifisere farer, samtidig som det muliggjør risikostyring knyttet til virksomhetens aktiviteter, med sikte på å forebygge ulykker.

---

The NSA NO 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.

Sikkerhetsstyringssystemet skal også omfatte felles risiko med andre aktører i jernbanesystemet, for eksempel jernbanevirksomheter og foretak med ansvar for vedlikehold. I tillegg vil andre aktører som har potensiell innvirkning på sikker drift av jernbanesystemet, som produsenter, vedlikeholdsleverandører, brukere, tjenesteleverandører, entreprenører, transportører, avsendere, mottakere, laste-/losseoperatører, opplæringssentre, passasjerer og tredjeperson osv., kunne være en del av virksomhetens risikobilde. Tilstrekkelig implementering av alle relevante elementer i et sikkerhetsstyringssystem kan gi en virksomhet den nødvendige tilliten til at den kontrollerer, og vil fortsette å kontrollere, alle risikoene som er forbundet med virksomheten den driver, og under alle forhold.

En moden virksomhet innser at hensiktsmessig risikostyring kun kan oppnås gjennom en prosess som bringer sammen tre kritiske komponenter, et samspill mellom menneske, teknologi og organisasjon (MTO): En teknisk komponent med bruk av verktøy og utstyr, en menneskelig komponent bestående av førstelinjepersonell og deres ferdigheter, opplæring og motivasjon, samt en organisatorisk komponent bestående av prosedyrer og metoder som definerer oppgaveforholdet.

Et godt sikkerhetsstyringssystem overvåker og forbedrer alle de tre komponentene med risikostyringstiltak. Mange funksjoner i sikkerhetsstyringssystemene for jernbanedriften er svært like styringspraksisen for helse, miljø, sikkerhet og kvalitet. Prinsippene for god styring vil derfor enklere kunne integreres ved bruk av felles sikkerhetsmetoder som er basert på HLS. Det er ikke sikkert at det er nødvendig med en fullstendig restrukturering av systemer hos virksomheter som allerede har disse på plass.

Strukturerte styringssystemer gir verdiskaping til virksomheten gjennom hensiktsmessig styring av samhandling. Dette bidrar til å forbedre den generelle ytelsen, innføre hensiktsmessighet i driften, forbedre forbindelser med leverandører og underleverandører, kunder og myndigheter, samt bidra til å bygge en positiv sikkerhetskultur.

En søker må utforme sikkerhetsstyringssystemet slik at det møter kravene i artikkel 9 i sikkerhetsdirektivet. Til dette formål må den vise samsvar med kravene i vedlegg I og II i CSM SMS. Disse kravene er utarbeidet for å danne et komplett bilde av virksomhetens sikkerhetsstyringssystem der man følger PDCA-hjulet: Plan (planlegg), do (utfør), check (kontroller/sjekk), act (korriger). Søkeren må vurdere hvert enkelt av kravene, samt hvordan de passer sammen for å danne et sammenhengende sikkerhetsstyringssystem som håndterer de relevante risikoene.

## 0.7 Sikkerhetsstyringssystem og prosesstilnærming

Sikkerhetsstyringssystemet bør integreres i virksomhetens forretningsprosesser, og skal ikke kun være et papirbasert system som er utviklet for å dokumentere samsvar med lovverket. Sikkerhetsstyringssystemet bør være dynamisk og i kontinuerlig forbedring. Sikkerhetsstyringssystemet skal følge virksomhetens utvikling. Kravene som ligger til grunn for vurderingen av et sikkerhetsstyringssystem kan oppfylles gjennom en dokumentert prosess (eller prosedyre, etc.), men det skal også integreres i og på tvers av virksomhetens ulike forretningsområder. Nasjonale sikkerhetsmyndigheter kan for eksempel sjekke at det foreligger en sikkerhetspolitikk, men de må også styre virksomhetens forpliktelse til å etterleve den. En praktisk måte å gjøre dette på, er at nasjonale sikkerhetsmyndigheter kan kontrollere hvordan sikkerhetsstyringssystemet blir overvåket og vurdert på toppledelsesnivå, hvordan personellet er involvert i dette og hvordan resultatene formidles til dem. Virksomheten har ikke nødvendigvis bestemte prosedyrer for å håndtere sikkerhetsrelevant informasjon, men den må beskrive hvordan de relevante delene i virksomheten håndterer denne informasjonen på en egnet måte (for eksempel kommunikasjon av sikkerhetsrelevant informasjon til lokomotivførere).

I CSM SMS vedlegg I og II er kravene strukturert etter prosess. Dette finner vi også igjen i ISO-standarder for styringssystemer, der de ulike prosessene i styringssystemet henger sammen. En konsekvent anvendelse av

---

The NSA NO 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.

prosessbasert styringssystem vil bidra til å oppnå virksomhetens mål. Vedlegg I og vedlegg II i CSM SMS identifiserer noen viktige koblinger mellom prosesser for å gi større forståelse av prosesstilnærmingen. Dette trenger ikke å bety at det må eksistere slike koblinger i den relevante virksomheten, eller at koblingene må dokumenteres for å vise samsvar. En virksomhets evne til å vise hvordan prosessene i styringssystemet er knyttet sammen, er en god indikator på forståelsen av hvordan styringssystemet fungerer på en hensiktsmessig måte.

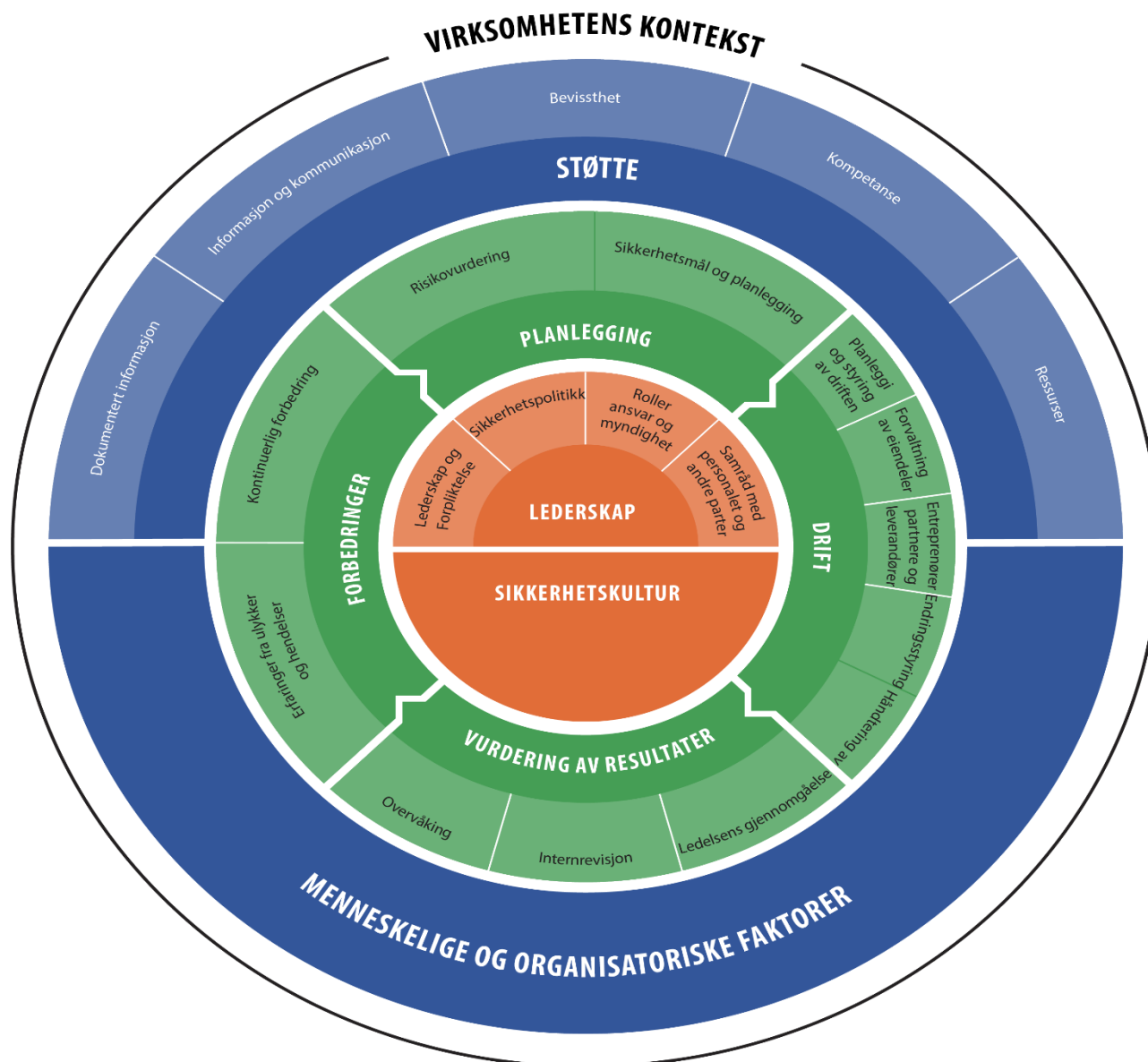
Elementene i sikkerhetsstyringssystemet kan anvendes i PDCA-hjulet: Plan (planlegg), do (utfør), check (kontroller/sjekk), act (korrigjer) (se figur 2). PDCA-konseptet gjenspeiler de funksjonelle forbindelsene mellom de viktigste elementene i sikkerhetsstyringssystemet:

- **Planlegging:** Identifisere risikoer og muligheter, fastsette sikkerhetsmessige mål og identifisere prosesser og tiltak som er nødvendige for å levere resultater i samsvar med virksomhetens sikkerhetspolitikk
- **Drift:** Utvikle, implementere og anvende prosesser og tiltak som planlagt
- **Ytelseevaluering:** Overvåke og evaluere ytelsen i implementerte prosesser og etablerte tiltak med hensyn til mål og planlegging, og rapportere resultatene
- **Forbedring:** Gjennomføre tiltak for kontinuerlig forbedring av sikkerhetsstyringssystemet og sikkerhetsnivået, for å oppnå de tilskattede resultatene

Denne kjerneprosessen utfylles med andre elementer i sikkerhetsstyringssystemet:

- «**Virksomhetens kontekst**» inneholder innspill til planleggingsfasen
- «**Ledelse**» som drivkraft for PDCA-hjulet
- Ulike «**Støtte**»-funksjoner som støtter alle elementene i sikkerhetsstyringssystemet

Vedlegg 7 skisserer en metode for å identifisere funksjonelle forbindelser mellom de ulike elementene i sikkerhetsstyringssystemet.



Figur 2: Sikkerhetsstyringssystem for jernbanedrift

## 0.8 Sikkerhetsstyringssystem og sikkerhetskultur

Sikkerhetskulturen er et sett av atferdsmønstre og tenkemåter, som i stor grad deles av en gruppe aktører i en virksomhet når det kommer til kontroll av alvorlig risiko knyttet til deres aktiviteter. Det kan eksistere flere kulturer innen en og samme virksomhet. Sikkerhetskulturen vil kunne variere med hensyn til blant annet verdier, funksjoner, roller og geografi. Sikkerhetskulturen bygges daglig ved samhandling mellom aktørene i en virksomhet.

En direkte måte å beskrive sikkerhetskulturen på er å se på faktorene som bidrar til atferden. Sikkerhetsstyringssystemet danner grunnlaget: Ved å definere arbeidsforhold og resultater, vil en virksomhet kunne identifisere arbeidsmetoder og de tekniske hjelpemidler som er nødvendig for virksomheten. For å kunne arbeide trygt, må virksomheten forutse uønskede situasjoner, og implementere regler og virkemidler

The NSA NO 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.

for å håndtere dem. I tillegg kommer virksomhetens atferdskultur: egenskaper, følelser, betydninger og forhold som påvirker samhandlingsmønstre mellom personer i virksomheten. Dette refererer hovedsakelig til de «uskrevne reglene som styrer atferd og avgjørelser hos en gruppe mennesker». Sammen bidrar den strukturelle og kulturelle delen av virksomheten til organisatorisk yteevne.

Det foreligger en risiko for at en teoretisk tilnærming til sikkerhetsstyring ikke samsvarer med virkeligheten. Dette kan gi et sikkerhetsstyringssystem som ikke virker etter hensikten, for eksempel: Hvis ressursene brukes på å utarbeide, vedlikeholde og dokumentere at man har et dokumentert system, samtidig som man ignorerer operative innspill, kan det gi et gap mellom «forestilt arbeid» og «reelt arbeid».

Sikkerhetsstyringssystemet kan likevel ha en positiv innflytelse på sikkerhetskulturen i virksomheten, og påvirke det fysiske miljøet samt de ansattes atferd på en måte som fremmer og underbygger sikkerheten.

Samsvar mellom den strukturelle og kulturelle delen av virksomheten danner grunnlaget for sikkerheten. For å bidra til at alle kan utføre oppgavene sine, må virksomheten forstå hvordan mennesker (med sine evner og begrensninger) anvender kunnskap for å løse problemer, og ta hensyn til denne kunnskapen når arbeidsmiljøet utformes. Det samme gjelder regler og forskrifter: Så lenge de ansatte som gjennomfører dem ikke blir tatt hensyn til når arbeidsprosedyrene utformes, vil de bli tvunget til å gå på akkord med reglene for å få arbeidet gjort når det oppstår inkonsekvens eller konflikter.

I dette dokumentet fremheves de grunnleggende egenskapene som er kjent for å bidra til en positiv sikkerhetskultur. Videre inneholder Vedlegg 4 grunnleggende informasjon om sikkerhetskultur, samt annen nyttig informasjon for at virksomheten kan utvikle sin egen strategi.

## 0.9 Dokumentasjon

Denne veilederen gir noen eksempler på dokumentasjon som søkeren må fremlegge ved søknad om sikkerhets sertifikat eller sikkerhetstillatelse.

Eksempelene tydeliggjør kravene, men de representerer ikke en fullstendig liste. Søkeren må beskrive hvordan hvert av kravene blir oppfylt. Saksbehandler kan be om dokumentasjon for å få avklart hvordan krav blir oppfylt. Søkeren kan fremlegge dokumentasjon for å underbygge hvordan kravene blir oppfylt. For søker og saksbehandler er det viktig at det kan redegjøres for hvordan kravene svares ut med henvisning til både krav og dokumentasjon i styringssystemet. Avsnittene med eksempler viser hvordan dette referansematerialet kan se ut.

Referanser, som kan være nyttige for en søker ved forberedelse av en søknad, finner man eksempler på i denne veilederen. Det er også gitt eksempler på problemstillinger som en saksbehandler kan gi av innspill til fremtidig tilsyn av virksomheten. Tilsynet gjennomføres av den relevante nasjonale sikkerhetsmyndigheten.

Prosesstilnærmingen som anvendes i ISO-styringssystemstandarter og CSM SMS er kun veiledende. Det forventes likevel dokumentasjon på etablerte relevante prosedyrer i virksomhetens sikkerhetsstyringssystem.

Fleksibiliteten som er overlatt til søkeren tar sikte på å gi virksomheten muligheten til etablere sitt sikkerhetsstyringssystem på en måte som gjenspeiler virksomhetens art og omfang.

Fleksibilitet i sikkerhetsstyringen vil kunne resultere i at man beveger seg bort fra en papirbasert test av etterlevelse, og heller til en vurdering av et dynamisk system i utvikling som på en egnet måte gjenspeiler virksomhetens sikkerhetsstyringssystemer, slik de virker i praksis.

Begrepet «dokumentert informasjon» ble introdusert som en del av HLS og er et vanlig begrep i andre styringssystemstandarter. Definisjonen av «dokumentert informasjon» finnes i *ISO 9000 paragraf 3.8*. Dokumentert informasjon kan brukes til å formidle et budskap, gi dokumentasjon på hva som var planlagt,

The NSA NO 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.

hva som faktisk er gjort, eller utveksling av kunnskap. Den inkluderer, men er ikke begrenset til, dokumenter og arkiver som prosedyrer, møtetreferater, rapporter, formell kommunikasjon om mål, resultater, avtaler, kontrakter osv. Ytterligere forklaringer finnes i *Veiledning for krav til dokumentert informasjon i ISO 9001:2015* tilgjengelig på ISO-nettsiden:

[https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/documented\\_information.pdf](https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/documented_information.pdf).

Begrepet «prosedyre» innebærer ikke et frittstående dokument som kun dekker etterlevelsen av hvert enkelt element i sikkerhetsstyringssystemet. Begrepet «prosedyre» er heller ment å kreve at et nytt sett med dokumenter skal utarbeides. Når dette dokumentet refererer til en «prosedyre», viser det til «dokumentert informasjon» som beskriver prosessen som anvendes. Når det refereres til en «prosess», viser denne til hensikten med en oppgave eller hvordan man når et mål.

## 0.10 Kryssreferanser til andre EU-forordninger og gjeldende lovfestede krav

Referanser til andre EU-forordninger forsterker det juridiske rammeverket, samtidig som man anerkjenner forbindelsene mellom dem. Sikkerhetsstyringssystemet må alltid overholde gjeldende lovverk, med mindre annet er angitt (for eksempel spesifikke overgangsbestemmelser). Når en EU-forordning oppheves, blir alle referanser fra den opphevede forordningen vanligvis videreført som referanser i den nye forordningen (hvis de er angitt).

Alle jernbanevirksomheter må overholde en rekke lovfestede krav utover de som bare omfatter sikkerhet. Noen av disse andre kravene vil enten direkte eller indirekte påvirke sikkerhetsarbeidet i en virksomhet. Dette kan for eksempel gjelde etterlevelse av lovgivning som følger av interoperabilitetsdirektivet (EU) 2016/797 eller lovgivning som følger av direktiv (EU) 2012/34 (om opprettelse av et felles europeisk jernbaneområde). Derfor må sikkerhetsstyringssystemet til en virksomhet også sikre at andre lovfestede krav overholdes.

## Innhold

<b>0</b>	<b>INNLEDNING .....</b>	<b>1</b>
0.1	FORMÅLET MED VEILEDEREN .....	2
0.2	HVEM ER DENNE VEILEDEREN RETTET MOT? .....	2
0.3	OMFANG .....	2
0.4	VEILEDERENS STRUKTUR .....	3
0.5	ISO-STANDARDER .....	4
0.6	FORMÅLET MED SIKKERHETSSTYRINGSSYSTEMET .....	4
0.7	SIKKERHETSSTYRINGSSYSTEM OG PROSESSTILNÆRMING .....	5
0.8	SIKKERHETSSTYRINGSSYSTEM OG SIKKERHETSKULTUR .....	7
0.9	DOKUMENTASJON .....	8
0.10	KRYSSREFERANSER TIL ANDRE EU-FORORDNINGER OG GJELDENDE LOVFESTEDE KRAV .....	9
<b>1</b>	<b>VIKRSOMHETENS KONTEKST .....</b>	<b>14</b>
1.1	LOVBESTEMT KRAV .....	14
1.2	FORMÅL .....	14
1.3	FORKLARENDE MERKNADER .....	14
1.4	DOKUMENTASJON .....	15
1.5	EKSEMPLER PÅ DOKUMENTASJON .....	16
1.6	REFERANSER OG STANDARDER .....	17
1.7	RELEVANTE TEMA FOR TILSYN .....	17
<b>2</b>	<b>LEDERSKAP .....</b>	<b>18</b>
2.1	LEDERSKAP OG FORPLIKTELSE .....	18
2.1.1	Lovbestemt krav .....	18
2.1.2	Formål .....	18
2.1.3	Forklarende merknader .....	19
2.1.4	Dokumentasjon .....	19
2.1.5	Eksempler på dokumentasjon .....	19
2.1.6	Referanser og standarder .....	20
2.1.7	Relevante tema for tilsyn .....	20
2.2	SIKKERHETSPOLITIKK .....	21
2.2.1	Lovbestemt krav .....	21
2.2.2	Formål .....	21
2.2.3	Forklarende merknader .....	21
2.2.4	Dokumentasjon .....	21
2.2.5	Eksempler på dokumentasjon .....	22
2.2.6	Relevante tema for tilsyn .....	22
2.3	ROLLER, ANSVAR OG MYNDIGHET I VIKRSOMHETEN .....	23
2.3.1	Lovbestemt krav .....	23
2.3.2	Formål .....	23
2.3.3	Forklarende merknader .....	23
2.3.4	Dokumentasjon .....	24
2.3.5	Eksempler på dokumentasjon .....	24
2.3.6	Referanser og standarder .....	25
2.3.7	Relevante tema for tilsyn .....	25
2.4	SAMRÅD MED PERSONALET OG ANDRE PARTER .....	26
2.4.1	Lovbestemt krav .....	26
2.4.2	Formål .....	26
2.4.3	Forklarende merknader .....	26

The NSA NO 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.

2.4.4	Dokumentasjon.....	26
2.4.5	Eksempler på dokumentasjon.....	27
2.4.6	Relevante tema for tilsyn.....	27
<b>3</b>	<b>PLANLEGGING .....</b>	<b>28</b>
3.1	TILTAK FOR Å HÅNDTERE RISIKO.....	28
3.1.1	Lovbestemt krav.....	28
3.1.2	Formål.....	28
3.1.3	Forklarende merknader.....	29
3.1.4	Dokumentasjon.....	30
3.1.5	Eksempler på dokumentasjon.....	31
3.1.6	Referanser og standarder .....	32
3.1.7	Relevante tema for tilsyn .....	32
3.2	SIKKERHETSMÅL OG PLANLEGGING.....	33
3.2.1	Lovbestemt krav.....	33
3.2.2	Formål.....	33
3.2.3	Forklarende merknader.....	33
3.2.4	Eksempler på dokumentasjon.....	34
3.2.5	Relevante tema for tilsyn .....	34
<b>4</b>	<b>STØTTE.....</b>	<b>35</b>
4.1	RESSURSER .....	35
4.1.1	Lovbestemt krav.....	35
4.1.2	Formål.....	35
4.1.3	Forklarende merknader.....	35
4.1.4	Dokumentasjon.....	35
4.1.5	Eksempler på dokumentasjon.....	35
4.1.6	Relevante tema for tilsyn .....	36
4.2	KOMPETANSE .....	37
4.2.1	Lovbestemt krav.....	37
4.2.2	Formål.....	37
4.2.3	Forklarende merknader.....	38
4.2.4	Dokumentasjon.....	38
4.2.5	Eksempler på dokumentasjon.....	39
4.2.6	Referanser og standarder .....	39
4.2.7	Relevante tema for tilsyn .....	40
4.3	BEVISSTHET.....	41
4.3.1	Lovbestemt krav.....	41
4.3.2	Formål.....	41
4.3.3	Dokumentasjon.....	41
4.3.4	Eksempler på dokumentasjon.....	41
4.3.5	Relevante tema for tilsyn .....	42
4.4	INFORMASJON OG KOMMUNIKASJON .....	43
4.4.1	Lovbestemt krav.....	43
4.4.2	Formål.....	43
4.4.3	Forklarende merknader.....	43
4.4.4	Dokumentasjon.....	44
4.4.5	Eksempler på dokumentasjon.....	44
4.4.6	Relevante tema for tilsyn .....	45
4.5	DOKUMENTERT INFORMASJON.....	46
4.5.1	Lovbestemt krav.....	46
4.5.2	Formål.....	47
4.5.3	Forklarende merknader.....	47

The NSA NO has kindly provided its assistance to the revision of the translation of this guide.

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

4.5.4	Dokumentasjon.....	48
4.5.5	Eksempler på dokumentasjon.....	48
4.5.6	Referanser og standarder.....	49
4.5.7	Relevante tema for tilsyn.....	49
4.6	INTEGRASJON AV MENNESKELIGE OG ORGANISATORISKE FAKTORER.....	50
4.6.1	Lovbestemt krav.....	50
4.6.2	Formål.....	50
4.6.3	Forklarende merknader.....	50
4.6.4	Dokumentasjon.....	50
4.6.5	Eksempler på dokumentasjon.....	51
4.6.6	Referanser og standarder.....	52
4.6.7	Relevante tema for tilsyn.....	52
<b>5</b>	<b>DRIFT.....</b>	<b>53</b>
5.1	PLANLEGGING OG STYRING AV DRIFTEN.....	53
5.1.1	Lovbestemt krav.....	53
5.1.2	Formål.....	54
5.1.3	Forklarende merknader.....	54
5.1.4	Dokumentasjon.....	56
5.1.5	Eksempler på dokumentasjon.....	56
5.1.6	Referanser og standarder.....	57
5.1.7	Relevante tema for tilsyn.....	58
5.2	FORVALTNING AV EIENDELER.....	59
5.2.1	Lovbestemt krav.....	59
5.2.2	Formål.....	60
5.2.3	Forklarende merknader.....	60
5.2.4	Dokumentasjon.....	61
5.2.5	Eksempler på dokumentasjon.....	62
5.2.6	Referanser og standarder.....	67
5.2.7	Relevante tema for tilsyn.....	67
5.3	ENTREPRENØRER, PARTNERE OG LEVERANDØRER.....	68
5.3.1	Lovbestemt krav.....	68
5.3.2	Formål.....	68
5.3.3	Forklarende merknader.....	69
5.3.4	Dokumentasjon.....	69
5.3.5	Eksempler på dokumentasjon.....	69
5.3.6	Relevante tema for tilsyn.....	70
5.4	ENDRINGSSTYRING.....	71
5.4.1	Lovbestemt krav.....	71
5.4.2	Formål.....	71
5.4.3	Forklarende merknader.....	71
5.4.4	Dokumentasjon.....	72
5.4.5	Eksempler på dokumentasjon.....	72
5.4.6	Relevante tema for tilsyn.....	72
5.5	HÅNDTERING AV NØDSITUASJONER.....	73
5.5.1	Lovbestemt krav.....	73
5.5.2	Formål.....	74
5.5.3	Forklarende merknader.....	74
5.5.4	Dokumentasjon.....	74
5.5.5	Eksempler på dokumentasjon.....	74
5.5.6	Relevante tema for tilsyn.....	75
<b>6</b>	<b>VURDERING AV RESULTATER.....</b>	<b>76</b>

The NSA NO 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.

6.1	OVERVÅKING.....	76
6.1.1	Lovbestemt krav.....	76
6.1.2	Formål.....	76
6.1.3	Forklarende merknader.....	76
6.1.4	Dokumentasjon.....	77
6.1.5	Eksempler på dokumentasjon.....	77
6.1.6	Relevante tema for tilsyn.....	77
6.2	INTERNREVISJON.....	78
6.2.1	Lovbestemt krav.....	78
6.2.2	Formål.....	78
6.2.3	Forklarende merknader.....	78
6.2.4	Dokumentasjon.....	78
6.2.5	Eksempler på dokumentasjon.....	79
6.2.6	Referanser og standarder.....	79
6.2.7	Relevante tema for tilsyn.....	79
6.3	LEDELSENS GJENNOMGÅELSE.....	80
6.3.1	Lovbestemt krav.....	80
6.3.2	Formål.....	80
6.3.3	Dokumentasjon.....	80
6.3.4	Eksempler på dokumentasjon.....	81
6.3.5	Relevante tema for tilsyn.....	81
<b>7</b>	<b>FORBEDRING.....</b>	<b>82</b>
7.1	ERFARINGER FRA ULYKKER OG HENDELSER.....	82
7.1.1	Lovbestemt krav.....	82
7.1.2	Formål.....	82
7.1.3	Forklarende merknader.....	83
7.1.4	Dokumentasjon.....	83
7.1.5	Eksempler på dokumentasjon.....	83
7.1.6	Referanser og standarder.....	84
7.1.7	Relevante tema for tilsyn.....	84
7.2	KONTINUERLIG FORBEDRING.....	85
7.2.1	Lovbestemt krav.....	85
7.2.2	Formål.....	85
7.2.3	Forklarende merknader.....	85
7.2.4	Dokumentasjon.....	87
7.2.5	Eksempler på dokumentasjon.....	88
7.2.6	Relevante tema for tilsyn.....	88
<b>VEDLEGG 1 — LOVSPEIL.....</b>		<b>89</b>
<b>VEDLEGG 2 — KRYSSAKSEPT AV TILLATELSER, GODKJENNELSER ELLER SERTIFIKATER FOR PRODUKTER ELLER TJENESTER SOM LEVERES I SAMSVAR MED EU-REGELVERKET .....</b>		<b>97</b>
<b>VEDLEGG 3 — SIDESPORSOPERASJONER, AVTALEORDNINGER OG SAMARBEID.....</b>		<b>101</b>
<b>VEDLEGG 4 — SIKKERHETSKULTUR .....</b>		<b>105</b>
<b>VEDLEGG 5 — MENNESKELIGE OG ORGANISATORISKE FAKTORER .....</b>		<b>109</b>
<b>VEDLEGG 6 – DEFINISJONER .....</b>		<b>112</b>

The NSA NO has kindly provided its assistance to the revision of the translation of this guide.

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

## 1 Virksomhetens kontekst

### 1.1 Lovbestemt krav

#### 1.1. Virksomheten skal:

- (a) beskrive virksomhetens art og omfang samt virkeområdet,
- (b) identifisere alvorlige sikkerhetsrisikoer som er forbundet med jernbanedriften, enten den utføres av virksomheten selv eller av entreprenører, partnere eller leverandører som er underlagt virksomhetens styring,
- (c) identifisere de berørte parter (f.eks. reguleringsorganer, myndigheter, infrastrukturforvaltere, entreprenører, leverandører, partnere), herunder parter utenfor jernbanesystemet, som er relevante for sikkerhetsstyringssystemet,
- (d) identifisere og opprettholde lovfestede krav og andre krav knyttet til sikkerhet fra de berørte parter som er nevnt i bokstav c),
- (e) sikre at kravene nevnt i bokstav d) tas i betraktning når sikkerhetsstyringssystemet utvikles, gjennomføres og vedlikeholdes,
- (f) beskrive sikkerhetsstyringssystemets virkeområde og angi hvilken del av virksomheten som er omfattet eller ikke omfattet av virkeområdet, idet det tas hensyn til kravene nevnt i bokstav d).

#### 1.2. I dette vedlegg (krav til infrastrukturforvalters sikkerhetsstyringssystem) menes med

- (a) «art» i forbindelse med jernbanedrift som utføres av infrastrukturforvaltere, driftens egenskaper i form av virkeområde, herunder infrastrukturens utforming og oppbygging, vedlikehold av infrastrukturen, trafikkplanlegging og trafikkstyring, og bruk av jernbaneinfrastrukturen, herunder konvensjonelle linjer og/eller høyhastighetslinjer, transport av passasjerer og/eller gods,
- (b) «omfang» i forbindelse med jernbanedrift som utføres av infrastrukturforvaltere, omfanget som kjennetegnes ved jernbanesporets lengde og infrastrukturforvalterens anslåtte størrelse målt i antall ansatte som arbeider i jernbanesektoren.

### 1.2 Formål

Søkeren skal dokumentere overfor sikkerhetsmyndighetene at sikkerhetsstyringssystemet dekker driften. Sikkerhetsmyndighetene må kunne se klart hva som er driftens omfang, og hvordan driften styres. Søkeren skal dokumentere at virksomheten har en klar forståelse av risiko knyttet til sin virksomhet, herunder risiko relatert til andre interessenter og hvordan dette håndteres i sikkerhetsstyringssystemet.

### 1.3 Forklarende merknader

Virksomhetens kontekst og omfanget av sikkerhetsstyringssystemet (1.1) gir saksbehandler bedre forståelse av virksomheten, relevante interessenter og miljøet virksomheten opererer i. Virksomhetens art er utgangspunktet for vurderingen - når denne informasjonen er oppgitt i begynnelsen av søknaden kan søkeren beskrive hva de gjør og hvordan virksomheten er strukturert, og dette vil igjen gjøre det mulig for

saksbehandler å ta beslutninger om hvordan man skal planlegge vurderingen. Hvis virksomheten for eksempel er sentralisert, driver ulike virksomheter med omfattende lokal frihet til å planlegge og organisere aktivitetene sine, eller hvis virksomheten leier inn ressurser i større eller mindre grad, vil det være en tilsvarende forventning til at søkerens virksomhet og dens sikkerhetsstyringssystem er strukturert for å håndtere relevante problemstillinger. Forklaringen av virksomhetens kontekst kan også indikere hvordan menneskelige og organisatoriske faktorer håndteres. Strukturen som er beskrevet i punkt 4 i HLS, kan bidra til å forstå det forberedende arbeidet som trengs før sikkerhetsstyringssystemet etableres. Det er viktig at saksbehandler forstår omfanget av driften hvis de skal kunne foreta en vurdering.

Typer drift **(1.1.1 (a))** omfatter per definisjon passasjertransport (med eller uten høyhastighetstjenester) og gods (med eller uten farlig gods) og skiftetjenester. Det kan også omfatte andre spesielle typer drift som testing av jernbanevogner, bruk av jernbanevogner for vedlikehold av jernbaneinfrastrukturen og drift på privateide sidespor. Mer informasjon om typen, omfanget og driftsområdet finnes i *Byråets søknadsveiledning for utstedelse av felles sikkerhetssertifikater*. Ytterligere informasjon om sidesporoperasjoner finnes i Vedlegg 3.

Identifisering av risiko innebærer at søkeren skal utarbeide en risikoanalyse. Denne risikoanalysen skal vise at virksomheten har identifisert de viktigste risikoområdene for sin aktivitet. Identifikasjon av risiko innebærer også at søkeren har utarbeidet et system for å håndtere risiko (eller er i ferd med å utarbeide det), og ut fra dette kan:

- *analysere farlige hendelser og vurdere risiko,*
- *bli gjort oppmerksom på det viktigste (når det gjelder konsekvenser og hyppighet) og*
- *prioritere tiltak som har til hensikt å forebygge ulykker. (1.1.1 (b))*

Dette bidrar til å klargjøre virksomhetens kontekst, og viser sikkerhetsmyndighetene at søkeren forstår det miljøet virksomheten drives i. Eksterne parters aktiviteter **(1.1.1 (c))** kan påvirke sikkerheten ved driften, og må derfor også vurderes som en del av risikovurderingen. Ytterligere informasjon om avtaleordninger og samarbeid finnes i Vedlegg 3.

Identifikasjon av gjeldende sikkerhetskrav **(1.1.1 (d))** omfatter alt fra bestemmelsene i gjeldende EU-forordninger (for eksempel relevante felles sikkerhetsmetoder for sikkerhetsstyringssystemer, særlig vedlegg I og vedlegg II, felles sikkerhetsmetoder for risikovurdering og evaluering, felles sikkerhetsmetoder for overvåkning, relevante tekniske spesifikasjoner for interoperabilitet, gjennomføringsforordning om opprettelse av praktiske ordninger for utstedelse av felles sikkerhetssertifikat, gjennomføringsforordning om opprettelse av praktiske ordninger for tillatelser til å ta i bruk kjøretøy og ECM-forordningen) og nasjonal lovgivning (for eksempel notifiserte nasjonale regler og nasjonale lover), til alle andre krav som virksomheten frivillig underlegger seg (foreksempel styringssystem og tekniske standarder som ISO, CEN/CENELEC, UIC).

I denne veilederen har begrepene «personell», «ansatte og «arbeidere» samme betydning, det vil si personer som arbeider under direkte ledelse av søkerens virksomhet.

## 1.4 Dokumentasjon

- *For jernbaneforetak: Informasjon om driftens art, for eksempel passasjertransport og/eller frakt, transport av farlig gods, geografisk dekning (ved å vedlegge et kart eller en ruteplan) og driftsomfanget (inkludert typer kjøretøy og antall ansatte) (1.1 (a))*
- *For infrastrukturforvaltere: Informasjon om hvilke tjenester de utfører, for eksempel frakt og passasjertransport, skifting eller andre anleggstjenester (som nevnt i vedlegg II til direktiv 2012/34/EU, om et felles europeisk jernbaneområde) som har innvirkning på jernbanesikkerhet,*

---

The NSA NO 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.

geografisk dekning (ved å vedlegge et kart eller ruteplan) og omfanget av jernbaneforetak som opererer på jernbanenettet. Infrastrukturforvalteren må også ta med opplysninger om kjøretøy (inkludert anlegg for vedlikehold eller måling av infrastruktur) som de eventuelt drifter, og oppgi antall ansatte i virksomheten **(1.1 1 (a))**

- Søkeren av et sikkerhetssertifikat eller en sikkerhetstillatelse må dokumentere hvordan relevante forskriftskrav er identifisert. Dette vil for eksempel være CSM-kravene, tekniske spesifikasjoner for interoperabilitet, da særlig dem som omfatter drifts- og trafikkstyring (TSI OPE), og gjeldende nasjonalt lovverk, samt hvordan det sikres at disse etterleves (SMS-prosessene som bidrar til etterlevelse); **(1.1 1(c)-(d))**
- Søkeren må identifisere interessenter som er relevante (for eksempel leverandører) med en indikasjon på hvorfor dette er nødvendig; **(1.1 1(c) (d))**
- For begge parter: Søkeren må angi hvor i sikkerhetsstyringssystemet hvert av SMS-kravene, inkludert kravene i de gjeldende tekniske spesifikasjonene for interoperabilitet, særlig (TSI-OPE), og relevante notifiserte nasjonale regler, er oppfylt **(1.1 1(e))**
- Søkeren må oppgi de alvorligste sikkerhetsrisikoene som har innvirkning på virksomheten; **(1.1.1(b))**
- Søkeren må komme med opplysninger om omfanget av sikkerhetsstyringssystemet (inkludert grensesnitt mot andre deler av virksomheten). **(1.1.1(f))**

## 1.5 Eksempler på dokumentasjon

Et kart som viser det geografiske driftsområdet. Informasjon om kjøretøy som er tillatt tatt i bruk (mottatt tillatelse til å ta i bruk), eventuelt kjøretøy som er foreslått å ha i drift i løpet av sertifikatets eller tillatelsens gyldighet, samt eventuelle begrensninger i bruksområdet. Informasjon om hvilke typer tjenester som skal utføres (passasjertransport og/eller frakt).

Dersom søkeren er en infrastrukturforvalter, kan dokumentasjonen være:

- informasjonen i jernbaneinfrastrukturregistret som er opprettet i samsvar med Interoperabilitetsdirektivet (art. 49)
- innholdet i netterklæringen (Network Statement), særlig i del I, som er opprettet i samsvar med direktiv 2012/34/EU og
- ruteboken (TSI OPE)

Opplysninger som gis i søknad om sikkerhetstillatelse eller et felles sikkerhetssertifikat, er tilstrekkelig referert, og vil være tilstrekkelig dokumentert for å vise samsvar med relevant felles europeisk regelverk.

En indikasjon på nåværende og foreslått bemanning innenfor virketiden til det felles sikkerhetssertifikatet så sant dette er kjent.

Et jernbaneforetak skal kunne oppgi informasjon om operative grensesnitt, herunder grensesnitt mot infrastrukturforvalteren, andre jernbaneforetak, leverandører og nødetatene. Disse opplysningene inkluderer også spesifikke krav fra infrastrukturforvalter som påvirker jernbaneforetakets sikkerhetsstyringssystem.

For jernbanevirksomheter kan en kryssreferanseliste legges ved som en del av søknadsfilen for et felles sikkerhetssertifikat. Denne kan brukes til å forklare hvordan forskriftene etterleves.

En infrastrukturforvalter skal kunne vise en tilsvarende liste over grensesnitt mot for eksempel jernbaneforetak som opererer på infrastrukturen, leverandører, grensende infrastrukturforvaltere, anleggsområder, relevante myndigheter og nødetater.

Informasjon om lovkrav (både nasjonale og europeiske) som skal etterleves.

En beskrivelse (inkludert organisasjonskart) som viser oppbyggingen av sikkerhetsstyringssystemet og hvordan det styres i virksomheten. Det skal også kunne dokumenteres hvordan sikkerhetsstyringssystemet ivaretas i daglig drift.

En kopi av årsrapporten som beskriver i detalj risikoer virksomheten står overfor, hvordan man vurderer dem og hvordan de prioriteres.

## 1.6 Referanser og standarder

- *TSI OPE-søknadsveiledninger*

## 1.7 Relevante tema for tilsyn

Ved søknad om fornyet felles sikkerhetssertifikat kontrolleres mottatt dokumentasjon mot kjent informasjon om virksomheten. Ved søknad om nytt felles sikkerhetssertifikat kontrolleres dokumentasjon mot annen tilgjengelig informasjon.

Sjekk at sikkerhetsstyringssystemet inneholder prosedyrer/bestemmelser for å håndtere sikkerheten i praksis.

Sjekk at relevant samhandling virksomheten har med andre parter (alle relevante grensesnitt), gjenspeiles i styrende dokumentasjon i sikkerhetsstyringssystemet.

## 2 Lederskap

### 2.1 Lederskap og forpliktelse

#### 2.1.1 Lovbestemt krav

- 2.1.1. Den øverste ledelsen skal vise lederskap og forpliktelse til å utvikle, gjennomføre, vedlikeholde og kontinuerlig forbedre sikkerhetsstyringssystemet ved å taking overall accountability and responsibility for safety;
- (a) vise ansvar og påta seg det overordnede ansvaret for sikkerheten,
  - (b) sikre forpliktelse når det gjelder sikkerhet på ulike ledelsesnivåer i virksomheten gjennom ledelsens virksomhet og forbindelser med personale og underleverandører,
  - (c) sikre at sikkerhetspolitikken og sikkerhetsmålene fastsettes, forstås og er forenlige med virksomhetens strategiske retning,
  - (d) sikre at sikkerhetsstyringssystemets krav integreres i virksomhetens forretningsprosesser,
  - (e) sikre at de nødvendige ressursene for sikkerhetsstyringssystemet er tilgjengelige,
  - (f) sikre at sikkerhetsstyringssystemet effektivt styrer de sikkerhetsrisikoene som er forbundet med virksomheten,
  - (g) oppmuntre personalet til å bidra til å overholde sikkerhetsstyringssystemets krav,
  - (h) fremme kontinuerlig forbedring av sikkerhetsstyringssystemet,
  - (i) sikre at sikkerheten tas i betraktning når virksomhetens risiko identifiseres og håndteres, og beskrive hvordan en konflikt mellom sikkerhet og andre forretningsmål vil bli erkjent og løst,
  - (j) *fremme en positiv sikkerhetskultur.*

#### 2.1.2 Formål

Fokusering på sikkerhetsstyring har effekt på hvordan risiko styres. Sikkerhetsmyndighetene må være sikre på at søkeren vil tilordne ressurser slik at virksomheten ledes på en sikker måte med hensiktsmessig risikostyring. Ledelsens engasjement om menneskelige og organisatoriske faktorer gjenspeiles i retningslinjer, mål og gjennom ledelsens opptreden. Videre vil ledelsens tilnærming til menneskelige og organisatoriske faktorer føre til at opplæring og utvikling av prosedyrer baserer seg på oppgaven som skal utføres.

Sikkerhetspolitikken fremhever viktigheten og prioriteringen av sikkerheten i en virksomhet. Dette inkluderer menneskelige og organisatoriske faktorer og er med på å fremme sikkerhetskulturen .

God sikkerhetsstyring handler om mer enn å overholde prosedyrer. En virksomhet må alltid være kritisk til utøvelse av egen virksomhet. Videre er alle aktører i virksomheten klar over at uansett kvaliteten på planlegging og organisering, tekniske barrierer og prosedyrer, kan det alltid være et gap mellom hva som er forventet og hva som er realitet. For å få kontroll på et aktuelt gap, benyttes ulike kilder til å identifisere og analysere relevante situasjoner.

Virksomhetens kommunikasjon om sikkerhet må være i tråd med ledelsesbeslutninger.

For at et sikkerhetsstyringssystem skal fungere hensiktsmessig og forbedres, må ledelsen sette sikkerhet på dagsordenen. Ledere, på alle nivåer i en virksomhet, har stor påvirkning på organisasjonskulturen, og det er derfor viktig at de kommuniserer riktig til de som arbeider under deres ledelse. Atferden til ledere på alle nivåer i virksomheten og søkelyset de setter på sikkerheten i sine daglige beslutninger, vil i stor grad påvirke andre aktørers atferd når det gjelder å utføre deres sikkerhetsoppgaver. I tillegg bør lederne legge til rette for det fysiske og sosiale arbeidsmiljøet slik at operativt arbeid utføres sikkert.

### 2.1.3 Forklarende merknader

«Toppledelse» **(2.1.1)** viser i denne sammenhengen til ledere som tar endelige beslutninger i en virksomhet. Vanligvis vil dette være administrerende direktør, medlemmer i toppledelsen, styreleder og styremedlemmer. Som en gruppe og som enkeltpersoner er «toppledelsen» pålagt å utvise godt lederskap og engasjement i og ved hjelp av sikkerhetsstyringssystemet.

Sikkerhetsrisikoen skal vektlegges tilstrekkelig **(2.1.1 (j))** for å balansere andre risikoer på arbeidsplassen, for å unngå situasjoner der ledelsen prioriterer forretningsbehov på en slik måte at det går utover sikkerheten. Toppledelsen må sørge for at målene håndteres på en slik måte at sikkerheten opprettholdes, og at risikoen kan håndteres så langt det i rimelig grad er mulig. Motstridende mål må ikke resultere i motstridende oppgaver for enkeltpersoner, som kan føre til at det går utover sikkerheten.

Integrering av menneskelige og organisatoriske faktorer i ledelse og styring vil si å sette mål, forventninger og ansvar for sikkerhetsatferden på alle nivåer i virksomheten, og sikre tilstrekkelige tilbakemeldinger og kommunikasjon.

### 2.1.4 Dokumentasjon

- *Det foreligger sikkerhetspolitikk og sikkerhetsmål og det foreligger dokumentasjon på at disse er gjort tilgjengelige for og forstått av alle ansatte, og det er klargjort hvordan disse passer inn i andre prosesser i virksomheten **(2.1.1 (a)(b)(g)(e))***
- *Sikkerhetspolitikken vektlegger menneskelige og organisatoriske faktorer i alle sikkerhetsrelaterte prosesser, for å oppnå et høyt sikkerhetsnivå i virksomheten. Virksomheten viser hvordan menneskelige og organisatoriske faktorer er håndtert i virksomhetens prosesser **(2.1.1 (c))***
- *Forholdet mellom sikkerhetsstyringssystemet og andre forretningsaktiviteter er tydelig fastsatt i en prosedyre eller et organisasjonskart **(2.1.1 (i))***
- *Det foreligger informasjon i sikkerhetspolitikken eller i andre prosesser som viser at ledelsen vil sørge for og opprettholde nødvendige ressurser for at sikkerhetsstyringssystemet skal fungere hensiktsmessig **(2.1.1 (e))***
- *Det foreligger dokumentasjon på at ledelsen fremmer en positiv sikkerhetskultur; **(2.1.1 (j))***
- *Det foreligger dokumentasjon på hvordan det sikres at ansatte forstår sine roller og sitt ansvar, og hvordan de ansatte på denne måten påvirker virksomhetens sikkerhetsstyring **(2.1.1 (d)(f)(i))***
- *Det fremkommer i sikkerhetspolitikken eller annen dokumentasjon at virksomheten informerer sine ansatte om betydningen de har for å sikre et fungerende sikkerhetsstyringssystem **2.1.1 (e)***
- *Det foreligger prosesser som beskriver hvordan menneskelige og organisatoriske faktorer skal håndteres og formidles i virksomheten relatert til virksomhetens forretningsmål og virksomhetsprosesser. Dette kan for eksempel være prosjekter, granskning av hendelser og ulykker, risikoanalyser og andre sikkerhetsrelaterte aktiviteter for virksomhetens eget personale, samarbeidspartnere og leverandører; **(2.2.1 (c)(d)(e))***
- *Det foreligger dokumentasjon som viser at ledelsen har på plass prosesser for å sikre at menneskelige og organisatoriske faktorer er tilstrekkelig tatt hensyn til hos virksomhetens leverandører **(2.2.1 (c)(d)(e))***

### 2.1.5 Eksempler på dokumentasjon

En sikkerhetspolitikk som er undertegnet av administrerende direktør og datert, som klart beskriver ledelsens engasjement for å oppnå god sikkerhet og forbedring av sikkerheten, og hvordan de ansatte er involvert i risikostyring. Det skal også vises hvordan sikkerhetspolitikken skal evalueres.

Et klart sett med sikkerhetsmål fastsatt for virksomheten, som er Spesifikke, Målbare, Oppnåelige (Achievable), Realistiske og Tidsbestemte (SMART-modellen), og det finnes en klar metodikk for eksempel i en prosedyre for å etablere målene og for å analysere om man har nådd dem eller ikke.

Ledelsen skal tydelig fremme en positiv sikkerhetskultur i virksomheten, og det må fremkomme hvordan de ansatte er involvert og engasjert i prosessen.

En oversikt over toppledermøter, inkludert møtefrekvens, der sikkerhet er et fast punkt på dagsordenen.

En klar redegjørelse for hvordan virksomheten sørger for nødvendige ressurser slik at sikkerhetsstyringssystemet fungerer hensiktsmessig.

Et organisasjonskart som tydelig beskriver hvordan sikkerhetsstyringssystemet fungerer, og hvem som er ansvarlig for hva.

I design av nytt utstyr er det tatt hensyn til menneskelige og organisatoriske faktorer, for eksempel for nye tog. Dette inkluderer brukererfaringer i utarbeidelse av designkrav, samt analyse av oppgaver for å identifisere kognitive og fysiologiske utfordringer.

Bruk av retningslinjer for menneskelige faktorer som for eksempel ulike ISO- eller UIC-standarder vil redusere sannsynligheten for utarbeidelse av design som ikke er hensiktsmessig. Disse retningslinjene/standardene kan for eksempel brukes ved analyse av arbeidsbelastning og utmattende arbeid for å sikre at ansatte er i stand til å utføre sine oppgaver, eller ved utarbeidelse av risikoanalyser for å identifisere potensielle problemer og finne kompenserende tiltak for disse. Miljøfaktorer som snø, varme, regn, etc. tas hensyn til på lik linje med organisatoriske prioriteringer, anskaffelser og nasjonal kultur.

Ved sin tilstedeværelse ute i den spisse enden, og ved ønske om å gå foran som gode eksempler, viser ledelsen engasjement for å fremme positiv sikkerhetskultur.

#### 2.1.6 Referanser og standarder

- [Sikkerhetskultur](#) (SKYbrary)

#### 2.1.7 Relevante tema for tilsyn

Gapet mellom retningslinjer og prosedyrer som fremkommer av vurdert dokumentasjon, det som observeres under tilsyn, i hvilken grad virksomheten er klar over gapet mellom disse, er relevant for videre tilsyn.

Ledelsens forpliktelse og de ansattes engasjement i sikkerhetsarbeid og fremming av sikkerhetskultur, bør undersøkes under tilsyn. Dette kan gjøres ved å undersøke virksomhetenes egne prosesser for forståelse og utvikling av sikkerhetskultur og sikkerhetsstyringssystemet.

Sjekk at virksomheten kan vise til tilstrekkelige ressurser som er tilordnet utvikling, implementering, vedlikehold og kontinuerlig forbedring av sikkerhetsstyringssystemet.

I samtaler med toppledelsen kan det sjekkes hvordan ledelsen uttrykker sitt engasjement, om de nevner hvor ofte og på hvilke måter de drøfter sikkerhetsspørsmål med de ansatte og/eller fremmer sikkerhetskultur (arbeidsgrupper, fora, dedikerte dager med fokusering på sikkerhet osv.) .

Undersøk om det er kommunikasjon fra toppledelsen om mål, enten ved at toppledelsen oppmuntrer ansatte til å bidra til å nå målene, eller ved at toppledelsen takker for at målene er nådd.

## 2.2 Sikkerhetspolitikk

### 2.2.1 Lovbestemt krav

- 2.2.1 Den øverste ledelsen skal utarbeide et dokument som beskriver virksomhetens sikkerhetspolitikk, og som
- (a) er hensiktsmessig ut fra virksomhetens art og jernbanedriftens omfang,
  - (b) er godkjent av virksomhetens administrerende direktør (eller en eller flere representanter for den øverste ledelsen),
  - (c) aktivt gjennomføres, formidles til og gjøres tilgjengelig for alt personale.
- 2.2.2 Sikkerhetspolitikken skal
- (a) omfatte en forpliktelse til å overholde alle lovfestede krav og andre krav knyttet til sikkerhet,
  - (b) opprette en ramme for å fastsette sikkerhetsmål og vurdere virksomhetens sikkerhetsnivå i forhold til disse målene,
  - (c) omfatte en forpliktelse til å styre sikkerhetsrisiko som oppstår både som følge av egen virksomhet, og som forårsakes av andre,
  - (d) omfatte en forpliktelse til kontinuerlig forbedring av sikkerhetsstyringssystemet,
  - (e) opprettholdes i samsvar med virksomhetens strategiske retning og sikkerhetsnivå

### 2.2.2 Formål

Sikkerhetspolitikken er viktig for å vise hvordan virksomheten forvalter sitt sikkerhetsansvar, sitt lederskap og sitt engasjement for hensiktsmessig sikkerhetsstyring. Søkeren skal kunne dokumentere at det foreligger en sikkerhetspolitikk som er i samsvar med kravene ovenfor, og som oppsummert beskriver grunnverdien for virksomhetens sikkerhetsstyring.

### 2.2.3 Forklarende merknader

Sikkerhetspolitikken er et uttrykk for lederskapets filosofi, og dette kapittelet er nært knyttet til kapittel 3.1 Ledelse og engasjement. For eksempel har ikke kravet som handler om sikkerhetspolitikk nevnt menneskelige og organisatoriske faktorer spesielt.

I kapittel 2.2.1 (a) i lovteksten over, om kravet som omhandler infrastrukturforvalter, vises det til infrastrukturforvalters art og omfang (hva slags infrastrukturforvalter det er snakk om) – dette er skrevet i blått.

### 2.2.4 Dokumentasjon

- *For et jernbaneforetak: En skriftlig sikkerhetspolitikk undertegnet av administrerende direktør som gjenspeiler art og omfang av virksomheten, som underbygger samsvar med lovfestede krav og andre krav, med fokusering på kontinuerlig forbedring av sikkerheten, og som brukes til å sette sikkerhetsmål. (2.2.1 (a),(b)), (2.2.2 (a-c))*
- *For en infrastrukturforvalter: En skriftlig sikkerhetspolitikk undertegnet av administrerende direktør som gjenspeiler art og omfang av virksomheten, som underbygger samsvar med lovfestede krav og andre krav, med fokusering på kontinuerlig forbedring av sikkerheten, og som brukes til å sette sikkerhetsmål (2.2.2 (a-c))*
- *For jernbanevirksomheter: Informasjon som viser at sikkerhetspolitikken har blitt formidlet til alle ansatte (2.2.1 (c))*

- *Informasjon om at sikkerhetspolitikken oppdateres slik at den alltid er tilpasset virksomhetens forretningsstrategi (2.2.2 (d))*
- *Dokumentasjon som viser at sikkerhetspolitikken forplikter å overvåke virksomhetens sikkerhetsnivå og at den gjennomgås jevnlig basert på analyse av virksomhetens sikkerhetsnivå med hensyn til fastsatte mål. (2.2.2 (b),(d))*

#### 2.2.5 Eksempler på dokumentasjon

En sikkerhetspolitikk som er undertegnet og datert av administrerende direktør som nøyaktig gjenspeiler virksomhetens art og omfang. Dokumentet forplikter til kontinuerlig forbedring av sikkerhetsstyringssystemet.

Sikkerhetspolitikken er oppdatert og blir gjennomgått regelmessig i tråd med forretningsstrategien.

Sikkerhetsmålene er i samsvar med sikkerhetspolitikken, at de er verdsatt og forstått av de ansatte, og at de ansatte på denne måten får et styrket engasjement i å oppnå målene.

Sikkerhetspolitikken inneholder informasjon eller referanser der det er beskrevet en prosess for hvordan den oppdateres etter en gjennomgang av virksomhetens sikkerhetsnivå med hensyn til de fastsatte målene.

Det foreligger en prosess for å formidle sikkerhetspolitikken via virksomhetens intranett og for å vise den frem på strategiske/operasjonelle steder.

#### 2.2.6 Relevante tema for tilsyn

Under tilsyn vil det være viktig å teste hvor godt sikkerhetspolitikken har blitt formidlet til alle ansatte og at de har forstått den, samt hva den betyr i praksis ved etablering av rammeverket for sikkerhet og innenfor virksomhetens kontekst. Et sentralt spørsmål er om sikkerhetspolitikken bidrar til å sette dagsordenen, eller om den bare foreligger fordi det er et lovfestet krav.

Sjekk om endringer i organisatorisk sikkerhetsnivå har ført til en gjennomgang av sikkerhetspolitikken.

Sjekk at sikkerhetspolitikken reflekterer virksomhetens daglige drift.

## 2.3 Roller, ansvar og myndighet i virksomheten

### 2.3.1 Lovbestemt krav

- 2.3.1. Roller, ansvar og myndighet for personale som har en rolle som påvirker sikkerheten (herunder ledelsen og annet personale som har sikkerhetsrelaterte oppgaver) skal fastlegges på alle nivåer i virksomheten og skal dokumenteres, tildeles og formidles til det berørte personalet.
- 2.3.2. Virksomheten skal sikre at personale med delegert ansvar for sikkerhetsrelaterte oppgaver har myndighet, kompetanse og tilstrekkelige ressurser til å utføre sine oppgaver uten å bli påvirket negativt av andre funksjoner i virksomheten.
- 2.3.3. Delegering av ansvar for sikkerhetsrelaterte oppgaver skal dokumenteres og formidles til det berørte personalet som skal godta og forstå oppgavene.
- 2.3.4. Virksomheten skal beskrive fordelingen av roller nevnt i nr. 2.3.1 på forretningsfunksjoner i og eventuelt utenfor virksomheten (se nr. 5.3 Entreprenører, partnere og leverandører).

### 2.3.2 Formål

Målet med dette kravet er å få søkeren til å gi et klart bilde av virksomhetens struktur, samt hvordan roller og ansvar blir tildelt og opprettholdt i hele virksomheten. Et klart bilde av virksomhetens struktur er nøkkelen til å forstå hvor godt virksomhetens sikkerhetsstyringssystem håndterer risiko. Søkeren skal vise hvordan relevante ansatte tildeles oppgaver, hvordan det sikres at de ansatte har en klar forståelse av sine roller og sitt ansvar, og hvordan de ansatte blir holdt ansvarlig for sine oppgaver.

### 2.3.3 Forklarende merknader

Det kan forekomme et gap i forståelsen av reglene i sikkerhetsstyringssystemet på operativt nivå og av styringsprosessene som er beskrevet i sikkerhetsstyringssystemet (for eksempel risikovurdering, overvåking). Identifikasjon av roller som er relevante i sikkerhetsstyringssystemet (**2.3.1**) vil for eksempel være sikkerhetsledere og sikkerhetsgrupper. Det gjelder i tillegg enhver som er involvert i sikkerhetsrelaterte oppgaver, også driftspersonellet, og er uavhengig av om stillingene er lederstillinger (dvs. ledere, linjeledere, annet personell/ansatte/arbeidere).

Roller, ansvar og myndighet som skal defineres (**2.3.1**) inkluderer utveksling av sikkerhetsrelatert informasjon, for eksempel de som er ansvarlig for å utstede sirkulærer til førere (se også **4.4.1** og **4.4.2**).

Toppledelsen er ansvarlig for at sikkerhetsstyringssystemet er i samsvar med CSM-kravene (**1.1.1 (d)**). Toppledelsen kan delegerer noe av ansvaret til relevant personell. Rapportering utføres i samsvar med kravene til gjennomgang av sikkerhetsstyringssystemet (kapittel 6.3 om ledelsens gjennomgåelse). Relevant personell er ansvarlig for å rapportere.

Sikkerhetsrelaterte oppgaver (**2.3.1**) er oppgaver som direkte har med sikkerhet å gjøre, for eksempel at personell styrer eller påvirker bevegelsen av et tog, og ikke-operasjonelle oppgaver som påvirker sikkerheten.

«Delegering» (**2.3.3**) betyr overføring av ansvar fra en person med myndighet til en relevant person i virksomheten, vanligvis for å effektivisere arbeidet i virksomheten. Sikkerhetsansvar kan delegeres, innenfor de gitte rammene for ansvar og myndighet, og denne delegeringen må dokumenteres. Ansvarlighet kan ikke delegeres. Dersom noe ikke er gjort, noe ikke fungerer eller mål ikke er nådd, vil den som eventuelt har delegert et ansvar for oppgaven likevel måtte stå til ansvar.

Delegering av ansvar for oppgaver **(2.3.3)**, inkludert sikkerhetsrelaterte oppgaver, er en del av daglig drift for hvordan personell blir tildelt ulike funksjoner, og dokumentasjon av denne prosessen bør kunne revideres.

Tildeling av roller **(2.3.4)** kan vises med et organisasjonskart.

Ledelsen skal ha tilstrekkelig kunnskap og forståelse av menneskelige og organisatoriske faktorer for å sikre at det hentes inn ekspertise når det er nødvendig. Roller, ansvar og myndighet for eksperter på menneskelige og organisatoriske faktorer, defineres i tråd med oppgavene som skal utføres **(2.3.3)**.

Det bør være på plass en prosess for å sikre at enkeltpersoner kan rapportere nestenulykker, uønskede hendelser og ulykker uten å være redd for at rapporteringen får konsekvenser for dem. Sikkerhetspolitikken skal støtte opp om den enkeltes rettighet og ansvar for å kunne stille spørsmål ved sikkerheten i virksomheten. Sikkerhetspolitikken har nulltoleranse for trakassering, trusler, irettesettelser og diskriminering. Nøkkelen til suksess i en rettferdig kultur er tillit og åpenhet i virksomheten. Dette er noe som bygges opp over tid, og avhenger av ledelsens vilje til å foreta analyser av uønskede hendelser, samt å lytte og ta til seg informasjon. Å være konsekvent i sikkerhetsarbeidet er viktig for å etablere en rettferdig kultur.

#### 2.3.4 Dokumentasjon

- *Et organisasjonskart med relevant forklarende tekst som viser virksomhetens struktur og hvordan sikkerhetsstyringssystemet fungerer, samt hvordan det er tilknyttet virksomhetens kontekst **(2.3.1)**, **(2.3.4)***
- *En liste over annen informasjon som beskriver sikkerhetsansvar i virksomheten **(2.3.1)**, **(2.3.3)***
- *Dokumentasjon på at det foreligger en ajourført styring av kompetanse for alle ansatte, som ivaretar at det foreligger personell med myndighet, tilstrekkelige ressurser og kompetanse for å utføre sikkerhetsrelaterte oppgaver **(2.3.2)***
- *Dokumentasjon på styring av kompetanse i virksomheten, eventuelt dokumentasjon av andre prosesser som viser at virksomheten sikrer at roller og ansvar blir tildelt, akseptert og klart forstått av ansatte, og at de ansatte blir holdt ansvarlig for å utføre tildelt rolle **(2.3.3)***
- *En beskrivelse av fordeling av ansvar og myndighet i virksomheten, herunder hvordan ansvar og myndighet er fordelt mellom ansatte og leverandører **(2.3.4)***
- *Strategi for menneskelige og organisatoriske faktorer skal vise når og hvordan ekspertise på menneskelige og organisatoriske faktorer blir hentet inn, og hva omfanget er **(2.3.1)**, (se også 4.6)*

#### 2.3.5 Eksempler på dokumentasjon

Et organisasjonskart med forklaring som gjør det mulig for saksbehandler å se hvordan sikkerhetsstyringssystemet er strukturert, og hvordan delene henger sammen.

Prosessten viser hvordan sikkerhetsansvar er delegert, hvor delegering er tillatt, samt viser eksempel på hvordan prosessen har fungert.

Eksempler på arbeidsbeskrivelser av sikkerhetsrelaterte oppgaver. Dette inkluderer også sikkerhetsrelaterte oppgaver som ikke direkte berører operativ drift, men som likevel påvirker driften (for eksempel: delegere jobber, planlegge drift, gi operativ informasjon til ansatte og overvåke driften).

Referanse til styring av kompetanse i virksomheten med informasjon om hvordan dette er strukturert, samt koblinger til hvor detaljene kan bli funnet.

En tilbakemeldingsprosess som brukes til å sikre at informasjon som har gått nedover i virksomheten er tydelig forstått.

Prosedyren(e) for å definere hvilken kompetanse og hvilke behov for ressurser som er nødvendig for at sikkerhetsoppgaver skal kunne utføres og hvordan ansvar er definert på alle nivåer i virksomheten.

Strategien for menneskelige og organisatoriske faktorer viser hvordan ansvar og myndighet integreres i prosesser og prosjekter. Ekspertisen og aktiviteter knyttet til menneskelige og organisatoriske faktorer er tilpasset virksomheten, prosessen eller prosjektet. Rollene og ansvaret, samt ansvarligheten og i hvilken grad man skal involvere ekspertisen på menneskelige faktorer, er definert i prosessen eller prosjektplanen.

#### 2.3.6 Referanser og standarder

- [Ansvarlighet og ansvar for sikkerhet](#) (SKYbrary)

#### 2.3.7 Relevante tema for tilsyn

For tilsyn vil hovedpunktene her være et spørsmål om grad. Spørsmålet som må besvares, er «i hvilken grad gjenspeiler oppgitt informasjon virkeligheten»?

En gjennomgang av virksomhetens system for styring av kompetanse vil være veien å gå for å få svar på de fleste spørsmålene i denne delen.

## 2.4 Samråd med personalet og andre parter

### 2.4.1 Lovbestemt krav

- 2.4.1. Personalet, deres representanter og eksterne berørte parter skal, når det er hensiktsmessig og relevant, rådspørres når det gjelder utvikling, vedlikehold og forbedring av sikkerhetsstyringssystemet i de relevante delene de har ansvar for, herunder sikkerhetsaspekter ved driftsmetoder.
- 2.4.2. Virksomheten skal fremme samråd med personale ved å innføre metoder og midler for å la personalet delta, registrere personalets synspunkter og gi tilbakemelding på personalets synspunkter.

### 2.4.2 Formål

Søker skal dokumentere at de aktivt involverer sitt eget personell (eller deres representanter), samt eksterne interessenter ved anvendelse og utvikling av sikkerhetsstyringssystemet. Dette vil også gi sikkerhetsmyndighetene en indikasjon på hvordan sikkerhetskulturen er i virksomheten, og hvor aktivt de involverer relevante tredjeparter i håndtering av sikkerhet der relevant risiko er delt mellom flere interessenter.

Virksomheten innser at ingen enkeltpersoner i en virksomhet har all informasjon som er nødvendig for å håndtere sikkerheten. Prosesseksperter, sikkerhetseksperter, stabsfunksjoner, førstelinjestøtte, ledelse og arbeidsledere, fagforeninger og eksterne leverandører har og anvender kunnskap og informasjon som er viktig for sikkerheten. De må kunne komme sammen for å drøfte og uttrykke sine synspunkter for å få en best mulig forståelse av de reelle forholdene på arbeidsplassen. Det må rettes oppmerksomhet mot organisatorisk samhandling mellom tjenester, avdelinger og virksomheter. Det oppfordres til utveksling av ideer og informasjon om analyse og håndtering av risiko, ulykker og uønskede hendelser.

Et miljø med tillit som støtter engasjement i rapportering av sikkerhetskritisk informasjon og deltakelse i analysering av farlige situasjoner og uønskede hendelser. I tillegg er det viktig med tidlig innspill fra driftspersonell når det gjennomføres risikovurderinger, ved design og bygging av tekniske installasjoner og ved utarbeidelse av nye prosedyrer.

### 2.4.3 Forklarende merknader

Disse eksterne partene (**2.4.1**) kan konsulteres i saker som er relevante for styringssystemet. For eksempel kan leverandører være ansvarlig for noen sikkerhetsrelaterte oppgaver, som klargjøring av tog eller vedlikehold av infrastrukturen. Når prosedyrene for klargjøring av tog eller vedlikehold av infrastrukturen gjennomgås og revideres, er det god praksis at disse leverandørene er involvert i prosessen.

Med eksterne interessenter menes virksomheter som har et grensesnitt med søkeren, som for eksempel leverandører, underleverandører, partnere, relevante myndigheter og nødetater.

Utvikling av en positiv sikkerhetskultur fremmes av god og relevant kommunikasjon til riktig tid.

### 2.4.4 Dokumentasjon

- Søker skal fremlegge opplysninger om prosessen for å konsultere relevante interessenter (også eksterne interessenter), herunder hvordan disse konsultasjonene fører til endringer i sikkerhetsstyringssystemet eller endringer i spesifikke driftsprosedyrer (**2.4.1**), (**2.4.2**)

The NSA NO 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.

- *Søker skal fremlegge informasjon om system for tilbakemelding til personellet om utfallet av konsultasjonene. (2.4.2)*

#### 2.4.5 Eksempler på dokumentasjon

Proessen eller prosedyren for å konsultere relevante interessenter i utviklingen av sikkerhetsstyringssystemet.

Eksempler på møtereferater etter møter med ansatte og utfallet av dem.

Eksempler på hvordan meninger og forslag fra ansatte blir samlet når det skal gjøres endringer (for eksempel et utkast til/endret/ny driftsprosedyre) og hvordan de behandles.

Det fremlegges dokumentasjon/prosedyre som viser hvordan driftspersonellet, som skal håndtere et nytt eller utviklet teknisk system, blir involvert tidlig (planlegging og utvikling) av arbeidet for å samle inn opplysninger, for eksempel om maskinens grensesnitt.

Det foreligger prosedyrer som beskriver hvordan menneskelige og organisatoriske faktorer skal håndteres, og hvordan prosedyrene formidles i virksomheten. Grensesnittene henger sammen med virksomhetens art og omfang. Eksempelvis: prosjekter, granskning av hendelser og ulykker, risikoanalyser og andre sikkerhetsrelaterte aktiviteter for eget personell, samarbeidspartnere og leverandører.

Virksomheten skal klart definere sikkerhetsforventninger og påkrevd atferd. Organisatoriske prioriteringer blir tilpasset for å unngå motstridende mål. En beskrivelse av prosess for planlegging, risikovurdering og kontrollaktiviteter for å sikre at sikkerheten ikke går på bekostning av andre forretningsmål, for eksempel bruk av veloverveide beslutninger. Sikkerhetsmål er knyttet til sikkerhetskulturen. Ledelsen har en aktiv rolle i planleggingen og gjennomføringen av nødvendige endringer i sikkerhetskulturen.

#### 2.4.6 Relevante tema for tilsyn

Konsultasjon og involvering av relevant personell, både internt og eksternt, er en viktig del av å sikre at de med relevant erfaring har en positiv innvirkning på virksomhetens sikkerhetsstyringssystem.

Tilsyn på dette området bør rettes mot historikk om hvordan personell og eksterne parter blir konsultert og hvordan deres kommentarer blir tatt i betraktning, samt gi en oversikt over endringer i sikkerhetsstyringssystemet som stammer fra dette feltet.

Det bør rettes spesiell oppmerksomhet mot hvordan tilbakemelding gis og hvordan man lærer av dette.

### 3 Planlegging

#### 3.1 Tiltak for å håndtere risiko

##### 3.1.1 Lovbestemt krav

###### 3.1.1. Risikovurdering

###### 3.1.1.1. Virksomheten skal

- (a) identifisere og analysere driftsmessig, organisatorisk og teknisk risiko som er relevant for virksomhetens art og omfang; slik risiko skal omfatte risiko som skyldes menneskelige og organisatoriske faktorer som arbeidsbelastning, arbeidets utforming, tretthet eller prosedyrenes egnethet samt andre berørte parter virksomhet (se nr. 1 Virksomhetens kontekst),
- (b) vurdere risiko nevnt i bokstav a) ved hjelp av egnede metoder for risikovurdering,
- (c) utvikle og innføre sikkerhetstiltak, med angivelse av tilhørende ansvarsområder (se nr. 2.3 Roller, ansvar og myndighet i virksomheten),
- (d) utvikle et system for å overvåke hvor effektive sikkerhetstiltakene er (se nr. 6.1 Overvåking),
- (e) erkjenne behovet for å samarbeide med andre berørte parter (for eksempel jernbaneforetak, infrastrukturforvaltere, produsenter, leverandører av vedlikeholdstjenester, enhet med ansvar for vedlikehold, innehavere av jernbanekjøretøy, tjenesteytere og oppdragsgivere), når det er hensiktsmessig, om felles risiko og innføring av egnede sikkerhetstiltak,
- (f) informere personalet og eksterne berørte parter om risiko (se nr. 4.4 Informasjon og kommunikasjon).

3.1.1.2. Ved vurderingen av risiko skal virksomheten ta hensyn til behovet for å fastsette, skape og opprettholde et trygt arbeidsmiljø som er i samsvar med gjeldende regelverk, særlig direktiv 89/391/EØF.

###### 3.1.2. Planlegging av endringer

3.1.2.1. Virksomheten skal identifisere mulig sikkerhetsrisiko og hensiktsmessige sikkerhetstiltak (se nr. 3.1.1 Risikovurdering) før gjennomføringen av en endring (se nr. 5.4 Endringsstyring) i samsvar med den risikohåndteringsprosessen som er angitt i forordning (EU) nr. 402/2013<sup>(1)</sup>, herunder vurdere sikkerhetsrisiko som følge av selve endringsprosessen.

##### 3.1.2 Formål

Dette kravet er kjernen i sikkerhetsstyringssystemet, da det er rettet mot å få søkeren til å vise hvordan deres systemer identifiserer og håndterer risiko de står overfor. Det krever også at søkeren viser hvordan de anvender utfallet fra risikovurderingen, for å forbedre risikostyringen og hvordan dette sjekkes over tid. Det er viktig å huske på at dette kravet ikke direkte handler om å håndtere risiko i forbindelse med krav til bruk av felles sikkerhetsmetode for risikovurdering (CSM RA), men det har flere likhetstrekk. Det gjøres oppmerksom på at det stilles krav til at risiko knyttet til menneskelige og organisatoriske faktorer skal inkluderes i vurdering av risiko, som for eksempel utforming av arbeidsoppgaver og risikostyring for tretthet.

Dokumentasjon på hvordan virksomheten styrer og formidler risiko som en del av sikkerhetsstyringssystemet, må beskrives i søknaden, og sikkerhetsstyringssystemet bør gjenspeile de

<sup>(1)</sup> Kommisjonens gjennomføringsforordning (EU) nr. 402/2013 av 30. april 2013 om den felles sikkerhetsmetoden for risikoevaluering og -vurdering og om oppheving av forordning (EF) nr. 352/2009 (EUT L 121 av 3.5.2013, s. 8).

risikoene virksomheten står overfor med hensyn til art og omfang (se kapittel 1, Virksomhetens kontekst). Virksomheten må beskrive både risiko som oppstår som følge av egen virksomhet og risiko som oppstår i forbindelse med tredjeparters aktiviteter der det er relevant.

En felles forståelse i virksomheten om hvordan man forebygger større ulykker, er en forutsetning for god sikkerhetsstyring. At en hendelse ikke forekommer ofte, bør ikke føre til at risikoen ved den blir ignorert. For å danne et realistisk bilde av et bestemt hendelsesforløp, bør både sikkerhetsstyringsekspertene og personell i den skarpe enden av virksomheten bidra til analyse og vurdering av risiko. Resultatene fra disse vurderingene formidles i et tilgjengelig og forståelig format til alle relevante aktører. Ledelsen legger aktivt til rette for at det etableres prosesser for å drøfte all relevant risiko som må håndteres, for å sikre en felles forståelse av, og dokumentasjon omkring, disse. Risiko skal overvåkes og håndteres gjennom alle virksomhetens faser.

### 3.1.3 Forklarende merknader

Søkeren må vise hvordan de overholder direktiv 89/391/EØF (arbeidsmiljødirektivet) og korresponderende forordninger. Vurderingen vil fokusere på hvordan utfordringer i arbeidsmiljøet løses, og ikke på selve utfordringen. Temaer som tretthet og stresshåndtering, samt testing av fysisk og mental helse, kan håndteres innenfor rammene for arbeidsmiljø og sikkerhet. Dette vil man blant annet forvente å finne spor av i system for styring av kompetanse i virksomheten (for eksempel for opptrening etter langtidsfravær) og ved delegering av oppgaver (ansatte skal kun tildeles bestemte oppgaver hvis man mener de passer for dem), som angitt i TSI-OPE.

«Aktiviteter» **(3.1.1.1 (a))** viser her til både handlinger som interessenter (leverandører og andre) utfører på vegne av virksomheten som søker, og aktiviteter der virksomheten samhandler med andre interessenter, samt eiendeler som brukes for å utføre disse handlingene. Hovedpoenget er at søkeren må dokumentere at de har en robust prosess for risikovurdering, og at alle relevante risikoer håndteres. Enkelte risikoer (for eksempel hydrogeologisk risiko, risiko ved planoverganger, stein som kastes på tog, ulovlig ferdsel i spor) må også tas i betraktning av virksomheten når dette er hensiktsmessig. Disse utfordringene er relatert til driftsmessig risiko (siden de alle påvirker togdriften).

«Andre interessenter» viser til både virksomheter og enkeltpersoner. Dette kan være eksterne parter i jernbanesystemet **(1.1.1 (c))**.

En endring trenger ikke å være sikkerhetsrelatert **(3.1.2.1)**. Virkningen av eventuelle sikkerhetsrelaterte endringer må vurderes, og hensiktsmessige tiltak må identifiseres for å redusere de aktuelle risikoene til et akseptabelt nivå. Implementeringen av endringer kan også føre til sikkerhetsrisikoer, særlig når det besluttes å utsette implementeringen av en endring når det er nødvendig for å unngå at en annen sikkerhetsrisiko oppstår. Risikostyring **(3.1.1.1)** gjelder imidlertid ikke bare for endringer. Generelt skal virksomheten sørge for at sikkerhetsrisikoene som er knyttet til virksomhetens drift håndteres. Behovet for å identifisere, administrere og håndtere disse sikkerhetsrisikoene som en del av søkerens sikkerhetsstyringssystem, går derfor videre enn endringer og anvendelse av CSM RA.

CSM RA gjelder for alle tekniske, driftsmessige eller organisatoriske endringer. For hver sikkerhetsrelatert endring, må søker/forslagsstiller først avgjøre om endringen er vesentlig. Hvis en endring anses å være vesentlig, må det dokumenteres at risiko som er knyttet til endringen er akseptabel ved bruk av prinsippene som er beskrevet i CSM RA. Tiltakene som identifiseres fra CSM RA-prosessen skal være hensiktsmessig implementert i systemet som endres. Risikovurderingen som gjennomføres må deretter vurderes av et uavhengig vurderingsorgan eller anerkjent organ. Vurderingsorganet utarbeider en sikkerhetsvurderingsrapport som er en vurdering av om risikovurderingen er gjennomført i henhold til kravene i CSM RA eller ikke. Nasjonale sikkerhetsmyndigheter vil vurdere slike rapporter i sin tilsynsaktivitet,

men kan ikke komme med innsigelser til resultatene i rapporten, med mindre de har grunn til å tro at prosessen med å vurdere risikovurderingen ikke har blitt fulgt som den skulle. Når endringen er sikkerhetsrelatert men ikke vesentlig, må søker/forslagsstiller dokumentere sin beslutning, og det vil fortsatt være nødvendig å risikovurdere endringen ved anvendelse av egne prosesser i sikkerhetsstyringssystemet. I så fall er det søkers ansvar å velge egnede risikovurderingsmetoder, for å fastslå at tiltakene som er etablert er hensiktsmessige for å håndtere aktuell risiko. Virksomheten kan velge å anvende CSM RA selv om endringen ikke er vurdert til å være vesentlig, for eksempel hvis man føler at endringen av kommersielle eller samfunnsmessige årsaker fortjener en uavhengig vurdering av arbeidet virksomheten har utført.

CSM RA inneholder seks kriterier som skal undersøkes for å fastslå om endringen er vesentlig. Disse er:

- **følger av svikt:** realistisk situasjon basert på det verst tenkelige tilfellet av svikt i det systemet som er til vurdering, idet det tas hensyn til sikkerhetsbarrierer utenfor systemet,
- **nyskaping benyttet ved gjennomføring av endringen:** Dette gjelder både hva som er nyskapende i jernbanesektoren, og hva som er nytt for virksomheten som gjennomfører endringen,
- **endringens kompleksitet,**
- **overvåking:** manglende evne til å overvåke den gjennomførte endringen i hele systemets levetid og treffe egnede tiltak,
- **reversibilitet:** manglende evne til å gå tilbake til systemet slik det var før endringen,
- **addisjonalitet:** vurdering av betydningen av endringen, idet det tas hensyn til alle nyere sikkerhetsrelaterte endringer av det systemet som er til vurdering, og som ikke ble bedømt som vesentlige.

Disse elementene brukes til å vurdere hvordan beslutninger om «vesentlighet» i henhold til CSM-RA er tatt.

Selv om risikostyringsprosessen som er fastsatt i CSM RA gjelder for sikkerhetsrelaterte og vesentlige endringer, er prinsippene som ligger til grunn for risikostyringsprosessen som er fastsatt i forordningen, vanlig praksis for risikostyring.

Det er en systematisk tilnærming for å identifisere sikkerhetskritiske arbeidsoppgaver og prosesser, og metoder fra området innen menneskelige faktorer brukes til å analysere sikkerhetskritiske arbeidsoppgaver, for eksempel oppgaveanalyser. Det bør brukes profesjonell ekspertise på menneskelige faktorer for å velge og anvende egnede metoder.

Risikovurderingsprosessen bør beskrive involveringen av menneskelige og organisatoriske faktorer og relevant kompetanse. Den kan for eksempel inneholde en beskrivelse av i hvilken grad ekspertise på menneskelige og organisatoriske faktorer skal være involvert i risikoanalyse, og i hvilken grad kompetanse på menneskelige og organisatoriske faktorer er nødvendig.

Det er beskrevet egnede metoder for å integrere menneskelige og organisatoriske faktorer i risikovurderinger. Dette kan være oppgaveanalyser, analyse av brukervennlighet og ulike risikovurderingsmetoder som inkluderer menneskelige og organisatoriske faktorer.

### 3.1.4 Dokumentasjon

- *Søkeren skal fremlegge dokumentasjon for at det foreligger en risikovurderingsprosess (inkludert beskrivelse av metodene som brukes, involvert personell og eventuell validering eller verifisering) som omfatter både risiko identifisert som vesentlige endringer under CSM RA og risiko som ikke anses som*

vesentlig, men som likevel skal kontrolleres, og prosessen dekker all driftsmessig, organisatorisk og teknisk risiko. **(3.1.1.1.(a),(b))**

- Dokumentasjon på at risiko forbundet med menneskelige og organisatoriske faktorer er tatt hensyn til i vurderingene. Strategien for menneskelige og organisatoriske faktorer skal vise hvordan og når menneskelige og organisatoriske faktorer integreres i risikovurderingsprosessen, samt vise anvendelsen av hensiktsmessige metoder og ekspertise **(3.1.1.1(a))**
- Dokumentasjon på måter å involvere relevante tredjeparter i risikovurderingsprosessen, herunder hvordan risiko fra tredjeparter som påvirker jernbanevirksomhetens eller infrastrukturforvalterens aktiviteter, håndteres **(3.1.1.1(a)), (3.1.1.1(e)), (3.1.1.1(f))**
- Dokumentasjon på at søkeren har etablert en prosess for å utvikle og iverksette tiltak for å håndtere risiko, herunder hvem som er ansvarlig for å sikre at de gjennomføres **(3.1.1.1 (c))**.
- Søkeren må beskrive hvordan de involverer og formidler resultatene av risikovurderinger og tilhørende tiltak til relevant personell **(3.1.1.1(f))**
- Søkeren skal vise hvordan effekten av tiltakene overvåkes, herunder hvordan prosesser eller prosedyrer oppdateres etter behov **(3.1.1.1 (d))**
- Sammen med dokumentasjonen skal søkeren beskrive hvordan behovet for å overholde annen gjeldende lovgivning overholdes, som for eksempel bestemmelsene i rådsdirektiv 89/391/EØF (arbeidsmiljødirektivet) **(3.1.1.2)**
- Søker fremlegger dokumentasjon som viser at virkningen av enhver endring systematisk evalueres. Dette vil innebære bruk av risikovurdering, herunder bruk av CSM RA, for å identifisere risiko og tiltak. Søker fremlegger også dokumentasjon på at tiltakene som ble identifisert i forbindelse med planlagt endring er gjennomført **(3.1.2.1)**

### 3.1.5 Eksempler på dokumentasjon

En risikovurderingsprosess eller -prosedyre, inkludert hvordan og når Feilmode- og effektanalyse (FMEA), Identifikasjon og analyse av farlige og operasjonelle forhold (HAZOP) eller andre teknikker brukes til å understøtte gjennomføringen av tiltak for å håndtere risiko.

Dokumentasjon, som for eksempel et fareregister, som viser at virksomheten har en systematisk vurdering av identifiserte farer som første trinn i sin risikostyring. Virksomheten skal overvåke sin styring av risiko, og et resultat av dette vil være å oppdatere fareregisteret når nye risikofaktorer oppdages, og supplere det med relevant informasjon om tiltak som er iverksatt for å holde risikoen under kontroll (for eksempel teknisk utstyr, driftsprosedyrer, personalopplæring).

En oversikt over hvordan menneskelige faktorer tas i betraktning i risikovurderingsprosessen, og hvordan eventuelt relevante tredjeparter er involvert.

Prosedyre for å formidle resultatene av risikovurderinger til ansatte, med eventuelle eksempler.

Prosedyre for å overholde annen relevant EU-lovgivning, som for eksempel rådsdirektiv 89/391/EØF (arbeidsmiljødirektivet), med hensyn til risiko knyttet til ansatte (død, midlertidig eller permanent personskade, nestenulykker).

En beskrivelse av prosessen som sikrer at sikkerhetsrelaterte oppgaver som delegeres til relevant personell er utformet på en slik måte at:

- *størrelsen på oppgavene som skal utføres ikke er for stor når en sikkerhetsrelatert oppgave utføres*
- *når sikkerhetsrelaterte oppgaver er kombinert, kan virksomheten vise at sikkerhetsnivået opprettholdes*

- *det ikke er motsetninger mellom utførelsen av sikkerhetsrelaterte oppgaver og andre mål som er delegert til ansatte (i samsvar med 2.1.1 (j)).*

En strategi for menneskelige og organisatoriske faktorer som knytter sammen risikovurderingsprosessene, og som viser at resultatene fra risikoanalyser blir anvendt og at tiltak blir implementert og evaluert.

### 3.1.6 Referanser og standarder

- [Veileder for Byrået for anvendelse av CSM vedrørende risikovurdering](#)
- [Risikoakseptkriterier for tekniske systemer og driftsprosedyrer som anvendes i ulike bransjer](#)
- [Retningslinjer for gjennomføring av \(EU\) forordning 2015/1136 om harmoniserte standarder \(CSM DT\) i virkeområdet til CSM vedrørende risikovurdering](#)
- ISO 31000:2009 Risikostyring
- ISO 31010:2009 Risikostyring - risikovurderingsteknikker

### 3.1.7 Relevante tema for tilsyn

Proessen for å håndtere risiko bør være kjernen i sikkerhetsstyringssystemet. Det bør være mulig ut fra samtaler og kontroll av dokumentasjon og prosesser i forbindelse med tilsyn å finne ut om dette stemmer med virkeligheten. Eventuelle funn fra tilsyn som vil være relevant for fremtidig fornyelse av et felles sikkerhetssertifikat eller sikkerhetsgodkjenning, er av stor betydning. I tillegg kan eventuelle funn fra tilsyn med risikovurderingsprosesser være innspill i tilsynsstrategien til nasjonale sikkerhetsmyndigheter.

Følgende informasjon kan fungere som innspill for senere tilsyn:

- *En oversikt over farer/risiko i virksomheten, identifiserte tiltak og status for tiltak*
- *En klassifisering av farlige hendelser etter type, konsekvens eller årsaker*
- *Resultater fra risikovurderinger, inkludert rapporter fra risikovurderingsorganet eller -organene der det er aktuelt*
- *Begrunnelse for bruken av risikovurderingsmetoder (for eksempel FMECA, FTA, ETA, HAZOP), inkludert hvordan konsekvens og sannsynlighet er bestemt, samt hvordan akseptkriterier for risiko er fastsatt*

Ansatte med ansvar knyttet til risikovurdering bør være oppmerksomme på sin rolle og betydningen av prosessen, samt inneha kompetanse til å utføre oppgaven på en hensiktsmessig måte.

Det er spesielt viktig at flere eksempler på risikovurderinger undersøkes, da det av disse vil fremkomme om risikoene vurderes på riktig måte ved hjelp av egnede metoder. Ved tilsyn hos virksomheten bør det påvises at de identifiserte tiltakene er på plass.

## 3.2 Sikkerhetsmål og planlegging

### 3.2.1 Lovbestemt krav

3.2.1.	Virksomheten skal fastsette sikkerhetsmål for relevante funksjoner på relevante nivåer for å opprettholde og så langt det er praktisk mulig forbedre sikkerhetsnivået.
3.2.2.	Sikkerhetsmålene skal <ul style="list-style-type: none"><li>(a) være i samsvar med sikkerhetspolitikken og virksomhetens strategiske mål (når det er relevant),</li><li>(b) være knyttet til de prioriterte risikoene som påvirker virksomhetens sikkerhetsnivå,</li><li>(c) kunne måles,</li><li>(d) ta hensyn til gjeldende lovfestede krav og andre krav,</li><li>(e) gjennomgås i forhold til oppnådde resultater og revideres ved behov,</li><li>(f) formidles.</li></ul>
3.2.3.	Virksomheten skal ha en eller flere planer som beskriver hvordan den vil oppfylle sikkerhetsmålene sine.
3.2.4.	Virksomheten skal beskrive strategien og planen(e) som brukes til å overvåke at sikkerhetsmålene oppfylles (se nr. 6.1 Overvåking)

### 3.2.2 Formål

Sikre at virksomheten oppfyller relevante lovfestede krav og sikre at konseptet om kontinuerlig forbedring av sikkerheten formidles til ansatte og at ledelsen står for dette.

Virksomheten må vise at det foreligger meningsfylte sikkerhetsmål og en prosess for å gjennomføre og overvåke dem i løpet av deres virketid.

### 3.2.3 Forklarende merknader

Sikkerhetsnivået betyr her virksomhetens nivå på sikkerhet både med tanke på virksomhetens fastsatte sikkerhetsmål og sikkerhetsstyringssystemets ytelse, samt alle prosesser og prosedyrer som underbygger dette.

Begrepet «sikkerhetsmål» har vanligvis en kvantitativ betydning. Sikkerhetsmål er forskjellige fra Felles sikkerhetsmål (CST) som er fastsatt på medlemsstatsnivå, men enkelte virksomheter kan bruke sistnevnte som mål som skal nås for å opprettholde eller forbedre sikkerheten.

Sikkerhetsmål er knyttet til risiko, og påvirker virksomhetens sikkerhetsnivå. Sikkerhetsmål kan være kvantitative, representert ved en reduksjon av antall hendelser som en absolutt verdi eller i prosent. Sikkerhetsmål kan også være kvalitative, uttrykt som en generell verdi som «sikkerheten på planoverganger vil bli forbedret» eller «det nåværende sikkerhetsnivået vil bli opprettholdt».

Med PDCA-hjulet kan målene vurderes regelmessig, og resultatene av risikovurdering og tidligere overvåking tas i betraktning. Granskning av ulykker og uønskede hendelser kan også tas i betraktning. Virksomheten må angi prioriteringer for å opprettholde og forbedre sikkerhetsnivået der det måtte være nødvendig.

Utfallet av virksomhetens overvåking av egne sikkerhetsindikatorer (som underbygger virksomhetens beslutninger om risikostyring), kan være innspill for å sette opp og vurdere sikkerhetsmål.

### Dokumentasjon

The NSA NO has kindly provided its assistance to the revision of the translation of this guide.  
Where it appears that there are differences between the translated version and the English version, the English version takes precedence.

- *Det foreligger et SMART-sett med sikkerhetsmål som passer inn i virksomhetens øvrige forretningsbehov (3.2.1), (3.2.2 (a),(b)),(c))*
- *En redegjørelse som oppgir de lovfestede kravene og hvordan de overholdes (3.2.2 (d))*
- *Beskrivelse av hvordan disse målene kan oppnås og formidles til relevant personell (3.2.2 (f)), (3.2.3)*
- *Det foreligger en overvåkingsprosess som er i samsvar med kravene i CSM Monitoring (forordning (EU) 1078/2012), for å sikre at prosessen er forenlig med formålet, og for at virksomheten kan oppnå sine mål (3.2.2 (e)), (3.2.4)*

#### 3.2.4 Eksempler på dokumentasjon

Proessen som viser hvordan sikkerhetsmål er prioritert, hvordan de blir overvåket, og hvordan konflikter med andre mål unngås, eventuelt løses. Dette bør inkludere nivå på målene som er satt og hvordan sikkerhetsmål bidrar til å oppnå andre mål på andre nivåer i virksomheten der dette er hensiktsmessig, samt hvordan samhandling sikres, tidsperiode for sikkerhetsmål og eventuelle nødvendige kvalitative eller kvantitative data.

Sikkerhetsmål og planen som leveres sammen med prosessen som skal følges når det ser ut til at sikkerhetsmålene ikke kan nås.

Proessen eller prosedyren for hvordan man bruker resultatet fra overvåkingsprosessen til å fastsette sikkerhetsmål, planlegge tiltak for å oppnå sikkerhetsmål og fastsette relevante indikatorer for å nå sikkerhetsmålene.

#### 3.2.5 Relevante tema for tilsyn

Et nøkkelspørsmål for tilsyn vil være hvor oppnåelige de fastsatte målene er i praksis, og hva som skjer dersom det begynner å bli klart at sikkerhetsmålene sannsynligvis ikke kan nås.

Hvordan sikkerhetsmålene er fastsatt og vurdert - at målene fokuserer på sårbare eller kritiske aktiviteter/kontroller og anvender resultat- og aktivitetsindikatorer.

Hvordan virksomheten viser kontinuerlig forbedring av risikostyring gjennom sine sikkerhetsmål.

Vurdering av virksomhetens mulighet for å kunne overvåke sitt sikkerhetsnivå på en hensiktsmessig måte, og om den bruker CSM monitoring for å vurdere nivået mot sikkerhetsmål og relaterte sikkerhetsindikatorer.

Ta et eksempel på et mål (som for eksempel er definert for noen år siden) og se på hvilken måte det kan spores fra det ble fastsatt til det ble nådd (eller ikke nådd).

## 4 Støtte

### 4.1 Ressurser

#### 4.1.1 Lovbestemt krav

4.1.1. Virksomheten skal sørge for de ressursene, herunder kvalifisert personale og effektivt og brukbart utstyr, som er nødvendige for å opprette, gjennomføre, vedlikeholde og kontinuerlig forbedre sikkerhetsstyringssystemet

#### 4.1.2 Formål

Formålet med dette kravet er å sørge for at virksomheten har prosesser på plass for å sikre tilstrekkelige ressurser, som teknisk utstyr, systemer eller kompetent personell, slik at virksomheten gjennom sitt sikkerhetsstyringssystem kan håndtere risiko som oppstår i forbindelse med sin virksomhet.

#### 4.1.3 Forklarende merknader

Tilstrekkelige ressurser er på plass for kontinuerlig å kunne forbedre sikkerhetskulturen. Sikkerhetskulturen er et punkt i budsjettet. Sikkerhetskulturen er imidlertid ikke noe som vurderes en gang i året, men utviklingen av den avhenger av kontinuerlig innsats. Det er derfor viktig at tiltak knyttet til målene for sikkerhetskultur (**7.2.3**) gjenspeiler dette.

#### 4.1.4 Dokumentasjon

- Informasjon om system for styring av kompetanse. Hvordan virksomheten sikrer at den har tilstrekkelig kompetent personell dersom virksomheten ikke kan dokumentere at de har et system for styring av kompetanse (**4.1.1**)
- Informasjon om hvordan virksomheten skal sørge for at den har nødvendige ressurser, slik at virksomheten kan etablere og opprettholde et hensiktsmessig sikkerhetsstyringssystem som håndterer risiko (**4.1.1**)
- Informasjon om organisering av vedlikeholdsfunksjoner og hvordan vedlikeholdsfunksjoner er relatert til tilstrekkelig forvaltning av ressurser (**4.1.1**)

#### 4.1.5 Eksempler på dokumentasjon

En redegjørelse for hvordan krav til personell bestemmes, samt detaljer om relevante prosedyrer eller prosesser der ytterligere informasjon kan bli funnet.

Prosedyre for behandling av kompetanse eller detaljer om en prosess som skal sikre at virksomheten har kompetent personell i relevante funksjoner, med detaljerte opplæringsprogrammer etter behov (**se også 4.2**).

En redegjørelse som beskriver prosessen for tildeling av ressurser for å oppfylle driftsmessige behov, samt detaljer om relevante prosedyrer eller prosesser der ytterligere informasjon kan bli funnet.

Et dokument som beskriver hvordan ressurser om vedlikehold tildeles (inkludert personell og at nødvendig utstyr er på plass).

#### 4.1.6 Relevante tema for tilsyn

Sjekk at kravene som stilles til nødvendige ressurser (inkludert teknisk utstyr, systemer eller kompetent personell) henger sammen med funnene fra risikovurderingene.

Ved å sjekke system for styring av kompetanse, kan nasjonale sikkerhetsmyndigheter kontrollere at virksomheten har på plass system for å identifisere og opprettholde personell med egnede ferdigheter slik at de kan utføre sine oppgaver på en trygg måte. Hvordan systemet for styring av kompetanse holdes oppdatert er viktig.

For vedlikeholdsaktiviteter som er satt ut på kontrakt, kan nasjonale sikkerhetsmyndigheter kontrollere at jernbanevirksomheten eller infrastrukturforvalteren har på plass et system for å sikre at leverandørene de bruker, leverer et trygt produkt.

Sjekk av gap i utvalgte områder i sikkerhetsstyringssystemet kan brukes som en indikator på om det er tilstrekkelig nok kompetent personell.

Sjekk av måten teknisk utstyr brukes på, for eksempel hvor stort behovet er for reservedeler, kan være en indikasjon på kvaliteten på det tekniske utstyret og på denne måten indikere utilstrekkelige tekniske ressurser.

## 4.2 Kompetanse

### 4.2.1 Lovbestemt krav

4.2.1.	Virksomhetens styring av kompetanse skal sikre at personale som har en rolle som påvirker sikkerheten, har kompetanse innenfor de sikkerhetsrelaterte oppgavene de har ansvar for (se nr. 2.3 Roller, ansvar og myndighet i virksomheten), og det skal minst omfatte <ul style="list-style-type: none"><li>(a) fastsettelse av den kompetansen (herunder kunnskaper, ferdigheter, atferd og holdninger på andre områder enn tekniske områder) som kreves for sikkerhetsrelaterte oppgaver,</li><li>(b) utvelgingsprinsipper (grunnleggende utdanningsnivå, psykisk og fysisk skikkethet som kreves),</li><li>(c) grunnleggende opplæring, erfaring og kvalifikasjoner,</li><li>(d) løpende opplæring og regelmessig ajourføring av eksisterende kompetanse,</li><li>(e) regelmessig vurdering av kompetanse og kontroll av psykisk og fysisk skikkethet for å sikre at kvalifikasjonene og ferdighetene opprettholdes over tid,</li><li>(f) særskilt opplæring i relevante deler av sikkerhetsstyringssystemet slik at de kan utføre de sikkerhetsrelaterte oppgavene</li></ul>
4.2.2.	Virksomheten skal sørge for et opplæringsprogram som nevnt i nr. 4.2.1 bokstav c), d) og f) for personale som utfører sikkerhetsrelaterte oppgaver, som sikrer at <ul style="list-style-type: none"><li>(a) opplæringsprogrammet gjennomføres i samsvar med de fastsatte kompetansekravene og personalets individuelle behov,</li><li>(b) opplæringen i relevante tilfeller sikrer at personalet kan fungere under alle driftsforhold (under normale forhold, ved driftsforstyrrelser og i nødssituasjoner),</li><li>(c) opplæringens varighet og hyppigheten av oppfriskingsopplæringen er tilpasset opplæringsmålene,</li><li>(d) det føres registre for alt personale (se nr. 4.5.3 Styring over dokumentert informasjon),</li><li>(e) opplæringsprogrammet gjennomgås og revideres regelmessig (se nr. 6.2 Internrevisjon), og endres ved behov (se nr. 5.4 Endringsstyring).</li></ul>
4.2.3.	Det skal finnes ordninger for personale som kommer tilbake til arbeidet etter ulykker/hendelser eller langt fravær fra arbeidet, herunder tilleggsopplæring ved behov

### 4.2.2 Formål

Formålet med dette kravet er å sikre at virksomheten har på plass hensiktsmessig struktur og ressurser for å håndtere risikoen de står overfor, slik at kompetent personell blir satt til sikkerhetsfunksjonene, og da særlig sikkerhetskritiske funksjoner. System for styring av kompetanse vil også gi virksomheten muligheten til å opprettholde kompetansen, kunnskapen og erfaringen til de ansatte over tid.

Kompetanse spiller en viktig rolle for å sikre at aktivitetene utføres på en tilfredsstillende måte. Behovet for å ha kompetent personell omfatter både førstelinjestøtte (inkludert leverandører) og ansatte i lederstillinger. Krav til lederkompetanse blir ofte oversett, men ledere treffer imidlertid viktige beslutninger som kan ha fundamental og omfattende innvirkning på helse og sikkerhet. Dette kan omfatte å sørge for opplæring av alle ansatte i henhold til relevante sikkerhetsstandarter. Ledelsen skal også sørge for å opprettholde kompetansen til de ansatte, også når det oppstår problemer som for eksempel tilgjengelighet på personell. I tillegg er ledelsen ansvarlig for å overvåke kompetansen om standarder som skal følges.

I denne sammenheng er sikkerheten sett på som en integrert del av profesjonell atferd og fagkompetanse - og ikke som et «ekstra lag» som skal legges på toppen av faglige ferdigheter. I tillegg vil evnen til en virksomhet med hensyn til å håndtere uventede hendelser, være avhengig av kompetansen til førstelinjepersonell og deres overordnede. Slik kompetanse kan utvikles med trening og regelmessig opplæring i komplekse scenarier.

#### 4.2.3 Forklarende merknader

Et opplæringsprogram **(4.2.2)** kan etableres via et tredjeparts kurscenter. I slike tilfeller skal virksomheten sørge for at kurscenteret har kompetanse til å levere relevante tjenester, enten ved at de er sertifisert som et anerkjent opplæringscenter etter nasjonal eller europeisk ordning, eller ved direkte overvåking av opplæringen og resultatene den gir. Et kurscenter kan enten levere all nødvendig opplæring, eller det kan levere deler av nødvendig opplæring til en virksomhet, basert på hvilken kompetanse kurscenteret har på ulike områder.

«Holdning» **(4.2.1 (a))** brukes til å beskrive hvordan mennesker reagerer på bestemte situasjoner og hvordan de oppfører seg generelt (for eksempel å være på offensiven, ha evnen til å komme overens med andre mennesker). Dette er svært viktig for å kunne samkjøre ulike deler av arbeidet i sikkerhetsstyringssystemet.

Det bør være en systematisk tilnærming for å sikre at kompetansen om menneskelige og organisatoriske faktorer er tilgjengelig, enten i relevante roller basert på behovsanalyse eller gjennom jobbsamtaler.

Kompetansen om menneskelige og organisatoriske faktorer bør for eksempel brukes i prosjekter i forbindelse med ny eller modifisert design, ved ulykkesanalyse for å gi et ikke-teknisk perspektiv, eller vedrørende problemer med menneskelige faktorer.

#### 4.2.4 Dokumentasjon

- Søker skal fremlegge opplysninger om sitt system for styring av kompetanse og hvordan det fungerer for å oppfylle forholdene som er oppgitt i kravene **(4.2.1), (4.2.2(a)-(f))**
- Dokumentasjonen skal inneholde opplysninger om opplæringsprogrammene som foreligger for personell (herunder krav til kompetanse til instruktører) og hvordan disse oppdateres og gjennomgås **(4.2.2 (a)-(f))**
- Dokumentasjonen skal inneholde gjeldende ordninger for å komme tilbake i arbeid etter ulykker og uønskede hendelser eller langtidsfravær, herunder hvordan andre opplæringsbehov identifiseres **(4.2.3)**
- Dersom søker bruker et anerkjent kurscenter som er sertifisert i henhold til EU-forordninger, vil en kopi av det aktuelle sertifikatet gi en indikasjon på samsvar med punktene ovenfor, i den grad de er dekket av sertifiseringsprosessen **(4.2.1 (a), (c)-(f), (4.2.2))**
- Søker må oppgi hvordan det sikres at det ikke er noen forskjeller mellom kompetansen til eget personell og personell fra leverandører **(4.2.1 (a) - (f))**
- Søker må oppgi hvordan kompetansebehov for menneskelige og organisatoriske faktorer vurderes, herunder å definere i hvilke roller og i hvilke prosesser kompetanse for menneskelige og organisatoriske faktorer er nødvendig, og hvilket kompetansenivå som er nødvendig. Søker må også oppgi hvordan tilgjengelighet på kompetanse for menneskelige faktorer (for eksempel formelle kvalifikasjoner for menneskelige faktorer, dvs. akademisk grad, intern/ekstern anerkjent kompetanse og erfaring) er tilpasset virksomhetens modenhet og kompleksitet. **(4.2.1 (a-f))**

#### 4.2.5 Eksempler på dokumentasjon

System for styring av kompetanse med en forklaring på hvordan det fungerer over tid, inkludert for personell som ikke jobber i førstelinjen der det er hensiktsmessig, samt lenker til dokumentasjonen som understøtter dette, inkludert de ulike opplæringsprogrammene og hvordan tredjeparts kurssentre administreres.

Kontraktsfestede avtaler (inkludert kompetanseområde) med sertifiserte kurssentre, sammen med dokumentasjon på sertifiseringen deres.

Eksempler på opplæringsprogrammer for grupper av ansatte.

Kvalifikasjoner, inkludert psykiske eller fysiske krav som anses som nødvendig for spesifikke sikkerhetsrelaterte funksjoner.

Prosedyrer for granskning av uønskede hendelser og ulykker, for å vurdere om prosedyrene fokuserer på tiltak som kan føre til endringer i opplæringsprogrammer.

Erfaringer fra gjennomførte tilsyn for å vurdere om utfallet av disse kan føre til endringer i opplæringsprogrammer.

Prosedyren eller prosessen for å sikre at de ansatte har spesifikk og oppdatert opplæring ved:

- *Forventede endringer som påvirker interne regler, infrastruktur, virksomhetsstruktur osv.*
- *Oppdateringer av delegerede oppgaver (for eksempel for lokomotivførere, nye ruter, nye lokomotiver, ny type tjeneste).*

Proessen for å sikre at:

- *Kompetansen opprettholdes av tilstrekkelig praksis innen feltet (for eksempel for lokomotivførere, kjennskap til driftsforhold, kjennskap til ulike typer kjøretøy, strekninger og stasjoner) og/eller ved planlegging av spesifikk opplæring, særlig hvor det har vært langtidsfravær (for eksempel pga. sykdom) eller ulykke/uønsket hendelse*
- *Nødvendige tiltak er iverksatt der det er oppdaget avvik eller uakseptabel atferd, som for eksempel der en person er tatt ut av tjeneste for en periode eller der deler av utstyr er ute av drift for en periode. Nødvendig tiltak som for eksempel spesifikk trening er iverksatt der det er identifisert et gap mellom kompetansekrav og faktisk kompetanse*
- *Det blir iverksatt hensiktsmessig tiltak for ansatte etter ulykker og uønskede hendelser (for eksempel for lokomotivførere som kjører på stoppsignal, ulykke som involverer personer osv.). Tiltakene kan for eksempel være at virksomheten forsikrer seg om at en lokomotivfører er egnet til å bli satt inn i tjeneste igjen eller blir erstattet med lokomotivfører som er kompetent for oppgaven*
- *Man har tatt til seg lærdom etter alvorlige ulykker eller andre uønskede hendelser, og dette blir meddelt, særlig når det oppdages nye risikoer som må håndteres på operativt nivå*
- *Overvåkingsprosessen for system for styring av kompetanse, inkludert hvordan effekten måles*

Proessen for å sikre at egnet kompetanse for menneskelige og organisatoriske faktorer foreligger, og at det er en systematisk tilnærming for å sikre tilstrekkelige ressurser.

Kompetanse innen sikkerhetskultur er basert på en behovsanalyse. Behov vurderes, og strategier legges for å sikre riktig kompetanse og ressurser. Ledelsen viser at de har grunnleggende kunnskap om sikkerhetskulturen, og fremmer viktigheten av den.

#### 4.2.6 Referanser og standarder

- *ISO10015:1999 «Kvalitetsstyring - veiledning for opplæring»*

---

The NSA NO 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.

- *ISO10018: «Kvalitetsstyring - veiledning for mennesker og kompetanse»*

#### 4.2.7 Relevante tema for tilsyn

Hvordan utfallet fra en risikovurdering er knyttet til en gjennomgang av kompetansestyring i virksomheten.

Når man ser på system for styring av kompetanse, er det viktig å huske at det vil være kompetansekrav som strekker seg utover virksomhetens ansatte, og som også gjelder for leverandører.

System for styring av kompetanse bør sjekkes for å se hvor oppdatert det er, og om opplæringen som er gjort i henhold til det gjenspeiler virksomhetens behov.

Virksomheten bør ha på plass midler for å sikre at innleid personell har kompetanse til å utføre arbeidet. Dette gjelder spesielt der bemanningsbyråenes styring av kompetanse kanskje ikke er så grundig som man skulle ønske.

Kompetansen som kreves for ansatte og innleid personell som utfører de samme oppgavene, bør være på samme nivå.

Det foreligger et system som sikrer at oppgaver med betydning for sikkerheten, inkludert sikkerhetskritiske oppgaver, blir identifisert.

Det er et robust og hensiktsmessig system for styring av kompetanse. Systemet bør inneholde identifisering av kunnskap og ferdigheter som trengs, opplæring, vedlikehold og ressurser for kompetanse; prosesser for rekruttering, opplæring, vurdering, kompetanseovervåking og registerføring, og vise hvordan alt dette bidrar til å nå og opprettholde kompetansenivået.

Fokusering på menneskelige faktorer - hva gjøres for å vurdere fysisk og mental helse (for eksempel lokomotivførere og for andre ansatte som utfører sikkerhetskritiske oppgaver).

## 4.3 Bevissthet

### 4.3.1 Lovbestemt krav

4.3.1. Den øverste ledelsen skal sikre at den selv og personalet som har en rolle som påvirker sikkerheten, er bevisst på relevansen, betydningen og konsekvensene av virksomheten og hvordan de bidrar til at sikkerhetsstyringssystemet anvendes riktig og er effektivt, herunder at sikkerhetsmålene nås (se nr. 3.2 Sikkerhetsmål og planlegging).

### 4.3.2 Formål

Bevissthet betyr å gjøre ansatte oppmerksomme på sikkerhetspolitikken i virksomheten, farer og risikoer man må være oppmerksom på, resultatene fra granskninger av ulykker og uønskede hendelser og hvordan alle kan bidra til sikkerheten i virksomheten. Begrepet omfatter også å gjøre ansatte oppmerksom på konsekvensene av å ikke bidra til etterlevelse av sikkerhetsstyringssystemet, både fra deres og virksomhetens ståsted. Hensikten med dette kravet er å løse problemstillinger i sikkerhetskulturen i virksomheten. Det er opp til toppledelsen å sette dagsordenen og hva virksomheten arbeider mot, og fastsette hvordan man skal arbeide. Personell som jobber i virksomheten er underlagt ledelsen. Søker må vise hvordan slike temaer håndteres i sine prosesser og prosedyrer.

### 4.3.3 Dokumentasjon

- Søker må vise at de har synliggjort viktigheten av at de ansatte bidrar til nå virksomhetens mål, herunder hvordan de vurderer effekt, vedlikehold og forbedring av synliggjøringen **(4.3.1)** (se også **2.3**)
- Informasjon om funksjoner i system for styring av kompetanse **(4.3.1)**

### 4.3.4 Eksempler på dokumentasjon

En forpliktelse fra ledelsen synliggjort i sikkerhetspolitikken eller i annen dokumentasjon som fremmer sikkerhetskulturen i virksomheten. Sikkerhetskulturen i virksomheten skal bidra til å håndtere risiko gjennom virksomhetsstyring. Alle ansatte bidrar til sikkerhetskultur gjennom sine handlinger og ved å bidra til å oppnå fastsatte sikkerhetsmål. Eventuelle henvisninger til spesifikke prosedyrer som fremmer disse ideene i virksomheten.

Forpliktelsen inneholder en indikasjon på hvordan virksomheten fremmer sin tilnærming til sikkerhetskulturen overfor sine leverandører.

Kommunikasjon fra toppledelsen vedrørende mål, enten ved å oppmuntre alle til å bidra til å nå målene, eller ved å takke alle for å ha bidratt til å nå dem.

Informasjon som viser at mellomledelsen og operasjonell personell er involvert i sikkerhetsarbeidet (arbeidsgrupper, fora, dedikerte dager med søkelys på sikkerhet, opplæringsprogrammer for å utvikle bevissthet om roller i sikkerhetsstyringssystemet, etc.).

En beskrivelse av hvordan bevissthet kommuniseres i virksomhet, hvilke kommunikasjonskanaler som brukes.

#### 4.3.5 Relevante tema for tilsyn

I samtaler med ansatte om kravet til bevissthet, er det viktig å få fastslått hvilken forståelse de har av sine roller og ansvarsområder. Dette vil indikere om virksomheten er i stand til å forstå betydningen av en hensiktsmessig virksomhetskultur eller bevissthet ved å bidra til sikkerhet gjennom etterlevelse av sikkerhetsstyringssystemet.

Hvordan virksomheten har grunnlagt sin nåværende sikkerhetskultur og hvilke skritt som skal tas for å forbedre og utvikle den, er viktige spørsmål ved tilsyn.

Sjekk overvåking av leveranser vedrørende sikkerhetsmål og ansvar, helse, risikobevissthet, rapporteringskultur - man ser etter forsømmelser, feil, brudd og andre avvik.

## 4.4 Informasjon og kommunikasjon

### 4.4.1 Lovbestemt krav

4.4.1.	Virksomheten skal fastsette egnede kommunikasjonskanaler for å sikre at sikkerhetsrelatert informasjon utveksles mellom de ulike nivåene i virksomheten og med eksterne berørte parter, herunder entreprenører, partnere og leverandører.
4.4.2.	For å sikre at sikkerhetsrelatert informasjon når fram til dem som skal foreta vurderinger og treffe beslutninger, skal virksomheten håndtere identifisering, mottak, behandling, utarbeiding og formidling av sikkerhetsrelatert informasjon.
4.4.3.	Virksomheten skal sikre at sikkerhetsrelatert informasjon er <ul style="list-style-type: none"><li>(a) relevante, fullstendige og forståelige for de tiltenkte brukerne,</li><li>(b) gyldige,</li><li>(c) nøyaktige,</li><li>(d) konsekvente,</li><li>(e) styrt (se nr. 4.5.3 Styring over dokumentert informasjon),</li><li>(f) formidlet før de trer i kraft,</li><li>(g) mottatt og forstått.</li></ul>

### 4.4.2 Formål

Samsvar med kravene demonstreres i søknaden ved å vise at egnede ressurser er satt til å identifisere sikkerhetsrelatert informasjon på de ulike nivåene, og for å formidle sikkerhetsrelatert informasjon til rett tid og til de riktige personene.

Ressursene skal vise at de regelmessige oppdaterer virksomhetens risiko slik at sikkerhetsrelatert informasjon alltid er relevant og oppdatert, og at det er et system på plass for å identifisere både nye farer og muligheter (politisk, sosialt, miljømessig, teknologisk, økonomisk og lovmessig).

Informasjonen skal nå frem til riktig personell (spesielt sikkerhetskritisk personell) i virksomheten som skal respondere. Dette vil omfatte hvordan de leverer relevant sikkerhetsrelatert informasjon til andre interessenter de samhandler med.

### 4.4.3 Forklarende merknader

Virksomheten spesifiserer hvilken type sikkerhetsrelatert informasjon som skal formidles, hvordan den skal formidles (**se også 4.5**), overfor hvem og under hvilke forhold formidlingsprosessen initieres (**4.4.1**). Sikkerhetsrelatert informasjon kan utveksles mellom personell som utfører sikkerhetsrelaterte oppgaver i virksomheten, med (under)leverandører, samarbeidspartnere, mellom jernbanevirksomheter og infrastrukturforvaltere og, der det er relevant, mellom infrastrukturforvaltere.

Det skilles mellom ulike typer informasjon:

- *Dokumentasjon for sikkerhetsstyringssystemet (se også 4.5)*
- *Statisk informasjon som er nødvendig for infrastrukturforvalteren for å utforme driftsregler og karakteristikk av jernbaneinfrastrukturen (for eksempel sporvidde, toglangde, stigningsvinkler og akselbelastning)*
- *Informasjon som kreves for planlegging av jernbanedriften, for eksempel grafisk rute, togoppgaver, ruter/strekninger, midlertidige hastighetsbegrensninger, endringer i jernbaneinfrastrukturen,*

The NSA NO 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.

*pågående jernbanearbeid, begrensninger i sporvidde, tog som skal omdirigeres fra den planlagte ruten, deler av linjen som skal brukes som enkeltspor, driftsoperative kunngjøringer (inkludert eventuelle endringer i togruter og/eller pendlingstjenester);*

- *Informasjon om togtrafikkstyring (mellom jernbanevirksomheter og infrastrukturforvaltere og, der det er relevant, mellom infrastrukturforvaltere), herunder identifisering av kompetent personell i virksomhetene som kan kontaktes i tilfelle nedsatt drift eller nødsituasjoner (**se også 5.5**), i og utenfor hovedarbeidstiden.*

Grunnleggende krav til utveksling av opplysninger (**4.4.2**) mellom jernbanevirksomheten og infrastrukturforvalteren er nedfelt i TSI-OPE, i ECM-forordningen for utveksling mellom jernbanevirksomheten og ECM og i CSM SMS for utveksling mellom jernbanevirksomheten/ infrastrukturforvalteren og myndighetene (Byrået, NSA).

Det foreligger også andre ordninger for utveksling av sikkerhetsrelaterte opplysninger mellom andre relevante parter. Dette kan være informasjon relatert til feil og mangler, design avvik, funksjonsfeil av tekniske systemer inkludert strukturelle delsystemer, eller informasjon om vedlikeholdsarbeidet utført gjennom SAIT (Safety Alert Tool) – avtalen som Byrået har fremmet sammen med jernbanesektoren.

«Gyldig» i **4.4.3 (b)** betyr oppdatert.

«Konsekvent» i **4.4.3 (d)** betyr ikke motstridende hvis det kommer fra forskjellige kilder.

«Forstått» i **4.4.3 (g)** betyr at søkeren viser at nødvendige skritt har blitt tatt for å sikre at sikkerhetskritisk informasjon er innforstått av dem den er rettet mot. Dette kan gjøres ved å stille kontrollspørsmål, under orienteringsmøter eller gjennom protokoller av sikkerhetskritisk kommunikasjon. Det kan for eksempel sjekkes om kommunikasjon av viktige meldinger blir bekreftet flere ganger for å bekrefte at de har blitt forstått riktig, for eksempel mellom signalgiver og lokomotivfører.

#### 4.4.4 Dokumentasjon

- *Søker beskriver kommunikasjonskanaler som brukes i virksomheten og formålet med dem (**4.4.1**)*
- *Søker fremlegger dokumentasjon på for eksempel internt sikkerhetsvarslingssystem, eventuelle systemer som gir bemanningen relevant og rutinemessig informasjon, og eventuelle systemer som gir bemanningen relevant og ad hoc-informasjon (**4.4.2**)*
- *Søker beskriver hvordan de får bekreftet at formidlet informasjonen har nådd ut og blitt forstått av dem den er ment for (spesielt de med sikkerhetskritiske roller) (**4.4.3**)*

#### 4.4.5 Eksempler på dokumentasjon

En redegjørelse av hvordan det kommuniseres både oppover og nedover i virksomheten, og hvordan de ulike informasjonstyper og -nivåer fungerer, herunder koblinger til spesifikke prosedyrer for sikkerhetsvarsler og rutinekommunikasjon.

Redegjørelse som beskriver hva som gjøres for at ulike typer kommunikasjon når frem og blir forstått av dem den er ment for.

Prosesser eller prosedyrer som sikrer at alle som berøres av sikkerhetsrelaterte oppgaver, gis korrekt versjon av dokumentasjon – og til rett tid.

Prosess eller prosedyre for at sikkerhetsrelaterte dokumenter bekreftes mottatt.

Proessen eller prosedyren for å sikre at eksterne parter, som infrastrukturforvalter(e), (andre) jernbanevirksomheter, myndigheter, etc., får oppgitt en kontaktperson som kan kommunisere med dem. Kontaktpersonen skal ha tilgang til omfattende informasjon.

Kjennskap til blankettsamling (formularsamling) (se TSI-OPE), som inneholder et sett med blanketter (formularer) eller hjelpemidler for tydelig og rask utveksling av formell informasjon (papirbasert eller papirløst medium, for eksempel registreringsutstyr) som har innvirkning på driften, spesielt for togdrift i avvikssituasjon.

Sikkerhetsinformasjon som skal utveksles i virksomheten eller med andre interessenter. Typiske eksempler:

- *Jernbanevirksomhet gir informasjon til infrastrukturforvalter om forhold som kan ha negativ innflytelse på togdriften (feil på rullende materiell, for eksempel akselbokser, slik at infrastrukturforvalteren kan iverksette risikoreduserende tiltak som stopp av trafikk på tilstøtende spor).*
- *Infrastrukturforvalter gir informasjon om infrastrukturfeil og eventuelle midlertidige sikkerhetstiltak som hastighetsreduksjon, til alle jernbanevirksomheter som opererer i det aktuelle området.*

For roller som skal administrere samhandling: Dokumentasjon på hvem sikkerhetsinformasjon sendes til, avhengig av driftsområdet.

Proessen eller prosedyren for å formidle informasjon om endringer i strukturen av virksomheten.

Kopier av instruksene som er gitt til dem som utfører sikkerhetsrelaterte oppgaver og til dem som følger driftsregler som er relevante for nettet. Disse må være:

- *Fullstendige: Alle regler og krav som er relevante for sikkerhetsoppgaver som er relevante for driften av jernbanevirksomheten, identifiseres og innarbeides i aktuell dokumentasjon*
- *Nøyaktige: Hver av reglene og hvert av kravene er korrekt innarbeidet og uten feil (for eksempel hva som skal gjøres før et signal, sikkerhetsrelatert kommunikasjon)*
- *Konsekvente: Kravene som gjelder for en enkeltperson eller et enkelt arbeidslag fra ulike kilder, må være forenlige og konsekvente, og ikke motstridende*

#### 4.4.6 Relevante tema for tilsyn

Sjekk at det foreligger teknikker og prosesser for å holde risikostyringen oppdatert, og at det søkes regelmessig etter ny risiko.

Sjekk at det foreligger en prosess for å overvåke formell informasjon.

Ved tilsyn er det viktig å sjekke hvor oppdatert informasjonen er og om den når frem til **alle** relevante medarbeidere til rett tid. For eksempel til dem som er på nattskift eller dem som jobber langt fra virksomhetens hovedkvarter.

## 4.5 Dokumentert informasjon

### 4.5.1 Lovbestemt krav

#### 4.5.1. Dokumentasjon av sikkerhetsstyringssystemet

##### 4.5.1.1. Det skal foreligge en beskrivelse av sikkerhetsstyringssystemet som omfatter

- (a) angivelse og beskrivelse av prosessene og aktivitetene i forbindelse med jernbanedriftens sikkerhet, herunder sikkerhetsrelaterte oppgaver og tilhørende ansvarsområder (se nr. 2.3 Roller, ansvar og myndighet i virksomheten),
- (b) samspillet mellom disse prosessene,
- (c) framgangsmåter eller andre dokumenter som beskriver hvordan disse prosessene gjennomføres,
- (d) angivelse av entreprenører, partnere og leverandører sammen med en beskrivelse av arten og omfanget av tjenestene som ytes,
- (e) angivelse av avtalefestede ordninger og andre forretningsavtaler som er inngått mellom virksomheten og andre parter nevnt i bokstav d), og som er nødvendige for å ha styring over virksomhetens sikkerhetsrisiko og sikkerhetsrisiko i forbindelse med bruk av underleverandører,
- (f) henvisning til dokumentert informasjon som kreves i henhold til denne forordning.

##### 4.5.1.2. Virksomheten skal sikre at en årlig sikkerhetsrapport inngis til vedkommende nasjonale sikkerhetsmyndighet (eller myndigheter) i samsvar med artikkel 9 nr. 6 i direktiv (EU) 2016/798, herunder

- (a) en sammenfatning av beslutningene om vesentlighetsnivå for sikkerhetsrelaterte endringer, herunder en oversikt over vesentlige endringer, i samsvar med artikkel 18 nr. 1 i forordning (EU) nr. 402/2013,
- (b) virksomhetens sikkerhetsmål for kommende år og hvordan alvorlig sikkerhetsrisiko påvirker fastsettelsen av disse sikkerhetsmålene,
- (c) resultatene av interne undersøkelser av ulykker/hendelser (se nr. 7.1 Erfaringer fra ulykker og hendelser) og annen overvåkingsvirksomhet (se nr. 6.1 Overvåking, 6.2 Internrevisjon og 6.3 Ledelsens gjennomgåelse), i samsvar med artikkel 5 nr. 1 i forordning (EU) nr. 1078/2012( ),
- (d) informasjon om framdrift i behandlingen av gjenstående anbefalinger fra nasjonale undersøkelsesorganer (se nr. 7.1 Erfaringer fra ulykker og hendelser),
- (e) virksomhetens sikkerhetsindikatorer som er angitt for å vurdere virksomhetens sikkerhetsnivå (se nr. 6.1 Overvåking),
- (f) i relevante tilfeller, konklusjonene fra sikkerhetsrådgiverens årsrapport, som nevnt i RID( ), om virksomhetens aktiviteter knyttet til transport av farlig gods( ).

#### 4.5.2. Utarbeiding og ajourføring

##### 4.5.2.1. Virksomheten skal sikre at egnede formater og medier brukes når dokumentert informasjon som gjelder sikkerhetsstyringssystemet, utarbeides og ajourføres.

#### 4.5.3. Styring over dokumentert informasjon

##### 4.5.3.1. Virksomheten skal ha styring over dokumentert informasjon som gjelder sikkerhetsstyringssystemet, særlig når det gjelder lagring, distribusjon og endringsstyring, for å sikre at opplysningene er tilgjengelige, hensiktsmessige og sikret, når det er relevant.

#### 4.5.2 Formål

Søker må dokumentere at sikkerhetsstyringssystemet deres er tilpasset for arten og omfanget av tjenestene som drives, og at det er i stand til å håndtere risikoer. Dette krever:

- en forklaring av virksomhetens sikkerhetspolitikk, en beskrivelse av virksomhetens organisering og nødvendig ledelsesforankring av virksomhetens sikkerhetsstyringssystem.
- detaljerte prosesser som fastsatt i ovennevnte krav i paragrafene 4.5.1.1 (a) til (f) og 4.5.1.2 (a) til (g).

Søkeren skal vise hvordan dokumentasjonen for sikkerhetsstyringssystemet administreres, dvs. identifisering, opprettelse, vedlikehold, håndtering, lagring og oppbevaring av dokumentert informasjon (dvs. dokumenter og data), for å sikre at den er oppdatert og at riktige versjoner er tilgjengelig for relevant personell ved behov.

#### 4.5.3 Forklarende merknader

Eventuelle dokumenter der søker viser sikkerhetsstyringssystemets samsvar med gjeldende krav **(4.5.1.1 (f))** er en del av den dokumenterte informasjonen til sikkerhetsstyringssystemet.

Følgende figur viser en typisk dokumentasjonsstruktur:



Figure 3: Typisk dokumentasjonsstruktur

Jernbanevirksomhetene kan sende inn en rapport for hvert driftsområde til de nasjonale sikkerhetsmyndighetene i medlemsstatene der de driver virksomhet **(4.5.1.2)**. Normalt er omfanget av rapporten kun den delen av driften som foregår i den respektive medlemsstaten. Byrået anbefaler imidlertid at rapporten dekker hele driftsområdet, da dette vil lette utvekslingen av informasjon mellom nasjonale sikkerhetsmyndigheter som fører tilsyn med jernbanevirksomheten.

Årsrapport fra sikkerhetsrådgiver **(4.5.1.2 (f))** om transport av farlig gods, i henhold til direktiv 2008/68/EF med endringer og RID, årsrapport fra sikkerhetsrådgiver for farlig gods er også et innspill til den årlige

sikkerhetsrapporten. Sikkerhetsrådgiveren i virksomheten er pålagt bestemte funksjoner, herunder å rådgi virksomheten, med hensyn til helse, miljø og sikkerhet i forbindelse med transport av farlig gods og utarbeidelse av nødvendige rapporter.

Identifikasjon, format (for eksempel språk, programvareversjon og grafikk) og medium (for eksempel papirbasert, elektronisk) som brukes til dokumentert informasjon **(4.5.2.1)** bestemmes etter virksomhetens skjønn. Dette trenger ikke å være i form av en papirbasert håndbok.

Dokumentstyring **(4.5.3.1)** er prosessen (eller prosedyren) som spesifiserer internkontroller, særlig gjennomgang og godkjenning for tilstrekkelighet før utstedelse og bruk, som må vurderes og implementeres for informasjon som skal dokumenteres. Den tar sikte på å identifisere gjeldende revideringsstatus for dokumentasjonen, for å hindre at det anvendes ugyldige eller foreldede dokumenter. Dette vil sikre at:

- *relevante utgaver av aktuelle dokumenter er tilgjengelig på steder med aktivitet der det er avgjørende at sikkerhetsstyringssystemet fungerer hensiktsmessig*
- *ugyldige eller foreldede dokumenter straks blir tatt ut av bruk, eller på annen måte sikret mot utilsiktet bruk*
- *foreldede dokumenter som oppbevares for juridiske formål eller for kunnskapens del merkes deretter*

#### 4.5.4 Dokumentasjon

- *Søker skal komme med en beskrivelse av sikkerhetsstyringssystemet og hvordan det fungerer med henvisning til relevante prosedyrer når det er nødvendig **(4.5.1.1 (a) - (c))***
- *Søker skal beskrive foreliggende roller og ansvar for sikkerhetsrelaterte oppgaver, og hvordan risiko fra søkerens egne samt andres aktiviteter, håndteres **(4.5.1.1 (a))***
- *Søker skal fremlegge dokumentasjon på at de har (eller har ordninger på plass for å utarbeide) årlige sikkerhetsrapporter som dekker punktene som er oppført i 4.5.1.2 ovenfor **(4.5.1.2 (a)-(f))***
- *Søker skal beskrive hvordan dokumentstyringssystemet fungerer, blant annet hvordan informasjonen gjøres tilgjengelig og egnet ved behov, hvordan informasjonen endres på en styrt måte i systemet og hvordan den lagres og vedlikeholdes på en slik måte at den er lett å hente frem igjen. Informasjonen i dokumentstyringssystemet bør i tillegg oppbevares på et beskyttet sted for å redusere sannsynligheten for forringelse eller skade, og for å hindre tap **(4.5.2.1), (4.5.3.1)***

#### 4.5.5 Eksempler på dokumentasjon

En beskrivelse av sikkerhetsstyringssystemet, dets struktur og koblingen til andre dokumenter som omhandler prosessene (for eksempel håndbøker, organisatoriske og operative prosedyrer, arbeidsinstrukser). ISO har et konsept med dokumentert informasjon, men virksomheten kan fortsette sin dokumentasjonsstruktur dersom den er egnet for formålet.

En oversikt over hvordan de ulike dokumentene er strukturert, publisert, tilgjengeliggjort, arkivert, vedlikeholdt, revidert og opphevet med henvisning til relevante dokumentstyringsprosedyrer.

Prosedyren for å utarbeide årsrapporten dersom søknaden gjelder det første felles sikkerhetssertifikatet. Prosedyren beskriver den foreslåtte utformingen av rapporten.

Dokumenthåndteringsprosessen eller -prosedyren som beskriver oppdatering av dokumenter etter regelmessige gjennomganger, samt etter ulykker eller uønskede hendelser. Prosessen eller prosedyren for tilfeller der avtalte oppdateringer ikke har funnet sted innenfor den fastsatte tidsrammen, eller hvor det ikke blir enighet om hvordan dokumentet skal oppdateres.

---

The NSA NO 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.

Et konsist språk (dvs. bruk av korte, klare setninger og å unngå sjargong) anvendes for god forståelse og datakvalitet.

Personellet som har myndighet til å godkjenne dokumenter for utstedelse, sjekker at innholdet er nøyaktig og at det kan forstås av alle sluttbrukere.

Der det måtte være av praktisk betydning, kan endringene fremheves i dokumentet eller eventuelle vedlegg for å lette gjennomgangen og godkjenningen.

Oppbevaringstider for dokumenter og registre er fastsatt, dokumentert og overholdt.

#### 4.5.6 Referanser og standarder

- *Veiledning til kravene til dokumentert informasjon i ISO 9001:2015, ISO/TC 176/SC2/N1286, på:*  
[www.iso.org/tc176/sc02/public](http://www.iso.org/tc176/sc02/public)

#### 4.5.7 Relevante tema for tilsyn

Sjekk at kontraktsforholdene åpner for en hensiktsmessig overvåking og risikostyring i virksomheten (dvs. ved outsourcing av tjenester).

Sjekk forholdet mellom dem som administrerer dokumentstyringssystemet og dem som har ansvaret for å oppdatere informasjonen, og om deres kommunikasjon med hverandre fungerer i praksis. Det er ofte på dette nivået at det kan forekomme uregelmessigheter i dokumentstyringen. Viktigheten av å oppdatere dokumentasjonen oppfattes ulikt, noe som igjen kan føre til at oppdateringen av dokumentasjonen går tregt, med de risikoer det måtte innebære.

Sjekk de ansattes tilgang til oppdatert informasjon eller dokumentasjon.

Strukturen og driftsforholdene i sikkerhetsstyringssystemet bør gjenspeile arbeidet slik det utføres i virkeligheten.

## 4.6 Integrasjon av menneskelige og organisatoriske faktorer

### 4.6.1 Lovbestemt krav

- 4.6.1. Virksomheten skal vise at menneskelige og organisatoriske faktorer integreres i sikkerhetsstyringssystemet etter en systematisk metode. Denne metoden skal
- (a) omfatte utarbeiding av en strategi og bruk av fagkunnskap og anerkjente metoder fra området menneskelige og organisatoriske faktorer,
  - (b) håndtere risiko knyttet til utforming og bruk av utstyr, oppgaver, arbeidsvilkår og organisatoriske ordninger, idet det tas hensyn til menneskelige evner og begrensninger samt påvirkningen på menneskets yteevne.

### 4.6.2 Formål

Søker viser en systematisk tilnærming til menneskelige faktorer. Menneskelige faktorer er en integrert del av sikkerhetsstyringssystemet. Det er viktig å imøtekomme disse elementene for å vise at søkeren er kompetent til å drive en jernbanevirksomhet. Jernbanevirksomhetene viser at de har systemer for å håndtere risiko knyttet til menneskelige faktorer integrert i sitt sikkerhetsstyringssystem for å kunne håndtere risiko de står overfor.

### 4.6.3 Forklarende merknader

Menneskelige og organisatoriske faktorer handler om en brukersentrert tilnærming hvor menneskelige ferdigheter og begrensninger og samspillet med andre systemer under utførelse av oppgaver, tas i betraktning. Menneskelige og organisatoriske faktorer innebærer i tillegg å få et systematisk perspektiv, der samspillet mellom menneskelige, teknologiske og organisatoriske faktorer tas i betraktning. Virksomheten må identifisere behovet for å vurdere sikkerhetsstyring av menneskelige og organisatoriske faktorer med en tilnærming ut fra systemets virketid. Dette betyr at de må identifisere og håndtere menneskelige og organisatoriske faktorer i sikkerhetsstyringsaktiviteter som er relatert til forretningsmessige mål, ledelse, drift, menneskelig yteevne, utforming av arbeidsoppgaver og arbeidsplass på alle stadier av systemets virketid, for eksempel fra oppstart til avvikling. Strategien for menneskelige og organisatoriske faktorer spesifiserer en systematisk tilnærming til å håndtere menneskelige og organisatoriske faktorer i sikkerhetsstyringsaktiviteter, knyttet til risikostyring i virksomhetssammenheng.

Virksomheten bør engasjere den menneskelige og organisatoriske kompetansen som er nødvendig. Med eksperter innenfor menneskelige og organisatoriske faktorer menes at involvert personell bør være kvalifisert til å definere noen områder i nasjonale og/eller internasjonale standarder. For eksempel kan en ekspert oppfylle kravene fastsatt av Centre for Registration of European ergonomists eller andre tilsvarende internasjonale foreninger. Store virksomheter kan ha en avdeling med ekspertise på menneskelige faktorer som støtter virksomheten. I en mindre virksomhet kan ledere på alle nivåer ha ansvaret for å identifisere behovet for ekspertise på menneskelige faktorer.

Mer informasjon om en strategi for menneskelige og organisatoriske faktorer kan ses i vedlegg 5.

### 4.6.4 Dokumentasjon

- Søker skal vise gjennom en strategi hvordan menneskelige og organisatoriske faktorer er integrert i relevante prosesser i sikkerhetsstyringssystemet slik at risiko knyttet til mennesker, organisasjon og teknologi er ivaretatt. Dette kan for eksempel være en plan for hvordan menneskelige og

*organisatoriske faktorer håndteres når man anskaffer et nytt signalsystem. Søkeren skal da vise hvor relevante prosedyrer er i sikkerhetsstyringssystemet. (4.6.1)*

- *En brukervennlig designprosess basert på menneskelige og organisatoriske prinsipper og metoder, samt involvering av brukere, som for eksempel ved ny eller modifisert design, prosedyrer, trening og arbeidsmiljø. Dette er for å ivareta sikkerhet over lengre tid.*
- *Tilgjengelige menneskelige og organisatoriske designstandarder og best praksis er brukt. Relevante standarder er for eksempel ISO serien 11064 Ergonomisk design av kontrollsenter og ISO serien 9241 Ergonomi av interaksjon mellom menneske og system.*
- *Sluttbruker er involvert i designprosess, som for eksempel krav til definisjon, videre utvikling og prosess for testing.*
- *En brukervennlig designprosess er en iterativ prosess som har flere faser. Analyser er foretatt for å forstå og spesifisere bruk av konteksten (som for eksempel personell og kompetanseanalyse, oppgaveanalyse og risikoanalyse). Disse analysene danner grunnlag til brukerkrav. Designløsninger inkluderer design av grensesnitt, arbeidsplasser, trening, prosedyrer og virksomhet, og er fremkommet for å møte brukerkravene. Evalueringer av design er fremkommet gjennom formelle metoder, slik som oppgaveanalyse, risikovurdering, ekspertevaluering, brukerevaluering, verifikasjon og gyldighet.*

#### 4.6.5 Eksempler på dokumentasjon

En kopi av strategien for menneskelige og organisatoriske faktorer, som beskriver hvordan bruk av ekspertise og teknikker innen menneskelige og organisatoriske faktorer er beskrevet.

Virksomheten utfører en analyse ved hjelp av dokumentasjonbaserte metoder for drifts- og støtteprosesser for alle stadier i virketiden, fra design til avhending. Analysen skal identifisere alle menneskelige og organisatoriske faktorer og ytelsespåvirkende faktorer, som vil ha innvirkning på jernbanesikkerheten og sikkerhetsstyringsaktiviteter som er nødvendig for å håndtere risiko.

Strategien for menneskelige og organisatoriske faktorer skal vise at det foreligger sikkerhetsstyringsaktiviteter, samt en tilnærming til kontinuerlig overvåking og forbedring av hensikten med strategien. Strategien bør være basert på en proaktiv tilnærming, men bør inkludere reaktive aktiviteter etter behov.

For driftsprosesser må sikkerhetsstyringsaktiviteter som er relatert til støttefunksjoner og -systemer, utforming av arbeidsoppgaver, bemanningsnivåer, opplæring, design og bruk av utstyr, prosedyrer og blanketter (formularer), beskrives.

For eksempel bør strategien inneholde hvordan menneskelige og organisatoriske faktorer er integrert i prosessen til styring av endringer. Med integrering av menneskelige faktorer menes at det er på plass virksomme prosesser som integrerer menneskelige faktorer og ergonomi i virksomhetens daglige drift. Planen for integrering av menneskelige faktorer har en systematisk tilnærming, og definerer forholdet mellom alle relevante prosjekter og områder i virksomheten. Integrering av menneskelige faktorer i systemdefinisjon, design, utvikling og evaluering skal ivaretas for å optimalisere samhandlingen mellom menneske og maskin.

Hvis operasjonelle prosesser involverer komplekse arbeidsmønstre, bør risiko for tretthet være omhandlet i strategien for menneskelige og organisatoriske faktorer.

#### 4.6.6 Referanser og 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-standardserien, for eksempel
- ISO Series 6385:2004 *Ergonomic principles in the design of work systems*
- ISO Series 11064 *Ergonomic design of control centres*
- ISO Series 9241 *Ergonomics of human-system interaction*
- ISO Series 10075 *Ergonomic principles related to mental work-load*
- 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 Relevante tema for tilsyn

Sjekk at menneskelige faktorer vurderes i beslutningsprosesser for risikostyring gjennom risikovurdering, endringsstyring og forvaltning av eiendeler.

Sjekk at driftsdokumentasjonen gjenspeiler engasjementet til å håndtere menneskelige faktorer gjennom ergonomisk design (for eksempel: brukervennlig design, lettforståelig språk, grafikk for å forstå instruksjonene, enkel administrasjon av oppdateringer) for å bidra til god risikostyring.

Sjekk at jernbanevirksomheten i overvåking av ytelsen, retter søkelyset i analysen mot menneskelige faktorer som primær eller underliggende årsak til ulykker, hendelser eller farlige situasjoner.

Sjekk om det finnes dokumenterte eksempler på korrigerende tiltak som er utarbeidet for å eliminere faktorer som påvirker den menneskelige yteevnen og svekker sikkerheten.

## 5 Drift

### 5.1 Planlegging og styring av driften

#### 5.1.1 Lovbestemt krav

- 5.1.1. Når virksomheten planlegger, utvikler, gjennomfører og gjennomgår sine driftsprosesser, skal den sørge for at det under drift
- (a) anvendes kriterier for risikoakseptering og sikkerhetstiltak (se nr. 3.1.1 Risikovurdering),
  - (b) framlegges en eller flere planer for å nå sikkerhetsmålene (se nr. 3.2 Sikkerhetsmål og planlegging),
  - (c) samles inn informasjon for å måle at driftsrutiner anvendes på riktig måte og er effektive (se nr. 6.1 Overvåking).
- 5.1.2. Virksomheten skal sørge for at driftsrutinene oppfyller sikkerhetskravene i gjeldende tekniske spesifikasjoner for samtrafikkevne og relevante nasjonale regler samt andre relevante krav (se nr. 1 Virksomhetens kontekst).
- 5.1.3. For å ha styring over risikoen når det er relevant for sikkerheten i forbindelse med driften (se nr. 3.1.1 Risikovurdering) skal det tas hensyn til minst følgende:
- (a) Planlegging av eksisterende eller nye togruter og ny togtrafikk, herunder innføring av nye typer kjøretøy, behovet for å leie kjøretøy og/eller ansette personale fra eksterne parter og utveksle informasjon om vedlikehold for driftsformål med enhet med ansvar for vedlikehold.
  - (b) Utarbeiding og gjennomføring av ruteplaner.
  - (c) Klargjøring av tog eller kjøretøy før forflytning, herunder kontroll før avgang og togsammensetning.
  - (d) Togtrafikk eller kjøretøybevegelser under de forskjellige driftsforholdene (under normale forhold, ved driftsforstyrrelser og i nødsituasjoner).
  - (e) Tilpasning av driften når enhet med ansvar for vedlikehold ber om at kjøretøy tas ut av drift og melder om at kjøretøy kan gjeninnsettes i bruk.
  - (f) Godkjenninger av kjøretøybevegelser.
  - (g) Anvendelighet av grensesnitt i togenes førerrom, i togledersentraler og utstyr som brukes av vedlikeholdspersonalet.
- 5.1.4. For å styre fordelingen av ansvarsområder når det er relevant for sikkerheten i forbindelse med driften, skal virksomheten fastslå ansvaret for å samordne og håndtere sikker togtrafikk og kjøretøybevegelser samt definere hvordan oppgaver som har betydning for at alle tjenester ytes på en sikker måte, fordeles på kvalifisert personale i virksomheten (se nr. 2.3 Roller, ansvar og myndighet i virksomheten) og eventuelt på andre eksterne kvalifiserte parter (se nr. 5.3 Entreprenører, partnere og leverandører).
- 5.1.5. For å ha styring over informasjon og kommunikasjon når det er relevant for sikkerheten i forbindelse med driften (se nr. 4.4 Informasjon og kommunikasjon), skal det berørte personalet (f.eks. togpersonalet) få nærmere informasjon om særskilte vilkår for reisen, herunder relevante endringer som kan medføre fare, midlertidige eller varige driftsbegrensninger (f.eks. på grunn av bestemte typer kjøretøy eller bestemte ruter) og vilkår for spesialtransport, når det er relevant.
- 5.1.6. For å styre kompetansen når det er relevant for sikkerheten i forbindelse med driften (se nr. 4.2 Kompetanse), skal virksomheten i samsvar med gjeldende regelverk (se nr. 1 Virksomhetens kontekst) sikre at

- (a) personalets opplæring og arbeidsinstrukser følges, og at korrigerende tiltak treffes dersom det er påkrevd,
- (b) personalet får særskilt opplæring ved forventede endringer som påvirker driften av virksomheten eller personalets arbeidsoppgaver,
- (c) det vedtas egnede tiltak for personalet etter ulykker og hendelser.

### 5.1.2 Formål

Søker skal vise at det foreligger relevante prosesser for å håndtere operasjonelle risikoer gjennom sikkerhetsstyringssystemet, herunder å sørge for at de ansatte er innforstått med sine roller, operasjonelle risikoer de står overfor, og hvilke styringstiltak som foreligger, og at de har riktig kompetanse og opplæring i å håndtere disse i samsvar med sikkerhetsstyringssystemets dokumentasjon.

Søker skal sørge for at vognene eller infrastrukturen drives trygt i samsvar med gjeldende krav under ulike driftsforhold (dvs. normal drift, redusert drift og nødsituasjoner). Kravet vil også gjelde for testkjøring (for eksempel testing av hvordan vognene oppfører seg når de er i bevegelse, før det gis godkjenning) og ved spesialforsendelser (for eksempel transport av kjernefysisk materiale eller store deler som ikke kan deles opp og som ikke kan transporteres ved hjelp av andre transportmidler, som betongbjelker/bærebjelker for broer, etc.).

### 5.1.3 Forklarende merknader

Sikkerhetsdirektivet fastsetter at jernbanevirksomheter skal etablere et sikkerhetsstyringssystem for å håndtere sikkerhetsrisiko i forbindelse med jernbanevirksomheten. Den generelle oppfatningen innen sikkerhetsstyring er at sikkerheten skal integreres i normale forretningsprosesser så langt det lar seg gjøre. Årsaken til dette er at forretningsfokuseringen da er like mye rettet mot sikkerheten som andre forretningsprosesser, noe som vil føre til mindre konflikter mellom de ulike prosessene.

ISO fastsetter i veiledningsdokumentet (N360), som støttevedlegg til vedlegg SL, at hensikten med paragraf 8 (Drift) er å spesifisere de elementene som må implementeres i virksomheten for å sikre at styringssystemkravene oppfylles, samt for å sikre at prioritert risiko blir tatt i betraktning. I tillegg er det oppgitt at tilleggskrav (spesifikke for kategori) knyttet til driftsplanlegging og styring kan komme til å gjelde. De skal ikke være ødeleggende for virksomheten, men sørge for et tilstrekkelig rammeverk for å styre hvordan viktige sikkerhetsaspekter skal håndteres i virksomhetens forretningsprosesser.

Det har blitt lagt til uttrykkelige koblinger mellom driftskrav og andre styringssystemkrav (tilsvarende tilnærmingen som er vedtatt i vedlegg III til ECM-forordningen) for å gjøre det klart at spesifikke driftskrav skal vurderes med tanke på relevante styringssystemkrav (for eksempel er planlegging av ruter for jernbanevirksomheter en aktivitet som bør være gjenstand for risikovurdering). Denne tilnærmingen er ikke ment å være inngående, men har som formål å identifisere bestemte spørsmål som myndighetene mener er viktige (basert på deres erfaring), og som derfor bør undersøkes når de foretar vurdering eller tilsyn. Jernbanevirksomheter bør ikke bare fokusere på disse spesifikke kravene når de utvikler og implementerer sine sikkerhetsstyringssystemer (for eksempel uten hensyn til annen sikkerhetsrisiko). Jernbanevirksomheter må alltid anvende sikkerhetsstyringssystemkrav (for eksempel risikovurdering, overvåking, kompetanse, informasjon og kommunikasjon) for alle relevante forretningsprosesser for å vise at sikkerhetsrisikoene er tilstrekkelig styrt.

Integreringen av sikkerhetsstyringssystemet i forretnings-/driftsprosessene er av stor betydning, og for å oppnå dette må virksomheten overholde gjeldende TSI (5.1.2), som TSI-OPE, og regler fra nasjonale bestemmelser når samhandlingskravene ikke er fullt ut spesifisert i tekniske spesifikasjoner for

interoperabilitet (TSI). Godkjente metoder for etterlevelse kan også bli kunngjort av medlemsstaten eller dens myndigheter, for å lette etterlevelsen av nasjonale bestemmelser. Som et minimum bør følgende driftsprosesser vurderes der det er relevant:

- *Drift av infrastrukturen (styring av strekninger, tillatelse gitt til at kjøretøy er i bevegelse under alle forhold og sikring av vedlikehold av infrastruktur)*
- *Drift av kjøretøy (for relevante strekninger, uttak av tog, sikre togdrift under alle forhold, også testkjøring, samt vedlikehold og reparasjon av vogner)*
- *Skifting (flytting av vogner for å montere eller demontere et tog).*

TSI-OPE er viktig, fordi det beskriver grunnleggende driftsprinsipper (FOP), som bør gjenspeiles i de relevante delene av sikkerhetsstyringssystemet, og slik kan samsvar med TSI-OPE brukes til å vise samsvar med de relevante sikkerhetsstyringssystemkravene som nevnt ovenfor.

Utvexling av informasjon for driftsformål ved vedlikehold av kjøretøy **(5.1.3 (a))** under ECM-forordningen og dem som anvender den, er beskrevet i artikkel 5(3) i ECM-forordningen. Dette omfatter vedlikeholdsplan og begrensninger fastsatt i ECM-forordningen under vedlikehold (kortsiktig planlegging).

Når det henvises til utvikling og gjennomføring av ruteplaner **5.1.3 (b))**, betyr dette at søker skal vise hvordan man ved risikovurdering har håndtert risiko for aktivitetene i virksomheten og ved samhandling med andre aktører. For eksempel at de har tatt hensyn til

- *den ekstra arbeidsbelastningen for togleder/togekspeditører når det kommer flere tog til bestemte tider;*
- *egnede driftsavtaler med relevant infrastrukturforvalter for å stoppe trafikken, gjenoppta trafikken, utveksle informasjon og eventuelle andre tjenester som anses nødvendig*
- *administrere risiko knyttet til sporvedlikehold når togene er i drift 24 timer i døgnet.*

Ny togtjeneste **(5.1.3 (b))** kan omfatte ny type gods som skal transporteres.

Kjøretøy i bevegelse **(5.1.3 (d))** har en bredere betydning enn tog i bevegelse (dvs. planlagt bevegelse av kjøretøy) og tillatelse utstedt før togavgang. Det kan også omfatte slep av et havarert tog, kjøring av sporvedlikeholdsmaskiner eller uplanlagt utskifting av en skadet kjøretøy før togavgang.

I henhold til UIC-hefte 502-1, artikkel 1.1, foreslås følgende definisjon av begrepet «spesialforsendelser» **(5.1.5)**: «En forsendelse anses å være en spesialforsendelse dersom dens ytre dimensjoner, vekten eller dens egenskaper i forhold til det faste utstyret eller vognen til en jernbanevirksomhet som er involvert i transporten fører til særegne vanskeligheter, og således kun kan aksepteres under spesielle tekniske eller driftsmessige forhold».

Infrastrukturforvalteren skal identifisere og utstede vilkår og tiltak for å bruke en vogn for testing på jernbanenettet innen den fastsatte tidsrammen som er angitt i artikkel 21(3) og 21(5) i direktiv (EU) 2016/797 **(5.1.2)**.

Menneskelige og organisatoriske faktorer bør vurderes under driftsplanlegging i forbindelse med for eksempel arbeidsplaner, tretthet, stress, arbeidsmiljø (fysisk og psykososialt), arbeidsplasser og arbeidsprosesser, osv.

Driftsplanlegging og styring er utviklet for kontinuerlig forbedring av sikkerhetskulturen. Sikkerhetskulturen bør tas i betraktning i forbindelse med for eksempel arbeidsbelastning, arbeidsmiljø (fysisk og psykososialt), arbeidsprosesser osv. Dette er for å sikre at konsekvensene av endringene eller ordningene ikke har en negativ innvirkning på menneskelig yteevne eller den organisatoriske sikkerheten.

#### 5.1.4 Dokumentasjon

- Informasjon som viser at ved planlegging, utvikling, gjennomføring og gjennomgang av driftsprosesser planlegger man å nå sikkerhetsmål, og at man anvender risikovurderingstiltak og overvåker resultatene, herunder at det benyttes egnet merking der ytterligere informasjon om prosedyrer kan bli funnet **(5.1.1 (a)-(c))**
- Dokumentasjon på at virksomheten er klar over og faktisk gjennomfører alle obligatoriske sikkerhetskrav i alle kategorier som gjelder for driften, og en skissering av hvordan sikkerhetsstyringssystemet sikrer at de overholdes.
- Informasjon der søkeren forsikrer om at driftsordningene samsvarer med gjeldende krav (lovgivning, standarder, osv.) **(5.1.2)**
- I rammeverket for godkjenning av vogntyper og/eller godkjenning for idriftssetting av vogner, er infrastrukturforvalteren i stand til å identifisere og dokumentere **(5.1.2)**
  - driftsforhold for tester på jernbanenettet, basert på informasjon som er oppgitt av søkeren for godkjenningen;
  - eventuelle nødvendige tiltak på infrastrukturens side for å sikre en trygg og pålitelig drift under testing, og/eller
  - eventuelle nødvendige tiltak i infrastrukturinstallasjonene for å utføre testing på jernbanenettet.
- Dokumentasjon på at driftsdokumentasjonen er i samsvar med kravene til styring av driften (og vedlikeholdet), samt ved organisatoriske og fysiske grenser, for eksempel organisatorisk, teknisk og driftsmessig samhandling med nærliggende infrastruktur, grensende stasjoner, samhandling med andre jernbanevirksomheter eller infrastrukturforvaltere, etc. **(5.1.2)**
- Informasjon om hvordan risikoen for driftsaktiviteter håndteres gjennom risikovurderingsprosessen og dekker punktene som er angitt i kravene ovenfor **(5.1.3 (a), (c) - (f))**
- Dokumentasjon på at artikkel 14(2) i direktiv 2016/798/EF overholdes av det ansvarlige organet for vedlikehold **(5.1.3 (e))**
- Informasjon om hvordan ansvaret for sikkerheten, inkludert ansvaret for tretthetsrisikostyring, håndteres for driftsaktiviteter **(5.1.4)**
- Informasjon om hvordan virksomheten håndterer informasjon og kommunikasjon for sikkerheten ved driftsaktiviteter **(5.1.5)**
- Informasjon om kompetansestyringssystemet og tilhørende prosedyrer, samt hvordan disse kobles til bestemte arbeids- eller oppgaveinstruksjoner for å opprettholde sikkerheten ved driftsaktivitetene **(5.1.6)**
- Dokumentasjon på at driftsdokumentasjonen (prosedyrer, arbeidsinstrukser, etc.) oppdateres når og der det er nødvendig **(se også 4.5.3)**.

#### 5.1.5 Eksempler på dokumentasjon

En liste over de obligatoriske kravene (inkludert TSI) og hvordan disse overholdes **(se også kapittel 2)**.

En forklaring på hvordan driftsrisiko håndteres gjennom risikovurderingsprosessen og hvordan det sikres at sikkerhetsmålene ved driften nås. Lenker til der man kan finne relevante prosedyrer.

En redegjørelse for hvordan felles sikkerhetsmetoder bidrar til styring av driftsrisiko, og hvordan informasjons- og kommunikasjonsflyten håndteres for å sikre korrekt risikostyring.

Detaljert informasjon om vedlikeholdssystemet for rullende materiell, herunder lenker til detaljert dokumentasjon som underbygger dette (der det ikke finnes noen ECM eller sertifiseringsordning).

Detaljert informasjon om kontroll før togavgang (TSI-OPE) som foreligger for å sikre ensartet kontroll av:

- *bremseegenskaper (klargjøring av bremseplaten);*
- *togsammensetning;*
- *fremre og bakre signaler;*
- *tilstand på last og vogner.*

En kopi av prosessen for å identifisere uoverensstemmelser og hvordan det sikres at det treffes nødvendige tiltak, som for eksempel å ta kjøretøy ut av drift, utskifting av ødelagt/defekt komponent/utstyr/kjøretøy eller iverksetting av driftsbegrensninger.

Et dokument som beskriver vogntypene som skal brukes på hver enkelt rute og hvilken drift som skal utføres, og som spesifikt beskriver:

- *driftsbegrensninger som gjelder for bestemte kjøretøy;*
- *begrensninger som gjelder for bruk av bestemte kjøretøy på bestemte strekninger;*
- *ekstra vedlikeholdskrav for bestemte strekninger (se også kapittel 5.2) .*

Et dokument som beskriver eventuelle tilleggskrav for å håndtere avvikssituasjoner (for eksempel hendelser med vogn) for jernbanenettet som er berørt av driften.

Det foreligger en prosess for styring av risiko knyttet til tretthet som gjelder for ansatte med uregelmessige arbeidstider. Prosessen er basert på dokumentasjon av metoder og faglig kompetanse. Prosessen tar hensyn til at en rekke faktorer må vurderes, samt en helhetlig tilnærming til styring av risiko knyttet til tretthet. Prosessen bør omfatte planlegging og tilsyn av arbeidsmiljøet og arbeidsoppgavene, for å redusere effekten tretthet har på årvåkenhet og yteevne så langt som praktisk og mulig og innen rimelighetens grenser, på en måte som samsvarer med risikoeksponeringsnivået og driftens art.

For etterlevelse av fundamentale operative driftsprinsipper (FOP) i TSI-OPE, fremlegges dokumentasjon på at jernbanevirksomheten kan forsikre om at for eksempel:

- *et tog skal kun gå på en del av linjen dersom togsammensetningen er kompatibel med infrastrukturen (FOP 3)*

*Dette gjelder bekreftelse av togkompatibilitet med infrastrukturen på ruten der det er planlagt å kjøre, før togdriften er godkjent. Kompatibilitet mellom tog og infrastruktur påvirkes først og fremst av dimensjonene på en vogn og hvilken last den transporterer; klaringene mellom toget og infrastrukturen eller togene på tilstøtende spor (måling); minimum påkrevd bremsekapasitet på toget; vekten og lengden på et tog og kapasiteten på infrastrukturen.*

Det foreligger dokumentasjon på at:

- *kontroll før togavgang vil finne sted for å sikre at passasjerer, bemanning og gods føres trygt frem, før et tog starter på eller fortsetter med reisen (FOP 4).*

*Dette gjelder toget og om det er klart for å settes i gang. Noen eksempler: Togets bremsekapasitet, hastigheten som toget har lov til å kjøre i, formasjonen og koplingen av toget, identifikasjon, lasting og sikring av gods, anskaffe tilstrekkelig informasjon til klargjøring av tog og driftspersonell. Formålet er å forhindre kollisjoner og avsporinger som følge av eksisterende risiko.*

#### 5.1.6 Referanser og standarder

- *ISO N360 JTCG konseptdokument som bilag til Vedlegg SL*
- *UIC-hefte 502-1*

---

The NSA NO 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.

- [RID](#)
- *Veileder for TSI-OPE*

#### 5.1.7 Relevante tema for tilsyn

Tilsynet med driftsaktiviteter skal gjennomføres ved å fokusere på særskilte områder og undersøke disse i detalj, for å se hvordan de er gjenspeilet i sikkerhetsstyringssystemet for virksomheten som føres tilsyn med, og om de har egnet bemanning på rett sted som utfører arbeidet korrekt. Dette vil gjøre det mulig for NSA å se om aktivitetene er omfattet av sikkerhetsstyringssystemet som en sammenhengende helhet, eller håndteres separat med svake koblinger til sikkerhetsmålene og den grunnleggende strategien.

Tilsynet bør spesifikt omfatte:

- *hvordan dokumentene i HLS-sikkerhetsstyringssystem overføres til lokale instruksjoner som blir brukt til å håndtere risiko i drift*
- *håndtering av nødsituasjoner eller andre situasjoner som ikke er en del av rutinen*
- *hvordan driftsgrenser/-begrensninger styres, herunder samhandlingsordninger med andre parter*
- *ordninger for håndtering av risiko grunnet tretthet*
- *håndtering av farlige stoffer*
- *ordninger for transport av farlig gods, herunder opplæring, roller og ansvar for virksomhetens ansatte, som beskrevet i kapittel 1.3 og 1.4 i RID*
- *etterlevelse av de grunnleggende driftsprinsippene (FOP) som er beskrevet i TSI-OPE*

## 5.2 Forvaltning av eiendeler

### 5.2.1 Lovbestemt krav

5.2.1.	Virksomheten skal håndtere sikkerhetsrisiko knyttet til fysiske eiendeler gjennom hele livssyklusen (se nr. 3.1.1 Risikovurdering) fra konstruksjon til sluttbehandling og oppfylle kravene som gjelder menneskelige faktorer, i alle faser av livssyklusen.
5.2.2.	Virksomheten skal <ul style="list-style-type: none"><li>(a) sikre at eiendelene brukes til det tilsiktede formålet og samtidig opprettholde sikker drift i samsvar med artikkel 14 nr. 2 i direktiv (EU) 2016/798 når det er relevant, og det forventede ytelsesnivået,</li><li>(b) forvalte eiendelene ved normal drift og driftsforstyrrelser,</li><li>(c) så snart som praktisk mulig påvise tilfeller av manglende overholdelse av driftskravene før eller under driften av eiendelen, herunder ved behov anvende bruksrestriksjoner for å garantere sikker drift av eiendelen (se nr. 6.1 Overvåking).</li></ul>
5.2.3.	Virksomheten skal sørge for at ordningene for forvaltning av eiendeler i relevante tilfeller oppfyller alle grunnleggende krav som angitt i gjeldende tekniske spesifikasjoner for samtrafikkevne og andre relevante krav (se nr. 1 Virksomhetens kontekst).
5.2.4.	For å ha styring av risikoen når det er relevant for levering av vedlikeholdstjenester (se nr. 3.1.1 Risikovurdering) skal det tas hensyn til minst følgende: <ul style="list-style-type: none"><li>(a) Identifikasjon av behovet for vedlikehold for å holde eiendelen i sikker drift, basert på den planlagte og faktiske bruken av eiendelen og dens konstruksjonsegenskaper.</li><li>(b) Håndtering når eiendelen tas ut av drift for vedlikehold, når det er avdekket feil eller når eiendelens tilstand forringes i en slik grad at den ikke lenger er innenfor grensene for sikker drift som nevnt i bokstav a).</li><li>(c) Håndtering når eiendelen gjeninnsettes i bruk, med eventuelle bruksrestriksjoner etter at det er utført vedlikehold for å garantere sikker drift av eiendelen.</li><li>(d) Styring av overvåkings- og måleutstyr for å sikre at eiendelen er egnet for det tilsiktede formålet.</li></ul>
5.2.5.	For å ha styring over informasjon og kommunikasjon når det er relevant for en sikker forvaltning av eiendeler (se nr. 4.4 Informasjon og kommunikasjon), skal virksomheten ta hensyn til <ul style="list-style-type: none"><li>(a) utveksling av relevant informasjon internt i virksomheten eller med eksterne enhet med ansvar for vedlikehold (se nr. 5.3 Entreprenører, partnere og leverandører), særlig om sikkerhetsrelaterte feil, ulykker og hendelser samt om eventuelle bruksrestriksjoner for eiendelen,</li><li>(b) sporbarhet av all nødvendig informasjon, herunder informasjon i forbindelse med bokstav a) (se nr. 4.4 Informasjon og kommunikasjon og nr. 4.5.3 Styring over dokumentert informasjon),</li><li>(c) opprettelse og ajourføring av registre, herunder styring av endringer som påvirker eiendelens sikkerhet (se nr. 5.4 Endringsstyring).</li></ul>

### 5.2.2 Formål

Søker må vise hvordan deres eiendeler forvaltes gjennom levetiden fra design til avhending, gjennom prosedyrer og ordninger som er angitt i sikkerhetsstyringssystemet. Søker må vise at det har blitt anvendt en menneskelig sentrert tilnærming for hver fase i løpet av levetiden. Det må beskrives hvor forvaltningen av eiendeler grenser til ulike elementer i sikkerhetsstyringssystemet, som kompetansestyring, driftsplanlegging og overvåking. Søker bør vise at det foreligger et robust system for forvaltning av eiendeler som gjenspeiler risiko som oppstår fra virksomhetens type og omfang.

### 5.2.3 Forklarende merknader

«Eiendeler» **(5.2)** viser til alt utstyr (fast eller mobilt), strukturer, programvare eller andre komponenter som krever vedlikehold over tid, og som er anskaffet for å drive jernbanevirksomheten. Eiendeler vil bli delt inn i hva som forvaltes av jernbaneforetaket (hovedsakelig kjøretøy) og hva som forvaltes av infrastrukturforvalteren (alle infrastrukturkomponenter, for eksempel skinner, utstyr for styring/signaler, sporvekslere, kraftforsyning, planoverganger, byggeteknikk, for eksempel broer, viadukter, tunneler, plattformer, heiser, rulletrapper, etc. En fullstendig liste kan finnes i vedlegg I til direktiv (EU) 2012/34).

Levetiden omfatter følgende faser:

- a) *Design;*
- b) *Gjennomføring (bygging/produksjon, installasjon, testing og idriftsetting);*
- c) *Drift og vedlikehold;*
- d) *Reparasjoner, endringer og ettermontering, som innebærer endringsstyring;*
- e) *Utsifting, avvikling og avhending.*

Krav knyttet til vedlikehold **(5.2.4)** er avledet fra ECM-forordningen. Godsvogner er en eiendel som et jernbaneforetak og muligens en infrastrukturforvalter skal forvalte. Kravene i ECM-forordningen er mer spesifikke og veiledende, mens de ovennevnte kravene hovedsakelig omfatter samhandling mellom jernbaneforetaket eller infrastrukturforvalterens sikkerhetsstyringssystem og ECMs vedlikeholdssystem, med sikte på å forsikre om at eiendeler er trygge for drift og vedlikehold. Risikovurderingen bør også fokusere på potensielle sikkerhetsfaktorer ved eventuelt erstatningsutstyr i løpet av vedlikeholdet (som er en del av levetiden til eiendeler) i samsvar med kravene i direktiv (EU) 2016/797 og relevante TSI-er.

Ikke alle eiendeler er regulert av TSI **(5.2.3)**, og selv om en TSI skulle gjelde (for eksempel TSI INF), reguleres bare hva som er nødvendig for interoperabilitet, noe som betyr at andre sikkerhetskrav fortsatt kan være nødvendig. Etterlevelse av de essensielle kravene i relevante TSI-er (ikke bare grunnleggende krav til sikkerhet) skal opprettholdes ved bruk av erstatningsutstyr, eller utskifting eller oppgradering i samsvar med bestemmelsene i direktiv (EU) 2016/797.

Begrepet «sikker drift» **(5.2.4 (a))** betyr at eiendeler skal drives innenfor dets sikre bruksgrenser. Sikkerhetsgrensene for bruk kan være i utvikling gjennom hele systemets levetid, men skal defineres med tanke på interoperabilitetsparametrene. Defekter kan identifiseres **(5.2.4 (b))** og på grunnlag av en årsaksanalyse kan de sikre bruksgrensene tilpasses i henhold til årsaksanalysen. For kjøretøy betyr sikker drift en sikker tilstand under drift i samsvar med artikkel 14(2) i direktiv (EU) 2016/798.

Endringer **(5.2.5 (c))** inkluderer den unike identifikasjonen på eiendelene, deres lokasjon, eventuelt vedlikehold som er gjort, etc. (og ikke bare styring av endringer). Endringsstyring for (tekniske) endringer gjelder for erstatningsutstyr.

Det skal utnevnes en ECM (enhet med ansvar for vedlikehold) i samsvar med artikkel 14(1) i direktiv (EU) 2016/798, for å sikre at godsvogner enheten vedlikeholder, er i forsvarlig driftstilstand. Det er ikke nødvendig å komme med detaljerte beskrivelser av aktiviteter som er utført av en ECM som er sertifisert i samsvar med

The NSA NO 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.

forordning (EU) nr. 445/2011. På en annen side er det nødvendig å angi hvilke elementer og hvilke aspekter som er omfattet av ECM-sertifikatet, og hvordan samhandling med ECM håndteres, spesielt hvilken informasjon som utveksles mellom søkeren og ECM, og hvordan dette gjøres.

Når det gjelder vogner som vedlikeholdes av ECM uten sertifisering (dvs. ikke sertifisert i samsvar med EU-forordning (EU) 445/2011), er det søkers ansvar å sørge for at vognene de drifter er i sikker driftstilstand, ved å påse at ECM-enheten uten sertifisering har utviklet og implementert et vedlikeholdssystem i samsvar med artikkel 14(2), 14(3) og vedlegg III til direktiv (EU) 2016/798. I tilfeller der ECM uten sertifisering ikke er en del av søkers virksomhet, må det sørges for at lovbestemte forpliktelser imøtekommes gjennom avtaleordninger.

Når det gjelder samarbeid mellom jernbanevirksomheter, forblir hver enkelt jernbanevirksomhet fullt ut ansvarlig for at driften utføres på en sikker måte, og håndterer således risiko knyttet til virksomheten, herunder å sørge for vedlikehold på vogner. Dersom en jernbanevirksomhet bruker et samarbeidspartners sikkerhets sertifikat for å håndtere risiko som er knyttet til vedlikehold, er dette ikke tilstrekkelig dersom det ikke er avtalefestet mellom de samarbeidende virksomhetene. Disse avtaleordningene må utvikles og overvåkes av hver av partene og være en del av begge parter sikkerhetsstyringssystemer, og er således underlagt tilsyn av respektive NSA. Respektive NSA skal koordinere for å løse eventuelle samhandlingsproblemer på tvers av grensene som kan ha blitt skapt av partene i avtalen.

#### 5.2.4 Dokumentasjon

- *Informasjon om systemet for forvaltning av eiendeler i virksomhetens sikkerhetsstyringssystem, inkludert relevante lenker til andre områder som risikovurdering, driftsplanlegging, endringsstyring osv. (5.2.1), (5.2.2), (5.2.5 (a)-(b))*

##### **Designfasen**

- *Dokumentasjon på prosesser og konsultasjoner for å fastslå behov for eiendeler*
- *Dokumentasjon på risikostyringsstrategier for anskaffelse og bruk av nye eller modifiserte eiendeler*
- *Dokumentasjon på alle relevante prosesser for design og levering av eiendeler*
- *Prosesser for risikostyring i designfasen*
- *Dokumentasjon på hvilke verktøy som brukes for å ivareta sikkerheten*
- *Informasjon om standarder eller annen sikkerhetsinformasjon som design og vedlikehold av eiendeler er gjenstand for, og eventuelle tester som anvendes til å bekrefte samsvar*
- *Om det foreligger en håndbok eller lignende som beskriver prosessene for drift og vedlikehold av eiendeler, og for risikostyring i drifts- og vedlikeholdsfasen*

##### **Implementeringsfasen**

- *Dokumentasjon på sikkerhetsstyring, testing og validering av prosesser som dekker bygging/produksjon og idriftssetting av eiendeler og at det er klart til å settes i drift*

##### **Drifts- og vedlikeholdsfasen**

- *Dokumentasjon på kontinuerlig etterlevelse av standarder og prosesser, samt styring av identifisert risiko*
- *Vedlikeholdsplaner og prosedyrer for vedlikehold av eiendeler*
- *Dokumentasjon på virksomhetens tiltak for å identifisere og eliminere risiko*
- *Dokumentasjon på prosessene som brukes til å rapportere om og håndtere eventuelle ytelsesproblemer, samt iverksette korrigerende tiltak*

---

The NSA NO 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.

- Dokumentasjon på anvendelse av ytelsesvalidering mot den antatte strategiske levetiden til en eiendel, for sporing av ytelse og planlegging av utskifting
- Prosesser for å identifisere feil og svikt, og iverksetting av korrigerende tiltak
- Håndtering av nødsituasjoner eller andre situasjoner som ikke er en del av rutinen, som kan påvirke sikkerheten ved eiendelene
- Dokumentasjon på at forvaltning av eiendeler er tatt hensyn til for meldepliktige hendelser og styring av felles risiko ved samhandling (**se også 3.1**)

#### **Utskifting, avvikling og avhending**

- Dokumentasjon på prosesser for håndtering av risiko knyttet til utskifting, avvikling eller avhending av eiendeler, i samsvar med virksomhetens omfang og art
- Dokumentasjon på en systematisk tilnærming for håndtering av menneskelige og organisatoriske faktorer i alle faser i løpet av eiendelens levetid (**5.2.1**)
- Dokumentasjon på at driftsdokumentasjonen står i samsvar til kravene til styring av (driften og) vedlikeholdet ved organisatoriske og fysiske grenser, for eksempel organisatorisk, teknisk og driftsmessig samhandling med nærliggende infrastruktur, grensende stasjoner, samhandling med andre jernbanevirksomheter eller infrastrukturforvaltere, etc. (**5.2.3**)
- Informasjon der søkeren viser at vedlikeholdsordningene samsvarer med foreliggende krav (lovgivning, standarder osv.) (**5.2.3**)
- Med hensyn til kjøretøy, en kopi av ECM-sertifikatet eller dokumentasjon på at artikkel 14(2), 14(3) og vedlegg III til direktiv (EU) 2016/798 etterleves av enheten med ansvar for vedlikeholdet. (**5.2.4 (a)-(d)**)

Ved partnerskap mellom jernbanevirksomheter der kjøretøy vedlikeholdes av samarbeidspartner: Dokumentasjon på at det foreligger avtaler mellom partene, herunder:

- Utveksling av informasjon som beskrevet i artikkel 5 i forordning (EU) 445/2011;
- Teknisk støtte når det er hensiktsmessig, spesielt for gamle CCS-systemer;
- Kontroll av evnen verkstedene vedlikeholdsleverandøren har til å utføre vedlikeholdet;
- Overvåking av vogner og utveksling av relevant informasjon som følge av denne overvåkingen (**se også 6.1**)
- Med hensyn til eiendeler som krever et samsvarssertifikat i henhold til EU-lovgivningen eller nasjonale bestemmelser, en kopi av slikt sertifikat sammen med en forklaring på i hvilken grad det er vesentlig som en del av sikkerhetsstyringssystemet (**5.2.4 (a)-(d)**)
- Informasjon om bruken av verktøy for sikkerhetsvarsling (SAIT) (**5.2.5 (a)**)
- Informasjon om hvordan dokumentstyringsdelen i sikkerhetsstyringssystemet fungerer for forvaltning av eiendeler, herunder dokumentasjon på at vedlikeholdsdokumentasjonen (prosedyrer, arbeidsinstrukser, etc.) oppdateres når og der det er nødvendig (**5.2.5 (a)-(c)**)
- Dokumentasjon på endringsstyring av eiendeler gjennom hele levetiden, inkludert eventuelle foreliggende prosesser for endringsstyring for å håndtere grunnkonfigurasjoner (**5.2.5 (c)**)

#### **5.2.5 Eksempler på dokumentasjon**

##### **Designfasen**

Virksomheten dokumenterer alle relevante prosesser og informasjon knyttet til design og levering av eiendeler ved knyttet til styring av endringer i eiendeler. Disse skisserer de tekniske og organisatoriske aktivitetene som etablerer og opprettholder kontroll over eiendeler gjennom hele levetiden.

Virksomheten etablerer og dokumenterer en prosess for å håndtere risiko knyttet til design av eiendelen, ved å:

- fastsette krav til eventuelle nye og/eller modifiserte eiendeler (*se også 1*) og drøfter dem med relevante interessenter (*se også 2.4*);
- håndtere risiko forbundet med å gjennomføre slike endringer (*se også 3.1*); og
- håndtere risiko knyttet til anskaffelse av eiendeler og kontraktstyring når det er relevant (*se også 3.1 og 5.3*).

Dette bør omfatte fare-/sikkerhetsanalyser for å identifisere områder som er mest utsatt for feil, og som gjennomgås for virksomhetens farelogg. Dette kan gjøres ved å identifisere sikkerhetskritiske systemer og etablere grunnleggende ytelsesmål gjennom å anvende hensiktsmessig risikoidentifisering, som for eksempel:

- RAMS-analyse (pålitelighet, tilgjengelighet, vedlikeholdstilpasning og sikkerhet) av design av eiendeler (hvor grunnleggende kriterier til sikkerheten formidles til utviklere for å sikre at eiendelen er egnet for formålet); og
- FMECA-analyse (feilmodus, effekter og kritikalitet) og/eller RCM (pålitelighetsstyrt vedlikehold) for å håndtere risiko i designfasen og sørge for at vedlikeholdsplanene opprettholdes.

Det er viktig for en virksomhet å vise hvordan den fanger opp og opprettholder (system- og) sikkerhetskrav for sine eiendeler, og hvordan disse blir verifisert, validert og sporet.

Disse kravene anvendes mot de spesifikke standardene og prosessene som anvendes for design, vedlikehold og drift av jernbaneinfrastrukturen og rullende materiell, som identifisert av virksomheten. Virksomheten skal sikre at:

- sikkerhetskritiske systemer er utformet for funksjonelle spesifikasjoner
- det foreligger en plan for validering og idriftssetting for å bekrefte at eiendeler er egnet for formålet og trygt å betjene og vedlikeholde
- det er utarbeidet drifts- og vedlikeholdsdokumentasjon, som beskriver prosesser for oppdatering, gjennomgang og vedlikehold av eiendeler (*se også 4.5*).

Virksomheten viser at den anvender hensiktsmessige systemtekniske prosesser og prosesser for å sørge for god sikkerhet (for eksempel EN50126/8/9 for komplekse systemer) i tilnærming til design og anskaffelser. Dette kan gjøres ved å utarbeide en SEMP-plan (systemteknisk styringsplan), som spesifiserer prosedyren for å identifisere og protokollføre interessenter, systemkrav og sikkerhetsbehov.

### **Implementeringsfasen**

For å sikre en vellykket og sikker implementering av eiendeler, skal virksomheten etablere prosesser for å håndtere risiko knyttet til konstruksjon, testing og idriftssetting, i tråd med prosessene i sikkerhetsstyringssystemet.

Det må også implementeres en prosess som omfatter:

- testing, verifisering og validering av system- og sikkerhetskravene til eiendeler, som kan gjøres ved å anvende en «Styringsplan for testing og idriftssetting» eller tilsvarende; og
- sjekk av at eiendelen er klart for drift, som kan gjøres med en sjekkliste for driftsklarhet.

### **Drifts- og vedlikeholdsfasen**

Virksomheten skal utvikle drifts- og vedlikeholdsdokumentasjon for eiendeler, som skisserer prosessene som anvendes til å oppdatere, gjennomgå og vedlikeholde sine eiendeler. Denne skal beskrive omfanget av driften og, der det er aktuelt, strategiene som foreligger for å dekke alle relevante aktiviteter.

Denne dokumentasjonen:

- skal sikre at eiendeler driftes og vedlikeholdes i samsvar med oppbyggingen av eiendelen
- skal identifisere og innlemme alle sikkerhetsrelaterte forhold, som beskriver hvordan bruken av eiendeler kan være begrenset, og foreliggende bruksvilkår
- beskriver de pågående kontrollene som skal utføres

Proessen for å konfigurere design og levering av foreslått eiendel (beskrevet i designfasen), er utvidet til å dekke hele levetiden ved å:

- etablere og vedlikeholde oppføringer over alle eiendeler gjennom å opprette et register over eiendeler. Dette inneholder informasjon som for eksempel unik identifikasjon på eiendeler, lokasjon, eventuelt utført vedlikehold osv.
- administrere dokumenter og informasjon om eiendeler i samsvar med virksomhetens sikkerhetsstyringssystem (**se også 4.4 og 4.5**)
- fastslå kritikaliteten av eiendeler, basert på resultatene av en risikovurdering. Sikkerhetskritiske eiendeler skal føres opp i et register over eiendeler.

Virksomheten skal vise hvordan informasjon om eiendeler er utviklet, vedlikeholdt og innarbeidet i fareloggen.

Virksomheten skal på kontinuerlig basis overvåke etterlevelse av fastsatte standarder og prosesser, for å sikre at jernbanedriften fortsetter å være sikker og hensiktsmessig. For dette formål skal virksomheten etablere prosesser for å sikre at:

- eiendeler driftes og vedlikeholdes i samsvar med relevante håndbøker
- tilstanden på eiendeler overvåkes
- utstyr som er nødvendig for å teste eller inspisere eiendeler kontrolleres, kalibreres og vedlikeholdes korrekt
- eventuelle risikoer knyttet til drift og vedlikehold av eiendeler håndteres i samsvar med risikostyringsprosessene og alle HMS-regler på arbeidsplassen
- reservedeler er tilgjengelig for vedlikehold, spesielt for sikkerhetskritiske eiendeler. Dette kan gjøres ved å fastslå behovet for reservedeler for eiendeler basert på kritikalitet, som identifisert ved anvendelse av «pålitelighetsstyrt vedlikehold» (RCM).

Virksomheten har på plass vedlikeholdsplaner for eiendeler for å:

- ta hensyn til krav til kompetanse, kapasitet og ressurser
- tilrettelegge for informasjonsstyring og logging
- skaffe til veie detaljerte planer som er etablert gjennom en risikobasert prosess, og som definerer de ulike vedlikeholds nivåene og etablerte standarder for virksomhetsstrukturer, prosedyrer og ansvar for vedlikehold av eiendeler
- sørge for kalibrering av verktøy og utstyr som skal brukes ved vedlikehold.

Dette kan spesifikt omfatte:

- en teknisk vedlikeholdsplan (TMP)
- arbeidsinstrukser som er utledet fra og revidert mot TMP

Planleggingen dokumenteres og styres, for eksempel ved hjelp av et databasert vedlikeholdsstyringssystem (**se også 4.5**).

Virksomheten skal ha prosesser på plass for å sikre at:

- når en vogn eller noe utstyr er dedikert en oppgave, så skal:

---

The NSA NO 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.

- samsvaret i oppgaven/oppdraget som skal utføres (for eksempel at hver type rullende materiell er kompatibel med rutene) kontrolleres ved inspeksjon og før togavgang
- vedlikehold av sikkerhetskritiske komponenter gjøres i henhold til foreliggende plan (forebyggende vedlikehold med hyppighet og arbeid som skal utføres)
- vedlikeholdsarbeid defineres når det registreres feil, eller når sikre bruksgrenser overskrides (korrigerende vedlikehold), med mindre det er implementert driftsbegrensninger
- det treffes nødvendige tiltak så snart som mulig etter at det er registrert behov for endringer, for eksempel når utstyr tas ut av drift eller ved justering av driftsbegrensninger.
- arbeidsinstrukser er tilgjengelige for alle sikkerhetskritiske aktiviteter
- alle oppgaver er kontrollert for samsvar med bestemmelser
- dokumentasjon om utført vedlikehold er kontrollert **(se også 4.5)**
- kompetansebasert opplæring er tilgjengelig i alle sikkerhetskritiske systemer **(se også 4.1)**

En prosess/prosedyre for å sikre at driftsbegrensninger, enten midlertidige eller permanente (for eksempel på grunn av bestemte vogntyper eller bestemte strekninger), er:

- hensyntatt når en vogn eller noe utstyr er dedikert en oppgave/et oppdrag;
- formidlet til rett tid til ansatte som fører vognen eller utstyret (for eksempel lokomotivførere, togleder).

Når det foreligger prosesser for å håndtere risiko forbundet med sikkerhetskritiske eiendeler, overvåker virksomheten ytelsen til eiendelen mot identifisert risiko og egne forventninger.

Virksomheten skal vise at den:

- forstår ytelsen til sine sikkerhetskritiske eiendeler ved å identifisere hva som må overvåkes, måles og rapporteres
- har etablert og protokollført metoden og hyppigheten for overvåkning, måling, analyse og evaluering av ytelsen til sikkerhetskritiske eiendeler
- overvåker ytelsen mot den forventede strategiske levetiden på et eiendeler **(se også 6.1)**
- rapporterer om ytelsesproblemer basert på sikkerhetsrisikonivået og rapporterer videre sikkerhetsproblemer slik at de blir tatt hånd om på en egnet måte
- bruker resultatene fra overvåkingen til å tilpasse vedlikeholdsplanen der det er relevant
- etablerer kommunikasjonskanaler for å formidle resultatene **(se også 4.4)**
- forbedrer samsvaret ved sikkerhetskritiske eiendeler med standarder ved å:
  - gjennomgå drifts- og vedlikeholdskontroller og vurdere risikoen for at eiendeler ikke oppfyller fastsatte standarder
  - identifisere årsaken(e) til sikkerhetsproblemene
  - identifisere tiltak som kan være nødvendig å iverksette for å få eiendeler tilbake til sikker driftstilstand
- kontinuerlig forbedrer sikkerhetsstyringssystemet ved å identifisere potensielle farer og iverksette korrigerende tiltak **(se også 7.2)**
- dokumenterer når det er iverksatt tiltak for å redusere eller eliminere risiko, og hvordan dette ble oppnådd

Virksomheten må ha på plass prosesser for å identifisere eventuelle feil eller svikt som kan oppstå på deres eiendeler, og sørge for at korrigerende tiltak iverksettes. Disse skal være i tråd med bestemmelsene og vedlikeholdsprogrammene eller -planene, og:

- sikre at feil registreres og resulterende korrigerende tiltak iverksettes
- håndtere sikkerhetskritiske feil
- sikre rapportering av meldepliktige hendelser

- *koordinere reparasjoner av sikkerhetsrelaterte eiendeler som ikke er planlagt*

Virksomheten:

- *dokumenterer feilhåndteringsprosessen*
- *anvender egnede analyseteknikker for sikkerhetskritiske funksjoner, for eksempel «årsaksanalyse» (RCA)*
- *implementerer registrering av feil, som kan inkludere feilkoder, feilmodus, effekt, kritikalitet og korrigerende tiltak*
- *utvikler prosedyrer for håndtering av vanlige reparasjonsaktiviteter*
- *innfører en tilbakemeldingsprosess for teknisk personell for å gjennomgå og forbedre systemene og minimere risikoen for fremtidige feil*

Dette kan oppnås ved å anvende feilrapportering, analyse og korrigerende tiltak (FRACAS), som:

- *registrering av feil som ble oppdaget og registrert under testing og idriftssetting, samt eventuelle feil som oppstod under drift eller vedlikehold*
- *administrasjon av etterfølgende korrigerende tiltak som er truffet for å håndtere dem*

Virksomheten må som et minimum dokumentere alle feil og korrigerende tiltak, og få en teknisk kompetent person til å styre eventuelle reparasjoner som ikke er planlagt.

Prosessen/prosedyren for å håndtere nedsatt drift eller nødsituasjoner for forvaltning av eiendeler.

Virksomheten må etablere prosesser for å håndtere eventuelle risikoer ved samhandling som kan oppstå under driften og vedlikeholdet av eiendeler (**se også 3.1.1**). Dette omfatter samhandling mellom eiendeler og mellom aktører som bruker dem.

### ***Utsiftings-, avviklings- og avhendingsfasen***

Virksomheten må kjenne til tilstanden på sine eiendeler, og hvis tilstanden forringes må eiendeler skiftes ut eller utbedres deretter.

Det må etableres planer for validering og idriftssetting for å bekrefte at den nye eiendelen er egnet for formålet, og kan driftes og vedlikeholdes på en sikker måte. Hvis virksomheten utvider levetiden til en eksisterende eiendel må det hentes frem relevant sikkerhetsinformasjon, for eksempel historikk, for å sikre at det forblir sikkert i bruk.

Realitet mot forventet ytelse må overvåkes (se drifts- og vedlikeholdsfasen).

Ved avhending av jernbaneinfrastruktur eller kjøretøy må virksomheten håndtere risikoene ved å ta eiendeler ut av drift.

### ***Håndtering av endringer i sikkerhetskritiske eiendeler***

I situasjoner der en virksomhet kan ønske å endre konfigurasjonsgrunnlaget for sikkerhetskritiske eiendeler, må det implementeres en prosess for endringsstyring for å sikre hensiktsmessig risikostyring, og etableres et konfigurasjonsgrunnlag for alle sikkerhetskritiske eiendeler med tilknyttet programvare (enten integrert i eksisterende systemer eller frittstående programvare). Hvis en operatør endrer konfigurasjonsgrunnlaget for sikkerhetskritiske eiendeler, må man der det er mulig:

- *håndtere risiko som følge av endringer i eiendeler*
- *registrere serienummer og modellnummer*
- *validere funksjonelle krav mot spesifikasjoner og risikostyringstiltak*
- *kontrollere frigjøring av konfigurasjonselementer*
- *sikre at status på alle eiendeler under konfigurasjonsstyringen er oppdatert*

Endringer i etablerte grunnlag, driftsforhold eller vedlikeholdsplaner for sikkerhetskritiske eiendeler, må ikke redusere sikkerheten ved jernbanedriften på noen måte.

### **Anvendelse av felles sikkerhetsmetoder**

Proessen/prosedyren for å påse at enheter som er ansvarlig for vedlikehold (for eksempel ECM), anvender CSM vedrørende risikovurdering og CSM vedrørende overvåking der det er aktuelt (dvs. enten som kreves av lov og/eller er avtalefestet).

### **Anvendelse av integrering av menneskelige faktorer**

Det må foreligge en systematisk prosess for å anvende integrering av menneskelige faktorer gjennom levetiden til et system, for eksempel en prosess med arbeidsprosedyrer og tilstrekkelige ressurser som sikrer at menneskelige og organisatoriske faktorer vurderes og hensyntas på riktig måte.

Virksomhetens program må spesifisere et rammeverk for hvordan identifiserte menneskelige og organisatoriske faktorer vil bli identifisert, vurdert, akseptert og utviklet, for å komme frem til løsninger gjennom hele prosessen for design og endringsstyring. Programmet må spesifisere forholdet til andre parter knyttet til design eller endringer.

Informasjon er tilgjengelig for bruk av SAIT (Safety Alert Information Tool) (se kapittel 5.4.3)

#### **5.2.6 Referanser og standarder**

- [Veileder for anvendelse av artikkel 14 \(a\) i sikkerhetsdirektiv og kommisjonsforordning \(EU\) nr. 445/2011 om et system for sertifisering av enhet med ansvar for vedlikehold av godsvoagner](#)
- CENELEC — EN50126 Jernbaneapplikasjoner — Spesifikasjon og demonstrasjon av pålitelighet, tilgjengelighet, vedlikeholdstilpasning og sikkerhet (RAMS) Del 1: Elementært, krav og generelt, prosess
- Office of the National Rail Safety Regulator — Asset management guideline (2015)

#### **5.2.7 Relevante tema for tilsyn**

Fra et tilsynsperspektiv er det viktig at det fokuseres på forvaltningen av eiendelen gjennom hele levetiden, fra design til avhending, og ikke på individuelle feil i forvaltning av virksomhetens eiendeler, med mindre disse går direkte utover sikkerheten.

Tilsynet bør ta i betraktning hvordan eksisterende eiendeler som er utdatert i henhold til gjeldende standarder, håndteres og vedlikeholdes.

Tilsynet bør vurdere om og hvordan virksomheten bruker SAIT.

## 5.3 Entreprenører, partnere og leverandører

### 5.3.1 Lovbestemt krav

5.3.1.	Virksomheten skal identifisere og ha styring av sikkerhetsrisiko som oppstår som følge av utkontraktert virksomhet, herunder drift eller samarbeid med entreprenører, partnere og leverandører.
5.3.2.	For å ha styring av sikkerhetsrisiko nevnt i nr. 5.3.1 skal virksomheten definere kriteriene for utvelgning av entreprenører, partnere og leverandører samt kontraktsvilkårene som de må oppfylle, herunder: <ul style="list-style-type: none"><li>(a) Lovfestede krav og andre sikkerhetsrelaterte krav (se nr. 1 Virksomhetens kontekst),</li><li>(b) Kompetansenivået som kreves for å utføre oppgavene angitt i kontrakten (se nr. 4.2 Kompetanse).</li><li>(c) Ansvar for oppgavene som skal utføres.</li><li>(d) Det forventede sikkerhetsnivået som skal opprettholdes i kontraktsperioden.</li><li>(e) Forpliktelsene med hensyn til utveksling av sikkerhetsrelatert informasjon (se nr. 4.4 Informasjon og kommunikasjon).</li><li>(f) Sporbarheten av sikkerhetsrelaterte dokumenter (se nr. 4.5 Dokumentert informasjon).</li></ul>
5.3.3.	I samsvar med prosessen som er beskrevet i artikkel 3 i forordning (EU) nr. 1078/2012, skal virksomheten overvåke <ul style="list-style-type: none"><li>(a) sikkerhetsnivået for all virksomhet og drift som utføres av entreprenører, partnere og leverandører for å sikre at de oppfyller kravene angitt i avtalen,</li><li>(b) entreprenørenes, partnernes og leverandørenes bevissthet om sikkerhetsrisiko som de påfører virksomhetens drift</li></ul>

### 5.3.2 Formål

Søker må vise at man har evnen til å identifisere, vurdere og håndtere risiko som oppstår i forbindelse med leverandøraktiviteter eller andre samarbeidspartneres aktiviteter. Dette er ikke bare et spørsmål om risikovurdering. Det kreves heller ingen liste over alle risikoer eller relevante risikokategorier, men søker må vise hvordan systemene og prosedyrene som helhet er utarbeidet og organisert for å gjøre identifisering, vurdering og håndtering av disse risikoene lettere. Bruk av nøye formulerte avtaler er en allment akseptert måte å håndtere risiko på. Hovedansvaret for administrasjon av leverandører og styring av leveransen mot de fastsatte spesifikasjonene, ligger imidlertid hos virksomheten. Bruk av leverandører eller underleverandører betyr ikke at jernbanevirksomheten eller infrastrukturforvalteren delegerer noe av ansvaret sitt for å sikre at de avtalte tjenestene utføres til de standarder som er fastsatt før driften starter.

Søker skal vise at det foreligger prosesser for å fastslå kompetansen til leverandørene, samt for å vurdere deres sikkerhetsytelse som en del av anskaffelsesprosessen.

Hver enkelt virksomhet er ansvarlig for å utføre overvåkingsprosessen som er fastsatt i CSM om overvåking (overvåkingsforskriften), og sikre at det gjennom avtaleordninger føres tilsyn med risikokontrolltiltak som er implementert av leverandørene i samsvar med CSM om overvåking. Hvis virksomheter identifiserer eventuelle relevante sikkerhetsrisikoer som mangler eller funksjonsfeil på teknisk utstyr, kreves det i henhold

til CSM om overvåkning å rapportere disse risikoene til andre involverte parter, slik at de kan ta nødvendige grep for å ivareta sikkerheten ved systemet.

### 5.3.3 Forklarende merknader

Ytterligere informasjon om avtaleordninger og samarbeid finnes i Vedlegg 3.

### 5.3.4 Dokumentasjon

- Dokumentasjon på hvordan virksomhetens sikkerhetsstyringssystem samhandler med styringssystemene til leverandører for å kontrollere relevant risiko **(5.3.1)**
- Dokumentasjon på at det utarbeides avtaleordninger basert på resultater fra risikovurdering **(5.3.1)** **(se også 3.1)**
- Det foreligger prosesser som beskriver hvordan menneskelige og organisatoriske faktorer skal håndteres og formidles i forbindelse med bruk av underleverandører, samt styring av underleverandører **(5.3.1)**
- Dokumentasjon på hvordan virksomheten styrer dokumentasjonen som omfatter leverandører **(5.3.2 (a)-(d))**
- Dokumentasjon på hvordan virksomheten velger ut leverandører for å sikre at de er kompetente og at sikkerhetsrisiko håndteres korrekt **(5.3.2 (a)-(e))**
- Det foreligger prosess for å sikre umiddelbar formidling av sikkerhetsinformasjon til eller fra leverandører **(5.3.2 (d))**
- Prosessen eller prosedyren for overvåking som virksomheten har etablert for å sikre at leverandørenes samarbeidspartnere eller ansatte er i stand til å håndtere risiko de står overfor **(5.3.3 (a)-(b))**
- Dokumentasjon på at samarbeidspartnere eller leverandører føres regelmessig tilsyn med i samsvar med CSM om overvåking (forordning (EU) 1078/2012) for å sikre at deres produkter eller tjenester oppfyller spesifikke krav og sikkerhetsmål. **(5.3.3 (a)) (se også 6.1)**

### 5.3.5 Eksempler på dokumentasjon

Prosedyren der samarbeidspartnere og leverandører velges ut og føres tilsyn med. Prosedyren gjør det klart at standardene som skal anvendes av leverandørene, er de samme som for direkte ansatt personale og hva rollene og ansvaret omfatter. Prosedyren dokumenterer den nødvendige informasjonsutvekslingen mellom sikkerhetsstyringssystemene til søkeren og samarbeidspartnere/leverandører.

Sikkerhetsmålene det forventes at samarbeidspartnere og leverandører skal nå, og hvilke indikatorer som skal brukes til å måle om de nås. Dette inkluderer sikkerhetskulturen hos samarbeidspartnere og leverandører, samt eventuelle menneskelige og organisatoriske faktorer som kan være relevante.

Strategien for menneskelige og organisatoriske faktorer beskriver detaljene for hvordan disse forholdene er dekket for leverandører og underleverandører.

Virksomhetens prosedyre for styring av dokumentasjon, som håndterer hvilke standarder som skal benyttes av leverandører, underleverandører, partnere og leverandører (se også 4.5.1.1 (e) Dokumentstyring).

En liste/oversikt over samarbeidspartnere og leverandører for intern eller ekstern bruk, med spesifikasjon av produkter og/eller tjenester de leverer **(se også 4.5.1.1 (d) og (e))** og en beskrivelse av hva som kan virke inn

på sikkerheten, sammen med tiltakene for å håndtere identifisert risiko (for eksempel utveksling av informasjon, ansvarsfordeling og opplæring) (**se også 3.1.1.1 (a)**).

Prosedyren for kompetansestyring som knytter seg til systemene hos samarbeidspartnere og leverandører.

Prosesen/prosedyren for administrasjon av samarbeidspartnere og leverandører må inkludere hvordan samhandlingsrisiko som oppstår som følge av samarbeidspartneres eller leverandørers virksomheter håndteres og deles med dem det er relevant for, hvordan disse inngår i avtaleordninger og hvordan utveksling av informasjon er integrert i virksomhetens sikkerhetsstyringssystem.

Den aktuelle prosessen for revisjons-/inspeksjonsplanlegging for samarbeidspartnere og leverandører med noen eksempler på slike aktiviteter, for eksempel revisjons-/inspeksjonsrapporter eller funn.

Prosesen eller prosedyren for hvordan relevante krav som gjelder samarbeidspartnere eller leverandører identifiseres og meddeles, og der det er relevant, hvordan de inngår i avtaleordninger som er dokumentert i system for dokumentstyring, slik at informasjonen kan spores.

Prosedyren for styring av dokumentasjon som administrasjon av sertifikater, godkjenninger, anerkjennelser eller annen form for dokumentasjon som viser at kravene for samarbeidspartnere eller leverandører etterleves, og som styrer gyldigheten over tid (for eksempel gjennom tilsyn).

### 5.3.6 Relevante tema for tilsyn

Ved tilsyn i en virksomhet kan det, for å få et komplett bilde av omfanget av styring og overvåkning, være nødvendig å gjennomføre tilsyn hos en samarbeidspartner eller leverandør sammen med en som jobber i virksomheten. Det kan også være nødvendig å få tilgang til dokumentasjonen som samarbeidspartneren eller leverandøren jobber med, og undersøke hvordan den er tilknyttet prosedyrene i virksomhetens sikkerhetsstyringssystem.

Ordninger for å sikre at samarbeidspartneres og leverandørers sikkerhetsytelse og kompetanse er en integrert del av anskaffelsesprosessen.

## 5.4 Endringsstyring

### 5.4.1 Lovbestemt krav

5.4.1. Virksomheten skal gjennomføre og styre endringer i sikkerhetsstyringssystemet for å opprettholde eller forbedre sikkerhetsnivået. Dette skal omfatte beslutninger i de ulike fasene av endringsstyringen og den etterfølgende gjennomgåelsen av sikkerhetsrisiko (se nr. 3.1.1 Risikovurdering).

### 5.4.2 Formål

Det er viktig at søker kan identifisere og reagere på ny risiko som kan oppstå ved driften, ved å anvende kravene ved vesentlige endringer i direktiv (EU) 2016/798 og CSM om risikovurdering (CSM RA) og annen vurdering (kommisjonens gjennomføringsforordning (EU) 402/2015). Sikkerhetsstyringssystemet må vise at det foreligger prosedyrer for å vurdere risiko og iverksette nye risikokontrolltiltak der det er aktuelt. Dette skal imøtekomme alle typer og nivåer i endringene — betydelige og mindre, permanente og midlertidige, umiddelbart og langsiktig. Det skal gjelde for endringer i:

- typer aktiviteter
- utstyr
- prosedyrer
- organisering
- bemanning
- samhandling

Proessen skal åpne for at risiko kan vurderes på en proporsjonal og robust måte, inkludert menneskelige faktorer når det er hensiktsmessig, og for å kunne iverksette kontrolltiltak.

Endringer i roller, ansvar, verktøy og utstyr, arbeidsmiljø, prosesser og prosedyrer støttes av en analyse av menneskelige og organisatoriske faktorer. Det er viktig for å identifisere mulig risiko knyttet til endringen. Metoder som brukes kan for eksempel være oppgaveanalyse, analyse av brukervennlighet, simulering, risikovurdering, HAZOP og sikkerhetsundersøkelse. Risikovurdering av endringer har en tilnærming som ivaretar menneskelige og organisatoriske faktorer. Spesielt kan dette gjelde for endring av arbeidsprosedyrer på grunn av endret utstyr, endring av arbeidsplaner eller omfordeling av ansvarsområder.

### 5.4.3 Forklarende merknader

Ikke alle endringer er underlagt risikovurdering (**5.4.1**). Når endringer håndteres aktivt gjennom andre prosesser i sikkerhetsstyringssystemet, som for eksempel i den daglige driften, trenger de ikke å anses som en endring i den formelle endringsprosessen.

Roller, ansvar og myndighet som skal defineres (**se også 2.3**) inkluderer endringsstyring (**5.4.1**), for eksempel tilordning av roller til et styre for gjennomføring av en større endring i en virksomhet.

De ansatte bør konsulteres under endringsprosessen (**se også 2.4**).

Endringer i roller, ansvar, verktøy og prosesser skal også foregå gjennom en analyse av sikkerhetskulturfaktor som er knyttet til endringen, for å identifisere mulig sikkerhetsrisiko. Sikkerhetsrisiko som følger av nedskjæringer, ledelsesendringer eller outsourcing av aktiviteter, herunder drift eller samarbeid med samarbeidspartnere og leverandører, skal håndteres og prioriteres på lik linje med intern risiko.

#### 5.4.4 Dokumentasjon

- En beskrivelse av prosessen for endringsstyring **(5.4.1)**
- En beskrivelse av prosedyrene og metodene som anvendes til å evaluere ny eller endret risiko og implementere nye prosedyrer og metoder **(5.4.1)**
- Kontrolltiltak inkludert henvisning til hvor detaljerte prosesser kan finnes **(5.4.1)**
- Informasjon om hvordan virksomheten identifiserer vesentlige endringer og beslutninger om når man skal anvende prosessene i CSM om risikovurdering og annen vurdering, eller når man skal utføre risikovurdering i henhold til prosedyrene for sikkerhetsstyringssystemet, inkludert vurdering av menneskelige og driftsmessige faktorer **(5.4.1)**
- Informasjon om ordninger i endringsstyringen som virksomheten har etablert for styring av tillatelse til å ta i bruk kjøretøy og endringer i felles sikkerhetssertifikat eller sikkerhetstillatelse **(5.4.2)**
- Informasjon om prosessen for varsling til relevante sikkerhetsmyndigheter om endringene, før idriftsettelse. **(5.4.2)**

#### 5.4.5 Eksempler på dokumentasjon

En kopi av prosedyren for endringsstyring som en del av søknaden. Dette dokumentet dekker behovet for risikovurdering av alle endringer i henhold til ulike lovfestede krav. Et eksempel på en problem- og planleggingslogg som regelmessig blir vurdert ved fremdriften i endringene. Til sist skal prosedyren også dekke prosessen for hvordan relevante nasjonale sikkerhetsmyndigheter blir varslet om endringene.

Proessen for endringsstyring skal vise at resultatene fra risikovurderingsprosessen er en del av endringsstyringsprosessen og at de tas i betraktning når man utvikler, implementerer og vurderer driftsprosesser.

#### 5.4.6 Relevante tema for tilsyn

For å fastslå om ordninger for endringsstyring i sikkerhetsstyringssystemet er robuste nok, vil det være nødvendig å følge en rekke endringer av ulike typer gjennom prosessen for å vise om de har (a) blitt håndtert hensiktsmessig og risikoer som følge av endringene er hensiktsmessig vurdert, og (b) om det har blitt innlemmet eventuelle erfaringer i revisjoner av prosedyrene i sikkerhetsstyringssystemet.

Vurdering av etterlevelse av ordningene i endringsstyringen mot CSM RA.

Virksomheten må ha på plass prosesser for implementering og kontinuerlig overvåking av relevante TSI-er, nasjonale bestemmelser og andre standarder, hvor det er hensiktsmessig å vise hvordan disse brukes gjennom hele levetiden til utstyret eller driften.

## 5.5 Håndtering av nødsituasjoner

### 5.5.1 Lovbestemt krav

- 5.5.1. Virksomheten skal identifisere nødssituasjoner og tilhørende tiltak som skal treffes til rett tid for å håndtere disse (se nr. 3.1.1 Risikovurdering) og for å gjenopprette normale driftsforhold i samsvar med forordning (EU) 2015/995<sup>(2)</sup>.
- 5.5.2. Virksomheten skal for hver identifiserte type nødssituasjon sikre at
  - (a) beredskapstjenestene umiddelbart kan kontaktes,
  - (b) beredskapstjenestene får all relevant informasjon, både på forhånd, for å forberede beredskapsinnsatsen, og når en nødssituasjon oppstår,
  - (c) førstehjelp gis internt.
- 5.5.3. Virksomheten skal identifisere og dokumentere roller og ansvarsområder for alle parter i samsvar med forordning (EU) 2015/995.
- 5.5.4. Virksomheten skal ha planer for tiltak, varsling og informasjon i nødssituasjoner, herunder ordninger for å
  - (a) varsle alt personale med ansvar for håndtering av nødssituasjoner,
  - (b) formidle informasjon til alle parter (f.eks. infrastrukturforvalter, underleverandører, myndigheter, beredskapstjenester), herunder instruksjoner for nødssituasjoner for passasjerene,
  - (c) treffe nødvendige beslutninger i samsvar med typen nødssituasjon.
- 5.5.5. Virksomheten skal beskrive hvordan ressurser og midler for håndtering av nødssituasjoner er fordelt (se nr. 4.1 Ressurser) og hvordan opplæringskravene er fastlagt (se nr. 4.2 Kompetanse).
- 5.5.6. Beredskapsplaner prøves ut regelmessig i samarbeid med andre berørte parter og ajourføres etter behov.
- 5.5.7. Virksomheten skal sikre at infrastrukturforvalteren enkelt og uten opphold kan kontakte kvalifisert ansvarshavende personale med tilstrekkelige språkkunnskaper og få riktig informasjon.
- 5.5.8. Virksomheten skal ha en framgangsmåte for å kontakte enhet med ansvar for vedlikehold eller innehaveren av jernbanekjøretøyet i en nødssituasjon.
- 5.5.7. Virksomheten skal samordne beredskapsplaner med alle jernbaneforetak som benytter virksomhetens infrastruktur, med beredskapstjenestene for å gjøre det lettere for dem å kunne gripe inn hurtig, samt med alle andre parter som kan være involvert i en nødssituasjon.
- 5.5.8. Virksomheten skal ha ordninger for om nødvendig å stanse drift og jernbanetrafikk umiddelbart og underrette alle berørte parter om de tiltak som er truffet.
- 5.5.9. Når det gjelder grensekryssende infrastruktur, skal samarbeidet mellom de relevante infrastrukturforvalterne forenkle den nødvendige samordningen og beredskapen til vedkommende beredskapstjenester på begge sider av grensen.

<sup>(2)</sup> Kommisjonsforordning (EU) 2015/995 av 8. juni 2015 om endring av beslutning 2012/757/EU om den tekniske spesifikasjonen for samtrafikkveier med hensyn til delsystemet «Drift og trafikkstyring» i Den europeiske unions jernbanesystem (EUT L 165 av 30.6.2015, s. 1).

### 5.5.2 Formål

Robuste systemer for beredskapsplanlegging er avgjørende, og må dekke informasjonen som skal formidles til beredskapstjenestene, slik at de kan utarbeide beredskapsplaner. Aspektene ved sikkerhetsstyringssystemet som er direkte relevante for virksomhetens beredskap, for eksempel opplæring i beredskap og testing av beredskapsplaner, er også viktig.

### 5.5.3 Forklarende merknader

Nødsituasjoner **(5.5.1)** er tilknyttet resultatene fra virksomhetens risikovurdering, selv om TSI-OPE (se punkt 4.2.3.7) har en omfattende liste over nødssituasjoner.

Kravene 5.5.7 og 5.5.8 i lovteksten står skrevet med blå tekst der kravet gjelder for infrastrukturforvalter, og i svart tekst der kravet gjelder for jernbaneforetakene. Kravet 5.5.9 er skrevet i blått, og gjelder kun for infrastrukturforvalter.

### 5.5.4 Dokumentasjon

Søker forventes å gi oversikt over:

- *typer nødstilfeller som dekkes, herunder nedsatt drift og foreliggende prosedyrer for å håndtere dem **(5.5.1)***
- *informasjon fra søker for å gjøre det mulig for beredskapstjenestene å planlegge hvordan de skal respondere ved en storulykke på jernbanen, der det er hensiktsmessig å henvise til forpliktelser i henhold til gjeldende EU-lovgivning og eventuelle relevante grenseoverskridende ordninger **(5.5.2 (a) og (b))***
- *planer, roller og ansvar (herunder for dem med dedikert kompetanse som er satt til å bistå infrastrukturforvalteren eller omvendt), opplæring og ordninger for å opprettholde kompetansen, og ordninger for hensiktsmessig kommunikasjon med beredskapstjenestene, relevant personell og kommunikasjon med dem som berøres av uønskede hendelser som passasjerer eller berørte tredjeparter (dette skal inkludere et dokument som beskriver alle parter roller og ansvar, hvordan ressurser og midler er tilordnet og der krav til opplæring er identifisert). Prosedyrene for å komme tilbake til normal drift etter en nødsituasjon **(5.5.1), (5.5.3), (5.5.4 (a) (c)), (5.5.5), (5.5.7) (5.5.8 og 5.5.9 (kravene gjelder kun for infrastrukturforvaltere))***
- *Spesifikke aspekter ved sikkerhetsstyringssystemet som er direkte relevante for beredskapsordningene, for eksempel opplæring i beredskap og testing av beredskapsplaner. Disse er også viktige for å identifisere eventuelle svakheter **(5.5.6)***
- *prosedyren for å kontakte enhet med ansvar for vedlikehold eller innehaver, ved nødsituasjoner som berører en av deres kjøretøy **(5.5.8 (kravet gjelder kun for jernbaneforetak))***

### 5.5.5 Eksempler på dokumentasjon

En kopi av prosedyrer for beredskapsstyring og tilknyttede planer (for eksempel prosedyrer for berging). Prosedyren må dekke hele jernbanenettet som drives, med spesifikke ordninger som er nødvendige for tunneler og andre steder med høy risiko og for grenseoverskridende samarbeid, bemanning og roller og ansvar, og som inkluderer lenker til beredskapsordninger hos infrastrukturforvalteren og hvordan man kommer i kontakt med andre relevante parter, som ECM, der det er relevant. I prosedyren må det være en referanse til kompetansekrav for ansatte som skal respondere på nødsituasjoner, samt sørge for at innleid personell kan imøtekomme de samme standardene.

Nødprosedyrene skal omfatte prosessen der ofre for uønskede hendelser og deres pårørende får veiledning om klageprosedyrer.

Prosedyren (dersom relevant) må inneholde informasjon om hva som skjer i en nødssituasjon der farlig gods er involvert, og jernbaneforetaket skal ha etablert en prosess for å sikre at:

- *den som laster, tankvognens eier der den er privateid, eieren eller innehaveren og operatøren i tilfelle en tank, mottakeren, etc., kan kontaktes umiddelbart.*
- *infrastrukturforvalteren må gis relevant informasjon så snart som mulig (for eksempel vognens registreringsnummer, vognens posisjon i togrekken, UN-nummer, RID-klassifiseringskode og fareidentifikasjonsnummer for farlig gods i samsvar med RID-bestemmelsene);*
- *virksomheten (infrastrukturforvalteren) må ha etablert en prosess for å sikre at myndighetene (for eksempel redningstjenester, politi, andre beredskapstjenester og myndigheter) får relevant informasjon om farlig gods (se eksemplene ovenfor).*

#### 5.5.6 Relevante tema for tilsyn

For å kunne vurdere prosedyrene i sikkerhetsstyringssystemet som gjelder beredskap, kan det være nødvendig å kryssjekke prosedyrene i sikkerhetsstyringssystemet med prosedyrene hos relevante aktører det samhandles med (spesielt forholdet mellom sentrale aktører som jernbaneforetak, infrastrukturforvalter og beredskapstjenestene) for å sikre at prosessene som foreligger for håndtering av slike hendelser er helhetlige.

Sjekke at det foreligger planer for alle forutsigbare nødsituasjoner.

Ordninger for testing av beredskapsplaner og koordinerte ordninger med nødetater, og ikke begrenset til teoretiske øvelser.

Det må foreligge samhandlingsordninger med andre interessenter og inkludere testing, kontroll, kommunikasjon, koordinering og kompetanse.

## 6 Vurdering av resultater

### 6.1 Overvåking

#### 6.1.1 Lovbestemt krav

- 6.1.1. Virksomheten skal foreta overvåking i samsvar med forordning (EU) nr. 1078/2012
- (a) for å kontrollere om alle prosessene og prosedyrene i sikkerhetsstyringssystemet, herunder driftsmessige, organisatoriske og tekniske sikkerhetstiltak, anvendes riktig og om de er effektive,
  - (b) for å kontrollere om sikkerhetsstyringssystemet som helhet anvendes riktig og gir de forventede resultater,
  - (c) for å undersøke om sikkerhetsstyringssystemet oppfyller kravene i denne forordning,
  - (d) for å fastslå og gjennomføre korrigerende tiltak og vurdere hvor effektive tiltakene er (se nr. 7.2 Kontinuerlig forbedring), ved behov, dersom relevante tilfeller av manglende samsvar med bokstav a), b) og c) blir oppdaget.
- 6.1.2. Virksomheten skal regelmessig overvåke hvordan sikkerhetsrelaterte oppgaver utføres på alle nivåer i virksomheten og gripe inn dersom oppgavene ikke utføres på riktig måte.

#### 6.1.2 Formål

Virksomheten skal fremlegge dokumentasjon på at det foreligger en prosess for å overvåke anvendelsen og hensiktsmessigheten ved sikkerhetsstyringssystemet, og at denne prosessen er tilpasset driftens størrelse, art og omfang. Virksomheten må vise at prosessen kan identifisere, evaluere og utbedre eventuelle feil i sikkerhetsstyringssystemets funksjon.

#### 6.1.3 Forklarende merknader

Virksomheten bør ha en prosess på plass for å evaluere hensiktsmessigheten av gjennomførte korrigerende tiltak etter at en risikovurdering er utført. Det bør gå en viss tid før gjennomførte korrigerende tiltak vurderes for å forsikre seg om at ventet reduksjon i sikkerhetsrisiko er oppnådd som følge av anvendelsen av tiltakene (6.1.1 (d)).

Overvåkingen bør omfatte vurderinger av hvor vellykket strategien for menneskelige og organisatoriske faktorer har vært.

Resultatene er systematisk vurdert med bakgrunn i virksomhetens strategi for forbedring av sikkerhetskulturen. Forbedring av sikkerhetskulturen bør være tilpasset og være en del av målet om forbedring av sikkerheten.

Selvkritiske og objektive vurderinger av virksomhetens sikkerhetskultur, praksis og ytelse, utføres med jevne mellomrom. Sikkerhetsinformasjon, som for eksempel korrigerende handlingsplan, menneskelig yteevne, hendelses- og ulykkesanalyse, undersøkelser og relevant intern og ekstern driftserfaring, samles systematisk inn og evalueres for å identifisere trender. I tillegg for å unngå organisatoriske og individuelle snarveier eller selvtilfredshet.

En vellykket vurdering kan bidra til å forbedre sikkerhetsytelsen ved å gi et klart bilde av hvordan virksomhetens sikkerhetskultur påvirker sikkerheten. Evalueringen søker å identifisere sterke og svake sider

i sikkerhetskulturen ved å sammenligne hvordan kulturen er, med hva den skal ta sikte på. Dette gjør det mulig å prioritere områder for å forbedre og gjennomføre endringer, for eksempel i behandling, opplæring og atferd. Evaluering av sikkerhetskulturen er et middel for å arbeide i forkant for å forbedre sikkerhetsresultat og øke sikkerhetsmarginene. Det anbefales å foreta uavhengige evalueringer av sikkerhetskulturen hvert tredje til femte år, og organisatoriske egenvurderinger hvert år eller annethvert år.

#### 6.1.4 Dokumentasjon

- *Informasjon om hvordan søkeren har implementert CSM om overvåking (6.1.1 (a))*
- *Informasjon om hvordan overvåkingsprosessen kan se om de forventede resultatene blir oppfylt (6.1.1 (b))*
- *Dokumentasjon på at sikkerhetsstyringssystemet har blitt tilpasset som følge av korrigering av feil i prosessene for sikkerhetsstyring som er identifisert under overvåking (6.1.1 (c))*
- *Virksomheten bør ha på plass en prosess for å fastsette ytelsesstandarter og indikatorer for overvåking knyttet til driftsprosesser, samt for gjennomførte endringer. Det bør være et program for kontinuerlig vurdering av ytelsen til prosesser knyttet til menneskelige og organisatoriske faktorer, samt resultatene fra disse prosessene, for eksempel at personellet overholder implementerte prosedyrer, og bruker nytt utstyr korrekt. (6.1.2)*

#### 6.1.5 Eksempler på dokumentasjon

En redegjørelse som viser at CSM-overvåking er tatt i bruk, og at det foreligger en prosedyre som dekker denne aktiviteten. Prosedyren må beskrive hvordan sikkerhetsresultatene måles og korrigeres gjennom styring av endringer og gjennom risikovurderingsprosessen, og hvordan feil i sikkerhetsstyringssystemet blir korrigert.

Virksomheten har prosesser og prosedyrer for systematisk å vurdere at ordningene for å inkludere menneskelige og organisatoriske faktorer er tilstrekkelige, og at de oppnådde resultatene er i samsvar med virksomhetens ytelsesstandarter.

Virksomheten har prosesser og prosedyrer for systematisk å vurdere yteevnen til ansatte med arbeidsoppgaver av sikkerhetsmessig betydning. Disse prosessene er basert på en tilnærming i forkant som fastsetter standarter for yteevne og systematisk evaluering. Det brukes dokumenterte metoder, for eksempel «crew resource management».

#### 6.1.6 Relevante tema for tilsyn

Vurder om overvåkingsprosessen og gjennomførte tiltak gjør sikkerhetsmyndighetene i stand til å fastslå om sikkerhetsstyringssystemet er «levende». Vurder også om erfaringer som virksomheten gjør seg, bedrer sikkerhetsstyringssystemet, eller om sikkerhetsstyringssystemet er «statisk» og forblir uendret over tid.

Sjekk at sikkerhetsstyringssystemet er i samsvar med CSM-overvåking ved å velge noen sentrale risikoforhold for å se om disse er hensiktsmessig styrt og at risikoforholdene er håndtert.

## 6.2 Internrevisjon

### 6.2.1 Lovbestemt krav

- 6.2.1. Virksomheten skal foreta internrevisjoner på en objektiv, upartisk og åpen måte for å samle inn og analysere informasjon til bruk i overvåkingen (se nr. 6.1 Overvåking), herunder
- (a) utarbeide en oversikt over planlagte internrevisjoner som kan endres avhengig av resultatene av tidligere revisjoner og overvåking av ytelsen.
  - (b) velge ut kvalifiserte revisorer (se nr. 4.2 Kompetanse).
  - (c) analysere og vurdere revisjonsresultatene.
  - (d) fastslå behovet for korrigerende tiltak eller forbedringstiltak.
  - (e) kontrollere om disse tiltakene er gjennomført og om de er effektive.
  - (f) dokumentere gjennomføringen og resultatene av revisjoner.
  - (g) formidle revisjonsresultatene til den øverste ledelsen.

### 6.2.2 Formål

Søker skal vise at det foreligger et internt revisjonssystem som involverer kompetent personell og genererer meningsfulle resultater, og som behandles av ledelsen og sikrer at sikkerhetsstyringssystemet fungerer i samsvar med lovfestede krav.

### 6.2.3 Forklarende merknader

Internrevisjoner (**6.2.1**) er overvåkingsverktøy i henhold til CSM-overvåking. Selv om det er et eget krav, er det ment å nå målene med overvåking i samsvar med CSM-overvåking.

Internrevisjonene (**6.2.1**) tar sikte på å innhente opplysninger om hvorvidt sikkerhetsstyringssystemet er i samsvar med gjeldende krav (**6.1.1 (c)**) og at det gjennomføres og vedlikeholdes hensiktsmessig (**6.1.1 (a), (b) og (d)**). Gjeldende krav refererer til kravene i vedlegg I og vedlegg II til CSM om samsvarsvurdering, og dermed til eventuelle andre gjeldende krav som virksomheten kan være underlagt (**se også 1.1**).

Revisor har ansvaret for å verifisere fullstendigheten og hensiktsmessigheten av korrigerende eller utbedrende tiltak (**6.2.1 (c)**) som skal utføres som et resultat av funnene fra revisjonen.

### 6.2.4 Dokumentasjon

- Dokumentasjon på at det foreligger en internrevisjonsprosess eller rammeverk som åpner for planlagte revisjoner og ytterligere målrettede revisjoner (**6.2.1 (a)**)
- Dokumentasjon på at det foreligger et system for styring av kompetanse som omfatter elementer som tar i betraktning kompetansen til dem som utfører internrevisjonen (**6.2.1 (b)**)
- Dokumentasjon på at det er iverksatt tiltak som følge av funn fra revisjoner både internt og eksternt (**6.2.1 (c), (d), (e), (f)**)
- Dokumentasjon på at resultatene fra revisjonene har blitt drøftet på toppledelsesnivå, og relevante tiltak iverksatt som et resultat av dette. (**6.2.1 (g)**)

### 6.2.5 Eksempler på dokumentasjon

Det må foreligge en internrevisjonsprosedyre for planlagte og supplerende revisjoner, inkludert drøfting av resultatene på toppledelsesnivå.

Eksempler på revisjonsrapporter og en oversikt over funnene fra internrevisjoner, som indikerer hvilke tiltak som er iverksatt for å håndtere dem.

Resultat fra revisjonsarbeid utført på tvers av virksomheten er samlet inn og analysert, og det har blitt gitt anbefalinger som skal brukes ved ledelsens gjennomgåelse.

Prosedyren har kompetansestyringssystemet (CMS) som referanse. CMS viser at revisorene har fulgt egnede revisorstandarder (for eksempel ISO).

### 6.2.6 Referanser og standarder

- *ISO 19011:2011 — retningslinjer for revisjon av sikkerhetsstyringssystemer*

### 6.2.7 Relevante tema for tilsyn

Ved gjennomføring av tilsyn er det avgjørende at resultatene fra revisjonene undersøkes. Dette vil avdekke om revisjonene retter seg mot de rette områdene, om resultatene virker fornuftige og om ansatte som utfører revisjonene er kompetente.

Sjekk at områdene som er valgt ut for revisjon står i forhold til virksomhetens risikoprofil.

Det må foreligge en mekanisme som utløser ekstraordinære revisjoner, og dette brukes ved å gjennomgå noen eksempler.

## 6.3 Ledelsens gjennomgåelse

### 6.3.1 Lovbestemt krav

- 6.3.1. Den øverste ledelsen skal med planlagte mellomrom vurdere om sikkerhetsstyringssystemet fortsatt er egnet og effektivt, og herunder minst ta hensyn til
- (a) informasjon om framdrift i gjennomføringen av gjenstående tiltak fra ledelsens tidligere gjennomgåelser,
  - (b) endrede interne og eksterne rammebetingelser (se nr. 1 Virksomhetens kontekst),
  - (c) virksomhetens sikkerhetsnivå i forbindelse med
    - i. ioppfyllelse av sikkerhetsmålene,
    - ii. resultatene av overvåkingsvirksomheten, herunder konklusjonene av internrevisjon, og interne undersøkelser av ulykker/hendelser samt status for tiltakene på de respektive områdene,
    - iii. de relevante resultatene av tilsynsvirksomheten som utføres av den nasjonale sikkerhetsmyndighet,
  - (d) anbefalinger om forbedringer.
- 6.3.2. På grunnlag av resultatene av ledelsens gjennomgåelse skal den øverste ledelsen påta seg det overordnede ansvaret for å planlegge og gjennomføre nødvendige endringer i sikkerhetsstyringssystemet.

### 6.3.2 Formål

Sterkt søkelys på sikkerheten fra ledelsen er avgjørende for et fungerende og hensiktsmessig sikkerhetsstyringssystem i en virksomhet, samt for virksomhetens kontinuerlige utvikling over tid. Virksomheten skal vise at ledelsen er aktivt involvert i å vurdere sikkerhetsstyringssystemets ytelse, samt utvikle det for fremtiden.

### 6.3.3 Dokumentasjon

- *Prosesser for ledermøter som dekker gjennomgang av sikkerhetsstyringssystemet og fremdriften i interne anbefalinger som følge av revisjon og gjennomgang (6.3.1 (a)-(d))*
- *Historikk over hvordan virksomheten har hatt fremdrift mot sine sikkerhetsmål (6.3.1(c),(i))*
- *Dokumentasjon på at anbefalinger fra relevante nasjonale sikkerhetsmyndigheter er tatt hensyn til i sikkerhetsstyringssystemet (6.3.1 (c),(iii))*
- *Virksomheten må kunne vise at det foreligger prosesser for å fastslå og fastsette mål i samsvar med type, omfang og relevante risikoer, regelmessig vurdere fremdriften mot mål, etterleve prosedyrer og anvende sikkerhetsinformasjon for å overvåke, gjennomgå og gjennomføre endringer i driftsordninger. (6.3.1)*
- *Dokumentasjon på at ledelsen påtar seg en aktiv rolle i planleggingen og gjennomføringen av nødvendige endringer i sikkerhetsstyringssystemet (6.3.2)*

*Det er prosesser og verktøy for å ha systematisk rapportering av alle typer av identifisert risiko, feil, nestenulykker, mangler og hendelser. I tillegg er det prosesser og verktøy i virksomheten som gjør*

*det mulig å kategorisere og analysere hva som rapporteres sett fra menneskelig og organisatorisk perspektiv for å kunne finne underliggende årsaker og hensiktsmessige tiltak.*

*Ekspertise innen menneskelige og organisatoriske faktorer er brukt i granskning av ulykker. Det er systematiske prosesser for læringssløyfer om utfordringer knyttet til menneskelige og organisatoriske faktorer, og disse vil være innspill til øvelse og design.*

Erfaringer fra ulykker og ulykkesgranskning er kommunisert til ansatte i virksomheten, og er tatt med i opplæring, design og andre områder for å redusere sannsynlighet for at ulykken inntreffer igjen.

Resultater fra ulykkesundersøkelser er rapportert i ledelsesmøter, og vurdert til å være verktøy for læring og forbedring.

Det er fastsatt en prosess for kvalitetssikring av granskning av ulykker.

#### 6.3.4 Eksempler på dokumentasjon

Prosedyre som dekker gjennomgang og fremdrift for interne anbefalinger som følge av revisjoner og vurderinger gjennomført av toppledelsen, samt møtereferater fra utvalgte møter.

En oversikt over utestående forhold/problemstillinger som må inneholde anbefalinger som er gitt, samt fremdriften i å korrigere feil, og som er fulgt opp av ledelsen.

Prosedyren for ledelsens vurdering av resultatene fra intern ulykkesgranskning og relevante resultater fra tilsyn fra nasjonale sikkerhetsmyndigheter.

Informasjonen er supplert med hvilke indikatorer som skal følges opp av toppledelsen, og hvilken frekvens oppfølgingen skal ha.

#### 6.3.5 Relevante tema for tilsyn

Under tilsynet er det viktig å observere at prosessen for å sikre at ledelsen gjennomgår hensiktsmessigheten av sikkerhetsstyringssystemet, resulterer i reelle endringer på driftsnivå.

Ledelsens bevissthet om endringer i interne og eksterne forhold. Sjekk om ledelsen gjennomfører kartlegging med tanke på fremtiden/PESTLE-analyse (politisk, økonomisk, sosialt og teknologisk, juridisk og miljømessig) for å få oversikten over utviklingen av sikkerhetsstyringssystemet.

Koblingen mellom resultatene fra ledelsens gjennomgåelse og hvordan resultatene fra disse er innspill til årlig sikkerhetsrapport.

## 7 Forbedring

### 7.1 Erfaringer fra ulykker og hendelser

#### 7.1.1 Lovbestemt krav

- 7.1.1. Ulykker og hendelser i forbindelse med virksomhetens jernbanedrift skal
- (a) rapporteres, registreres, undersøkes og analyseres for å fastslå årsakene,
  - (b) rapporteres til nasjonale organer når det er relevant.
- 7.1.2. Virksomheten skal sikre at
- (a) anbefalinger fra den nasjonale sikkerhetsmyndigheten, det nasjonale undersøkelsesorganet og undersøkelser foretatt av bransjen eller internt evalueres og gjennomføres dersom det er hensiktsmessig eller fastsatt,
  - (b) relevante rapporter/informasjon fra andre berørte parter, for eksempel infrastrukturforvaltere, enhet med ansvar for vedlikehold og innehavere av jernbanekjøretøy, vurderes og tas hensyn til
- 7.1.3. Virksomheten skal bruke informasjon fra undersøkelsen til å gjennomgå risikovurderingen (se nr. 3.1.1 Risikovurdering), for å benytte erfaringene til å bedre sikkerheten og eventuelt vedta korrigerende tiltak og/eller forbedringstiltak (se nr. 5.4 Endringsstyring).

#### 7.1.2 Formål

Virksomheten må vise at ulykker og hendelser granskes, for å ta lærdom av dem og forbedre risikostyring, at ansatte som har denne oppgaven er kompetent til å foreta granskning, blant annet av mennesker og organisatoriske faktorer, at ulykker rapporteres til relevante myndigheter, og at ledelsen iverksetter tiltak på grunnlag av anbefalinger og rapporter.

Analysen av uønskede hendelser bør ikke være en «heksejakt» eller ha som mål å avdekke en avdeling som er «mer ansvarlig enn en annen», men heller være en hjelp til forståelse og åpne for å bedre organisatoriske svakheter som førte til at hendelsen fant sted. Den viktigste utfordringen når man analyserer uønskede hendelser er å forhindre også «nærliggende» hendelser. Hvis analysen ender med å identifisere de umiddelbare årsakene, vil det bare være mulig å forhindre neste lignende hendelse. Hvis analysen på den annen side gjør det mulig å identifisere tekniske og organisatoriske hovedårsaker, vil tiltak for forbedring åpne for å kunne forebygge andre typer ulykker som deler de samme mekanismene. Hvis for eksempel analysen gjør det klart at en prosedyre ikke har blitt oppdatert, og at korrigerende tiltak bare har som mål å korrigere denne prosedyren, vil effekten være begrenset. Hvis analysen går dypere inn i materien og identifiserer svakheter i prosessen for oppdateringsprosedyrer, vil den positive effekten fra tiltak for forbedring være mye bredere.

I tillegg bør virksomheten anvende «double-loop-læring»: Lærdommen skal ikke bare være konsentrert om realiteten i uønskede hendelser, men også virksomhetens evne til å forbedre seg, ved å fokusere på elementer som enten fremmer eller hemmer formidlingen av kunnskap og informasjon på tvers av virksomheten.

Rapportere farlige situasjoner og hendelser med stort potensial er satt pris på, og terskelen for å rapportere disse er lave. Hvis det er nødvendig, finnes mekanismer som gjør at rapporteringene kan være anonyme. Hvis rapporteringen ikke er anonym, kan personellet og grupper som har sendt rapportene assistere med analyser og finne kortsiktige løsninger. Diskusjoner i grupper er organisert, og iverksatte tiltak kommuniseres til relevant personell og til virksomheten.

Det brukes ulik kompetanse og synspunkter fra alle relevante parter (inkludert nødvendige eksterne parter) i analyser av farlige hendelser.

«Just culture» er fremmet, gjenkjent og styrket i positive sikkerhetsinitiativ (rapportering av hendelser, involvering av personellet i analyser og kontinuerlig forbedring, støtte kollegaer osv.) Denne «just culture» bør fjerne frykt og skyldspørsmål, ved å definere hva som er akseptabel og ikke akseptabel grense. Det er lov å gjøre feil.

### 7.1.3 Forklarende merknader

Det er like viktig å granske nestenulykker og andre farlige hendelser for å være i forkant i å ivareta sikkerheten.

Erfaringer fra ulykker og uønskede hendelser bør utveksles med andre interessenter (infrastrukturforvalter, andre jernbanevirksomheter, ECM-er, for å utvikle samarbeidet og fremme den generelle forbedringen av sikkerhetsstyringssystemet).

For granskning som må ses fra et perspektiv med menneskelige og organisatoriske faktorer, må granskningspersonellet enten være opplært eller ha tilgang til egnet ekspertise for å undersøke problemene.

### 7.1.4 Dokumentasjon

- *Informasjon om rapportprosess for ulykker/uønskede hendelser, herunder hvordan hovedårsaken identifiseres og analyseres, inkludert rapportering innenfor virksomheten og til andre kompetente myndigheter og andre parter (7.1.1)*
- *Informasjon om fremgangsmåten virksomheten følger i forbindelse med granskning, inkludert menneskelige og organisatoriske faktorer, for å gjennomgå risikoanalysen og evalueringsprosessen etter en uønsket hendelse (7.1.3)*
- *Dokumentasjon på at anbefalinger fra kompetente myndigheter har blitt fulgt opp som følge av rapporter for ulykker og uønskede hendelser, og eventuelle nødvendige identifiserte endringer har blitt gjennomført (7.1.2 (a), (b))*
- *Gjennomgang av tidligere uønskede hendelser for å identifisere relevante faktorer ved en hendelse. Dokumentasjon på bredere organisatorisk lærdom fra uønskede hendelser og erfaringer, nasjonalt og internasjonalt. (7.1.3)*
- *Det er kjente metoder for granskninger som er basert på kunnskap om menneskelige og organisatoriske faktorer*
- *De som utfører granskninger av ulykker og hendelser har treningsprogram som er sett fra menneskelig og organisatorisk perspektiv.*

### 7.1.5 Eksempler på dokumentasjon

Prosedyren for ulykkesgranskning som beskriver granskningsmetodene, med referanse til kompetansestyringskrav til dem som gransker ulykker og uønskede hendelser.

Et utdrag fra rapporter for ulykker og uønskede hendelser av ulike typer, som viser at granskning har blitt utført av kompetent personell, og funn basert på dokumentasjon og anbefalinger er fulgt opp.

En kopi av prosedyren/prosessen som sporer korrigerende/forebyggende tiltak som er fastsatt etter en ulykke/uønsket hendelse.

Informasjon er lagt inn i SAIT for å holde oversikt over, og for å kunne gi råd til andre virksomheter om forhold som påvirker spesielle eiendeler.

Et team med opplært granskningspersonell er tilgjengelig.

Det foreligger opplæringsprogram for dem som gransker uønskede hendelser og ulykker.

Møtereferater fra styremøter som viser at resultatene fra granskning av ulykker/uønskede hendelser og korresponderende anbefalinger (dvs. korrigerende og/eller forbedrende tiltak) rapporteres tilbake til ledelsen, og hvordan de håndterer gjennomgang av sikkerhetsstyringssystemet (**se også 6.3**).

Menneskelige og organisatoriske faktorer er tatt i betraktning i granskningen av ulykker og uønskede hendelser. Granskningen har et systematisk perspektiv, det vil si ikke bare å se på de menneskelige, teknologiske og organisatoriske faktorene i seg selv, men også fokusering på samspillet mellom faktorene. Hvis for eksempel en lokomotivfører har vært involvert i en passhendelse, omfatter de foreslåtte granskningspunktene relevante problemer, for eksempel tretthet, kognitiv overbelastning, kompetanse, etc. (menneskelig), teknologisk innvirkning på yteevnen, som for eksempel grensesnitt mellom menneske og system, layout, signalplassering (teknologi), virksomhetens innflytelse på yteevnen, som opplæring, sikkerhetsstyringssystem, virksomhetsprioriteringer (virksomhet) og samspillet mellom de tre områdene som innflytelse på anskaffelser med hensyn til design eller endringsstyring med innføring av nytt design.

#### 7.1.6 Referanser og standarder

- IAEA (2002) — *Sikkerhetskultur på kjernekraftanlegg: Veiledning for anvendelse i forbedring av sikkerhetskulturen*. IAEA TECDOC-1529. Internasjonalt atomenergibyrå, Wien (2002).
- Mathis, T.L. & Galloway, S.M. (2013) — *Skrift for en god sikkerhetskultur*.
- Kecklund, L., Lavin, M. & Lindvall, J. (2016) — *Sikkerhetskultur: Et krav til nye forretningsmodeller. Lærdommer fra andre høyriskobransjer. I framgang presentert av Den internasjonale konferansen om menneskelige og organisatoriske aspekter ved sikring av atomenergisikkerhet — gjennomgang av 30 års sikkerhetskultur, Wien 22. til 26. februar 2016*
- RSSB (2015) — *Sikkerhetskultur og atferdsutvikling: Felles faktorer for å skape en kultur med kontinuerlig utvikling* ([www.sparkrail.org](http://www.sparkrail.org))

#### 7.1.7 Relevante tema for tilsyn

Kompetansen til dem som gransker ulykker/uønskede hendelser er kritisk, for å kunne komme med meningsfulle anbefalinger og få på plass egnede forebyggende tiltak. De som utfører tilsyn, bør be om innblanding fra ledelsens side om utfallet av rapporter for ulykker og uønskede hendelser, som kan påvirke kvaliteten på rapporten og utfall som kan utledes fra den.

Resultatene fra en intern granskning har ført til organisatorisk lærdom, som kan spores i dokumenter, rapporter eller andre informasjonskanaler (for eksempel intranett, interne bedriftsblader, etc.)

Kultur knyttet til rapportering om uønskede hendelser.

## 7.2 Kontinuerlig forbedring

### 7.2.1 Lovbestemt krav

- 7.2.1. Virksomheten skal kontinuerlig forbedre sikkerhetsstyringssystemets egnethet og effektivitet, idet det tas hensyn til rammen som er fastsatt i forordning (EU) nr. 1078/2012, og minst resultatene av følgende virksomhet:
- (a) Overvåking (se nr. 6.1 Overvåking).
  - (b) Internrevisjon (se nr. 6.2 Internrevisjon).
  - (c) Ledelsens gjennomgåelse (se nr. 6.3 Ledelsens gjennomgåelse).
  - (d) Erfaringer fra ulykker og hendelser (se nr. 7.1 Erfaringer fra ulykker og hendelser).
- 7.2.2. Virksomheten skal ha midler til å motivere personalet og andre berørte parter til aktivt å forbedre sikkerheten som en del av læringen i virksomheten.
- 7.2.3. Virksomheten skal ha en strategi for kontinuerlig å forbedre sikkerhetskulturen basert på fagkunnskap og anerkjente metoder for å fastslå atferdsrelaterte problemstillinger som påvirker ulike deler av sikkerhetsstyringssystemet, og for å iverksette tiltak for å håndtere disse.

### 7.2.2 Formål

Kontinuerlig forbedring spiller en viktig rolle i et hensiktsmessig sikkerhetsstyringssystem. Formålet med dette kravet er å få søker til å være villig til å gjøre forbedringer, og at sikkerhetsstyringssystemet støtter dette.

Ledelsen viser at det er felles ansvar for kontinuerlig forbedring av sikkerhetskultur og virksomhet.

Felles ansvar vises gjennom en strategi som anerkjenner at kulturelle trekk påvirker sikkerhetsytelsen og at kulturelle trekk derfor bør verdsettes høyere. Kulturelle trekk i en virksomhet kan være gjenstand for endring for å bedre sikkerhetskulturen.

### 7.2.3 Forklarende merknader

Kontinuerlig forbedring (**7.2.1**) fokuserer på elementene i sikkerhetsstyringssystemet som evaluerer og fører til forbedrende tiltak, men ikke på elementene som er gjenstand for forbedring, siden de allerede er en del av overvåkingsaktivitetene.

Virksomhetslæring (**7.2.2**) viser til prosessen med forbedrende tiltak gjennom bedre kunnskap og forståelse.

Sikkerhetskultur (**7.2.3**) er definert i 2.1.1 (j) og korresponderende merknad. En positiv sikkerhetskultur motiverer til og gjør det mulig for virksomheter og enkeltpersoner å bestrebe seg på å forbedre sikkerheten og ytelsen. Den øker jobbtilfredsheten, gjør at virksomheten holder på medarbeiderne sine og åpner for å spare kostnader. Den kan også bidra til å møte lovfestede forventninger, da sikkerhetsmyndigheter og tilsynsmyndigheter i økende grad anerkjenner rollen sikkerhetskulturen spiller i hensiktsmessig sikkerhetsstyring. Nærmere bestemt kan en positiv sikkerhetskultur føre til:

- *reduerte risikoer i driften gjennom en mer omfattende risikovurdering og forbedret forståelse av risiko*
- *reduksjon av personskader ved å eliminere farer som er identifisert gjennom økt rapportering om nestenulykker*

- *reduksjon av usikre handlinger og forhold gjennom forbedret engasjement i arbeidsstyrken og i lederutvikling*
- *reduksjon i kostnader knyttet til personskader, usikre handlinger og forhold*
- *forbedret yteevne gjennom økt personelloppplæring, engasjement, samt reduksjon i personskader, usikre handlinger og forhold*
- *forbedret og mer hensiktsmessig sikkerhetsstyringssystem med prosedyrer og regler som samsvarer med daglig drift*

På grunn av ulike kulturer som skapes gjennom daglig drift og som er vanskelig å endre, skal en strategi være langsiktig, forankret og fremmet av ledelsen.

Det er mange måter å forbedre sikkerhetskultur på, som for eksempel:

- *Å utvikle et system for å dele bekymringer. Dette er avhengig av modenheten til virksomheten. I et system for å dele bekymringer anonymt i starten og etter hvert som virksomheten utvikler seg, kan deling av bekymringer foregå åpent og tilgjengelig for alle. Det er viktig at tilbakemeldinger er en del av systemet for å sikre at personellet føler seg involvert og har en tilhørighet.*
- *Anskaffelser og kontraktsvilkår som oppmuntrer til god sikkerhetskultur for leverandører. Sikkerhetskultur kan være et kriterium for valg av leverandører.*
- *Synlig anerkjennelse for sikker atferd. Anerkjennelsen kan være alt fra å øke årslønnen gjennom bonus til ukentlig anerkjennelse for prestasjoner utover det vanlige.*
- *Skape spesifikke mål for sikkerhetsledere, for eksempel å oppmuntre ledelsen til å ha en mer synlig rolle, sette sikkerhetsstandarden ved å være gode rollemodeller.*

Man kan bruke ulike metoder for å vurdere sikkerhetskultur. Innsamling av data bør være basert på samfunnsvitenskapelige metoder. Det betyr at når man samler inn slike data skal det benyttes metoder som observasjon, dokumentanalyse og intervjuer.

Resultatene av vurderingene bør kommuniseres til alle nivåer i virksomheten. Resultatene bør brukes til å opprettholde og fremme positiv sikkerhetskultur, forbedre sikkerhetsledelse og til å fremme læring i virksomheten.

Identifisering og utvelgelse av relevante kulturelle trekk er en kompleks<sup>3</sup> oppgave og må vies stor oppmerksomhet fordi det har stor betydning for resultatet av vurderingene av sikkerhetskultur.

Denne oppgaven bør involvere personellet på alle nivåer i virksomheten, og ofte også involvere leverandører.

En spørreundersøkelse der personellet gir uttrykk for sine meninger og oppfatninger av sikkerhetskultur ansees generelt for å ikke være tilstrekkelig for å kunne si noe om kulturelle trekk som påvirker sikkerheten. I tillegg til en spørreundersøkelse, bør eksperter gjennomføre observasjoner, individuelle intervjuer og etablere fokusgrupper, for å kunne si noe om de kulturelle trekkene som påvirker sikkerheten i en virksomhet.

NB: En fokusgruppe samler en gruppe, vanligvis mellom 4 til 15 personer. Denne gruppen ledes av en moderator og fokuserer på et spesifikt tema. Hensikten er at gruppen skal diskutere sammen istedenfor å svare individuelt på formelle spørsmål. I tillegg skal gruppen produsere kvalitative data.

---

<sup>3</sup> Ulike aktiviteter og størrelse på virksomheten er noen eksempler på komplekse oppgaver

The NSA NO 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.

Basert på resultatene av vurderingen av sikkerhetskulturen, kan en handlingsplan bidra til endring av kulturelle trekk som defineres og støttes av ledelsen. Ledelsen overvåker implementering av tiltakene i handlingsplanen og reviderer den ved behov.

Vurderingene bør revideres hvert 2. til 5. år med samme tilnærming for å ha verdi for virksomheten. Frekvensen er avhengig av resultatene fra første vurdering av sikkerhetskulturen.

I flere høyrisikoindustrier foretas det en vurdering av sikkerhetskultur, og det blir utarbeidet en tilhørende handlingsplan (se figur 2: Vurdering av sikkerhetskultur).

Vurdering av sikkerhetskultur kan utføres uavhengig eller ved en egenvurdering. Fordelen med å bruke uavhengig vurdering er at virksomheten gis et mer objektivt bilde av sikkerhetskulturen, men det er også en risiko for at virksomheten kan bli misforstått, eller at virksomheten kan ha problemer med å akseptere konklusjonene. Fordelen med en egenvurdering er at den blir gjennomført med virksomhetens eget personell som har innsikt i egen virksomhet. Ulempen er at status og hierarki kan påvirke beslutningene. Noen kjennetegn på vurdering av sikkerhetskultur:

- 2 til 3 ukers vurderingsprosess i tillegg til en forberedende del
- Involvere personellet med tverrfaglig kompetanse
- Datainnsamling er basert på samfunnsvitenskapelige metoder (inkludert intervjuer, fokusgrupper, observasjoner)
- Vurderer hele virksomheten og dens grensesnitt
- Basert på en sikkerhetskulturmodell eller etter rammeverk
- Ledelsen er engasjert og betrakter vurderingen som mulighet for læring
- Resultatene er utbredt i virksomheten
- Resultatene gir bidrag til å designe/revidere en strategi for kontinuerlig å forbedre de valgte trekkene i virksomhetens sikkerhetskultur

Figur 2: Vurdering av sikkerhetskultur

Forbedring av strategi for menneskelige og organisatoriske faktorer er en integrert del av kontinuerlig forbedring av sikkerhetsstyringssystem.

En systematisk tilnærming er definert av en steg for steg-prosess for å håndtere utfordringer knyttet til sikkerhetskultur. For eksempel å ha en prosess for observasjon av risiko, hendelses- og ulykkesrapportering og hvordan informasjonen er brukt. I tillegg til hvordan erfaringer kan bidra til kontinuerlig forbedring.

Se vedlegg 4 for mer informasjon om sikkerhetskultur.

#### 7.2.4 Dokumentasjon

- Informasjon om prosessen for å samle inn dokumentasjon for å vise til kontinuerlig forbedring av sikkerhetsstyringssystemet **(7.2.1)**
- Prosedyrer som beskriver hvordan virksomheten følger opp resultatene fra overvåking, internrevisjon, ledelsens gjennomgang og lærdom fra ulykker og uønskede hendelser, for å forbedre sikkerhetsstyringssystemet **(7.2.1)**
- Informasjon om hvordan virksomheten søker å engasjere medarbeidere og andre i å forbedre sikkerhetsstyringssystemet **(7.2.2)**

- Søker må beskrive i strategien om hvordan sikkerhetskulturen kontrolleres, slik at risikoer som er forbundet med manglende kontroll av kulturen tas i betraktning i de relevante prosessene i sikkerhetsstyringssystemet. Søkeren bør vise til hvor ytterligere informasjon om de relevante prosedyrene kan bli funnet. **(7.2.3)**
- Sikkerhetskulturen vurderes kontinuerlig for å identifisere behov for forbedringer **(7.2.3)**.

Forbedringer i sikkerhetskultur bruker PDCA for å sikre at tiltak er hensiktsmessige. Man tar hensyn til erfaringer, og man evaluerer systematisk hvilke påvirkninger de har på sikkerhetskulturen **(7.2.3)**.

#### 7.2.5 Eksempler på dokumentasjon

Prosedyren som dekker overvåking, internrevisjon, ledelsens gjennomgang og granskning av ulykker og uønskede hendelser, spesifikt det som omhandler lærdommen som bør være tatt for sikkerhetsstyringssystemet.

«Nestenulykker»-initiativet i Network Rail ([www.safety.networkrail.co.uk/alerts-and-campaign/close-call](http://www.safety.networkrail.co.uk/alerts-and-campaign/close-call)), hvor medarbeiderne oppfordres til å være aktive i å varsle virksomheten om svakheter/hull i systemet eller situasjoner der det foreligger risikoer for helse og sikkerhet.

Eksempler på møtetreferater fra periodiske fagforeningsmøter/HMS-møter, som viser hvor situasjoner som er ansett som usikre/utrygge eller krever videre vurdering, har blitt diskutert.

Resultatene fra ulykkesgranskning rapporteres på ledermøter og betraktes som et viktig verktøy for å ta lærdom og forbedre seg.

En kopi av strategien for å forbedre sikkerhetskulturen, og hvordan dette knytter seg til de ulike delene i sikkerhetsstyringssystemet.

Strategien må vise til tilstrekkelig dokumentasjon på at det foreligger faglig kompetanse og nødvendig opplæring og erfaring, på feltet der sikkerhetskulturen skal ta sikte på å utføre og utvikle strategien.

Type opplæring og kompetanse som kreves er knyttet til forståelse av begrepet sikkerhetskultur, og måter og metoder for å måle ytelsen og jobbe mot kontinuerlig forbedring. Et ytterst viktig aspekt er at det er forståelse for sikkerhetskulturen som et helhetlig konsept som påvirker alle deler av sikkerhetsstyringssystemet, og at sikkerhetskulturen ikke kan behandles som et separat element.

Det foreligger en prosess som kontinuerlig evaluerer alle sikkerhetstiltak. Ønsket effekt av sikkerhetstiltak er spesifisert, og sikkerhetstiltak er implementert på en måte som gjør det mulig å evaluere dem.

#### 7.2.6 Relevante tema for tilsyn

Ved tilsyn bør ledelsens engasjement i kontinuerlig forbedring av sikkerhetsstyringssystemet bli testet gjennom samtaler, samt gjennom en dokumentasjonsanalyse. Gjøres det en risikobasert tilnærming til å målrette forbedring, dvs. i tilknytning til sårbare og kritiske kontroller?

Virksomhetenes bruk av modenhetsmodeller for å undersøke ytelsen av et sikkerhetsstyringssystem, bør undersøkes der dette foreligger.

## Vedlegg 1 — Lovspeil

Tabellene nedenfor viser en kolonnebasert sammenligning mellom vurderingskravene som er skissert i vedlegg II til tidligere forordning (EU) 1158/2010 og (EU) 1169/2010, og kravene i vedlegg I og vedlegg II til kommisjonens delegerte forordning (EU) 2018/762 [*Forskrift om felles sikkerhetsmetode for sikkerhetsstyringssystemer (CSM SMS)*]. Formålet er å legge til rette for overgangen fra det gamle sikkerhetsertifiseringsregimet i henhold til direktiv 2004/49/EF til det nye, som ble innført av direktiv (EU) 2016/798.

Samsvar med kommisjonens delegerte forordning (EU) 2018/762 [*CSM SMS*] gir ikke dokumentasjon for jernbanevirksomheters evne til å oppfylle de relevante kravene i sikkerhetsstyringssystemet i samsvar med artikkel 9 i direktiv (EU) 2016/798. Detaljene i de tidligere og nye vurderingskravene kan fortsatt variere, selv om de til en viss grad deler felles prinsipper. I tillegg korresponderer ikke alle vurderingskravene i vedlegg I og vedlegg II til kommisjonens delegerte forordning (EU) 2018/762 [*CSM SMS*] med den tidligere forordningen. Det kreves videre at jernbanevirksomhete viser at de etterlever de nye vurderingskravene (eller deler av dem).

Kravene til sikkerhetsstyringssystemet ifølge kommisjonens delegerte forordning (EU) 2018/762 [*CSM SMS*] som ikke korresponderer med dem i forordning (EU) 1158/2010 og/eller forordning (EU) 1169/2010, skal betraktes som nye krav, og i den forbindelse skal søker fremlegge ytterligere dokumentasjon som viser samsvar med dem. I de fleste tilfeller er det ikke mulig å oppnå et fullstendig samsvar mellom kriteriene i den tidligere forordningen og kravene i den nye CSM-forordningen. I slike tilfeller er sammenligningen således basert på hensikten med kravene. Det kan også hende at kravene er gjort tydeligere i kommisjonens delegerte forordning (EU) 2018/762 [*CSM SMS*] mens de har den samme hensikten. I slike tilfeller skal kravene i forordningen ikke betraktes som nye, men kan anvendes av de ulike partene som en hjelp til å forstå hvilke dokumentasjon som kan forventes at søkeren legger frem.

Korrespondanse med ISO High Level Structure (HLS)<sup>4</sup> er også gitt til jernbanevirksomheter som villige til å utvikle et integrert styringssystem. Likeledes inneholder ikke et styringssystem som er sertifisert mot én eller flere ISO-styringssystemstandarder (for eksempel ISO 9001, ISO 14001 eller ISO 45001) dokumentasjon for jernbanevirksomheters evne til å oppfylle de relevante sikkerhetsstyringssystemkravene i samsvar med artikkel 9 i direktiv (EU) 2016/798.

*Tabell 1: Kolonnebasert sammenligning — vurderingskriterier/krav som er felles for jernbanevirksomhetene*

<i>Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>ISO HLS paragraf nr.</i>	<i>Kommentar</i>
A.1	3.1.1.1	6.1	
A.2	3.1.1.1	6.1	
A.3	6.1.1	9.1	
A.4	3.1.1.1 (e)	N/A	
A.5	4.4 4.5.1.1	7.4	

<sup>4</sup> ISO/IEC-direktiver, del 1, konsolidert tillegg 2016, vedlegg SL vedlegg 2.

<i>Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>ISO HLS paragraf nr.</i>	<i>Kommentar</i>
A.6	6.1.1 5.4.1	9.1 8.1	
B.1	5.2.4	N/A	Vedlikehold er en fase i løpet av levetiden til en eiendel.
B.2	5.2.4	N/A	Vedlikehold er en fase i løpet av levetiden til en eiendel.
B.3	2.3.1 4.2.1	5.3 7.2	Definisjon og tilordning av ansvar for vedlikehold finnes i stor grad i 2.3.1. Beskrivelse av kompetansen som kreves for vedlikehold finnes i stor grad i 4.2.1.
B.4	6.1.1 5.2.5	9.1 7.4	Datainnsamling (funksjonsfeil, svikt) og analyse er en del av overvåkingsprosessen. Utveksling av data mellom de som er ansvarlige for den daglige driften og de som er ansvarlige for vedlikeholdet, er en del av informasjons- og kommunikasjonsprosessen som anvendes ved virksomhetens forvaltning av eiendeler.
B.5	6.1.1	N/A	Referert til i artikkel 4(2) i CSM om overvåking.
B.6	6.1.1	9.1	Evaluerings av ytelse og resultater fra vedlikehold er en del av overvåkingsprosessen som anvendes for vedlikehold.
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)	N/A	
C.4	5.2.5 (b) 5.3.2 (c)	N/A	
C.5	5.3.2 (c) 5.3.3 (a)	N/A	
D.1	3.1.1.1 (a)	N/A	
D.2	3.1.1.1 (c)	N/A	
D.3	6.1.1	N/A	
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	

The NSA NO 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>Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>ISO HLS paragraf nr.</i>	<i>Kommentar</i>
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	N/A	
F.4	4.5.1.1 (a) 4.2.1 2.3.1 2.3.2 2.3.3	4.4 5.3	Definisjon av sikkerhetsrelaterte oppgaver er en del av beskrivelsen i sikkerhetsstyringssystemet, herunder ansvarsfordeling. Ansvar er definert for hver enkelt relevant rolle i sikkerhetsstyringssystemet.
G.1	4.5.1.1 (a) 2.3.1	4.4 5.3	Definisjon av sikkerhetsrelaterte oppgaver er en del av beskrivelsen i sikkerhetsstyringssystemet, herunder ansvarsfordeling. Ansvar er definert for hver enkelt relevant rolle i sikkerhetsstyringssystemet.
G.2	6.1.1 6.2.1	9.1 9.2	Internrevisjon tar sikte på å sjekke at virksomheten overholder gjeldende krav.
G.3	2.1.1 (h) 2.3.2	N/A	
G.4	2.3.1	5.3	
G.5	4.1.1	7.1	Merk at det er en link her til kravet N2 (d) i 1158/2010
H.1	2.4.1	N/A	
H.2	(fjernet)	N/A	Personell som utfører sikkerhetsrelaterte oppgaver, bør være involvert i å utvikle, vedlikeholde og forbedre sikkerhetsstyringssystemet. Det er opp til virksomheten å implementere krav. 2.4.1 på en slik måte at etterlevelsen av det er sporbar.
I	7.2.1	10.1 10.2	
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	Sikkerhetsmålene må være i samsvar med sikkerhetspolitikken, som videre bør være egnet for typen og omfanget til jernbanevirksomheten.
K.3	3.2.4	6.2	Sikkerhetsmål er ikke begrenset til felles sikkerhetsmål som er fastsatt på medlemsstatsnivå.
K.4	6.1.1 5.4	9.1 8.1	

The NSA NO 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>Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>ISO HLS paragraf nr.</i>	<i>Kommentar</i>
K.5	3.2.4 (tilpasset)	9.1	Referanse til overvåkingsstrategi og plan(er) samsvarer med CSM om overvåking.
L.1	6.1.1 5.4	9.1 8.1	
L.2	4.2 4.4 4.5 5.2.2 (a)	N/A	Bruk av kompetent personell, prosedyrer, spesifikke dokumenter og rullende materiell, er kontrollert under kompetanse, informasjon og kommunikasjon og dokumentert informasjon og forvaltning av eiendeler.
L.3	1.1.1 (e) 6.1.1 6.1.2	4.3 9.2	Etterlevelse av gjeldende krav er for det meste framsatt i 3.1.2.2 (ikke spesifikt for vedlikehold). Overvåking sikrer korrekt anvendelse av prosedyrene. Internrevisjon sikrer at prosedyrene samsvarer med de gjeldende kravene.
M.1	3.1.2.1 5.4.1	6.1 8.1	I samsvar med ISO skal endringer først planlegges, inkludert risikoidentifikasjon og vurdering, og deretter kan endringen gjennomføres.
M.2	3.1.2.1	N/A	
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	N/A	
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	N/A	
P.1	4.4.3	N/A	
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	N/A	
Q.3	7.1.3	10.2	

The NSA NO 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>Forordning (EU) 1158/2010 og 1169/2010 Kriterium-ID</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>ISO HLS paragraf nr.</i>	<i>Kommentar</i>
R.1	5.5.1	N/A	
R.2	5.5.2	N/A	
R.3	5.5.3	N/A	
R.4	5.5.4	N/A	
R.5	5.5.5	N/A	
R.6	5.5.1	N/A	
R.7	5.5.6	N/A	
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) til (f)	9.2	
S.5	6.2.1 (g) 6.3.1	9.3	
S.6	6.2.1	9.2	

Tabellen nedenfor inneholder en kolonnebasert sammenligning mellom tidligere vurderingskriterier og de nye sikkerhetsstyringssystemkravene som kun gjelder for jernbaneforetak.

*Tabell 2: Kolonnebasert sammenligning — spesifikke vurderingskriterier/krav for jernbaneforetak*

<i>Forordning (EU) 1169/2010 Kriterium-ID</i>	<i>Forordning (EU) 2018/762. Vedlegg I Krav-ID</i>	<i>ISO HLS paragraf nr.</i>	<i>Kommentar</i>
R.8	5.5.7	N/A	
R.9	5.5.8	N/A	

Tabellen nedenfor inneholder en kolonnebasert sammenligning mellom tidligere vurderingskriterier og de nye sikkerhetsstyringssystemkravene som kun gjelder for infrastrukturforvaltere.

*Tabell 3: Kolonnebasert sammenligning — spesifikke vurderingskriterier/krav for infrastrukturforvaltere*

<i>Forordning (EU) 1169/2010 Kriterium-ID</i>	<i>Forordning (EU) 2018/762 Vedlegg II Krav-ID</i>	<i>ISO HLS paragraf nr.</i>	<i>Kommentar</i>
R.8	5.5.7	N/A	
R.9	5.5.8	N/A	
T.1	5.2.1	N/A	Sikkert design og installasjon av infrastrukturen er en del av levetiden til en eiendel.
T.2	3.1.2 5.4.1	N/A	Beskrivelse av tekniske endringer i infrastrukturen finnes i stor grad i 3.1.2. Håndtering av tekniske endringer i infrastrukturen finnes i stor grad i 5.4.1.
T.3	3.1.2	N/A	Etterlevelse av gjeldende regler som omhandler designet på infrastrukturen finnes i stor grad i 3.1.2.
U.1	5.1.1 5.1.3	N/A	Sikkerhetsstyring av infrastrukturen finnes i stor grad i 5.1.1.
U.2	5.1.1	N/A	Sikkerhetsstyring for fysiske grenser og/eller driftsgrenser i infrastrukturen finnes i stor grad i 5.1.1.
U.3	5.1.3 (c) 5.5.7	N/A	Håndtering av normal og nedsatt drift finnes i stor grad i 5.1.3 (c).
U.4	5.1.2 5.2.3	N/A	
V.1	5.2.4 6.1.1	N/A	Vedlikehold av infrastrukturen finnes i stor grad i 5.2.4. Revisjoner og inspeksjoner (der det er relevant) inngår i overvåkingsaktivitetene.
V.2	5.2.4	N/A	Vedlikehold av infrastrukturen finnes i stor grad i 5.2.4.
V.3	5.2.3	N/A	
W.1	5.1.3	N/A	
W.2	5.1.1	N/A	Sikkerhetsstyring for fysiske grenser og/eller driftsgrenser for trafikkontroll og signalsystemer finnes i stor grad i 5.1.1.
W.3	5.1.2 5.2.3	N/A	

Tabellen nedenfor inneholder en kolonnebasert sammenligning mellom tidligere ISO HLS og de nye sikkerhetsstyringssystemkravene.

*Tabell 4: Kolonnebasert sammenligning — ISO High Level Structure*

The NSA NO 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 paragraf nr.</i>	<i>Forordning (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	
5.3	2.3	
6.1	3.1.1 3.1.2	CSM om risikovurdering anvendes for å avgjøre om en endring er sikkerhetsrelatert (eller ikke), og deretter om den er vesentlig (eller ikke). Det «virtuelle» skillet som er dannet av ISO mellom det strategiske nivået (ISO HLS Paragraf 6) og det taktiske nivået (ISO HLS Paragraf 8) i planleggingen, er revurdert i lys av EUs regulerende rammeverk, og særlig anvendelsen av ovennevnte CSM (uavhengig av endringene).
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	

The NSA NO 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 paragraf nr.</i>	<i>Forordning (EU) 2018/762 Krav- ID</i>	<i>Kommentar</i>
8.1	5.1 5.2 5.3 5.4 5.5	I henhold til ISO veiledningsdokumentet (N360), er hensikten med paragraf 8 i ISO-HLS å spesifisere kravene som må implementeres i virksomhetens virksomhet, for å sikre at styringssystemkravene oppfylles, samt for å sikre at prioriterte risikoer og muligheter blir tatt i betraktning. I tillegg er det oppgitt at tilleggskrav (spesifikke for kategori) knyttet til driftsplanlegging og kontroll kan komme til å gjelde. På denne måten er kravene i 5.X sammenhengende med ISO-tilnærmingen. De skal ikke være ødeleggende for selskapets virksomhet, men tilveiebringe et tilstrekkelig rammeverk for å kontrollere hvordan viktige sikkerhetsaspekter skal håndteres i selskapets forretningsprosesser.
9.1	6.1	Begrepet «overvåking» refererer til overvåkingsrammene som er definert i CSM om overvåkning, og har derfor en bredere betydning som viser til overvåking, måling, analyse og evaluering definert i paragraf 9.1 i ISO HLS.
9.2	6.2	Internrevisjoner er overvåkingsverktøy i henhold til CSM om overvåking. Selv om det er et eget krav, er det ment å nå målene med overvåking i samsvar med CSM om overvåking.
9.3	6.3	
10.1	7.1	
10.2	7.2	

**Vedlegg 2 — kryssaksept av tillatelser, godkjenninger eller sertifikater for produkter eller tjenester som leveres i samsvar med EU-regelverket**

Den utstedende myndighet for felles sikkerhetssertifikat eller sikkerhetstillatelse, kan godta sertifikater som er utstedt av andre organer, for eksempel ISO-samsvarsvurderingsorganer, for å unngå dobbel vurdering og tilleggskostnader som søker må dekke. Den endelige avgjørelsen ligger alltid hos utstedende myndighet.

I henhold til artikkel 3(12) i gjennomføringsforordning (EU) 2018/763, skal imidlertid utstedende myndighet ved vurdering av søknader om felles sikkerhetssertifikat, akseptere tillatelser, godkjenninger (for eksempel opplæringssenter) eller sertifikater for produkter eller tjenester som leveres av jernbanevirksomheter eller deres samarbeidspartnere eller leverandører, og som er utstedt i samsvar med relevant EU-regelverk, som dokumentasjon på at jernbanevirksomheten imøtekommer de korresponderende kravene som er for den aktuelle typen produkter eller tjenester. Selv om det ikke foreligger tilsvarende bestemmelser i EU-regelverket for vurdering av søknader om sikkerhetstillatelse, oppfordres også de nasjonale sikkerhetsmyndighetene til å anvende samme prinsipper.

Følgende tabell viser de ulike tilfellene som eksisterer så langt i EU-regelverket, og inneholder illustrerende eksempler på typer produkter eller tjenester som kan dekkes av hvert tilfelle.

*Tabell 5: Tillatelser, godkjenninger eller sertifikater for produkter eller tjenester som leveres i samsvar med EU-regelverket*

<i>Tilfelle</i>	<i>Type produkter eller tjenester</i>	<i>Gjeldende EU-regelverk</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>Kommentar</i>
ECM-sertifikat	Vedlikehold av godsvogner	Artikkel 14(4) i direktiv (EU) 2016/798	5.2 5.3	I tilfeller fastsatt i artikkel 14(4) i direktiv (EU) 2016/798, må sertifisering av enheter med ansvar for vedlikehold og verksteder (alt etter hva som er relevant), inneholde tilstrekkelig dokumentasjon på at jernbanevirksomheter og infrastrukturforvaltere gjennom deres sikkerhetsstyringssystem er i stand til å håndtere risiko knyttet til vedlikehold av godsvogner, herunder bruk av leverandører.

<i>Tilfelle</i>	<i>Type produkter eller tjenester</i>	<i>Gjeldende EU-regelverk</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>Kommentar</i>
Godkjenninger	Opplæring av lokomotivførere	Direktiv 2007/59/EF  Beslutning 2011/765/EU	4.2.2	Opplæringssentre skal godkjennes av kompetent myndighet for å arrangere opplæringskurs for lokomotivførere og lokomotivfører kandidater, i samsvar med direktiv 2007/59/EF. Opplæringssentrene spiller en viktig rolle for å sikre at lokomotivførere er kompetente for de sikkerhetsrelaterte oppgavene som er tildelt dem. I denne sammenheng bør opplæringssentrene være kompetente med hensyn til opplæringen de gir, og det faktum at de er anerkjent av en kompetent myndighet bør, der det er relevant, tas i betraktning av sikkerhetssertifiseringsorganet og nasjonale sikkerhetsmyndigheter når det gjennomføres en vurdering av kompetansestyringssystemet.
Lokomotivførerbevis og sertifikat	Lokomotivførerens kompetanse og skikkethet	Direktiv 2007/59/EF	4.2.1	Førerbevis og sertifikater utstedt i samsvar med direktiv 2007/59/EF, gir tilstrekkelig dokumentasjon på lokomotivførernes kompetanse og skikkethet. Dette fritar ikke virksomheten fra å måtte vise at deres ordninger for kompetanse og dugelighet er tilstrekkelige.

The NSA NO 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>Tilfelle</i>	<i>Type produkter eller tjenester</i>	<i>Gjeldende EU-regelverk</i>	<i>Forordning (EU) 2018/762 Krav-ID</i>	<i>Kommentar</i>
Felles sikkerhets-sertifikat	Vedlikehold av infrastrukturen Sporveksling Testing av rullende materiell	Artikkel 10 i direktiv (EU) 2016/798	5.3	Infrastrukturforvaltere kan bruke underleverandører for vedlikehold av infrastrukturen for selskaper som bruker spesialvogner på jernbanen. Likeledes kan sporvekslings- eller testoperatører bli bedt om å måtte besitte et sikkerhetssertifikat. I de ovennevnte tilfellene er felles sikkerhetssertifikat tilstrekkelig dokumentasjon på at jernbanevirksomhetene og infrastrukturforvalterne gjennom sikkerhetsstyringssystemet kan håndtere risikoen knyttet til bruken av leverandører.
Tillatelse til idriftssetting/godkjenning av vogntype	Godkjenning av vogn(type)	Direktiv (EU) 2016/797	5.2	Godkjenning av vogn(type) sikrer, gjennom design, produksjon, verifisering og validering, samsvar med de grunnleggende kravene i all gjeldende lovgivning (inkludert sikkerhet), og at den kan sikkert tas i bruk på jernbanenettene der den skal operere, i henhold til bruksgrensene og bruksvilkårene som er angitt i det tekniske registeret for vognen/vogntypen.

I noen tilfeller er det ikke sikkert at besittelse av et sertifikat (eller tilsvarende) som er utstedt i samsvar med EU-reglementet, er tilstrekkelig til å håndtere alle sikkerhetsrisiko knyttet til produktene som leveres til, eller tjenestene som brukes av, jernbanevirksomheter og infrastrukturforvaltere.

For eksempel har jernbanevirksomheter i samarbeid det fulle ansvar for en trygg drift, og således å styre risikoen knyttet til deres aktiviteter, herunder å sørge for vedlikehold på vognene. Dersom en jernbanevirksomhet bruker et samarbeidspartners felles sikkerhetssertifikat for å håndtere risiko som er knyttet til vedlikehold, er ikke dette tilstrekkelig dersom det ikke er grundig avtalefestet mellom de samarbeidende virksomhetene. Disse avtaleordningene må utvikles og overvåkes i fellesskap ved å anvende prosedyrer i begge parter sikkerhetsstyringssystemer, og er således underlagt tilsyn av respektive NSA.

Således kan det felles sikkerhetssertifikatet brukes som et middel til å håndtere risiko knyttet til vedlikeholdsleverandører, og som et middel for å overholde kravene til håndtering av risiko forbundet med vedlikehold av vogner, når de tre følgende betingelsene er oppfylt:

1. *Det må foreligge avtaleordninger mellom samarbeidende jernbanevirksomheter som omfatter slike aspekter knyttet til vedlikehold av vogner:*

The NSA NO 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.

- a) *Utteksling av informasjon som beskrevet i artikkel 5 i forordning (EU) 445/2011;*
  - b) *Teknisk støtte når det er hensiktsmessig, spesielt for gamle CCS-systemer;*
  - c) *Kontroll av evnen verkstedene vedlikeholdsleverandøren har til å utføre vedlikeholdet;*
  - d) *Hensiktsmessig overvåking av vogner og utveksling av informasjon som følge av denne overvåkingen.*
2. *Disse avtaleordningene må være utarbeidet på grunnlag av risikovurdering, og må overvåkes regelmessig av hver enkelt jernbanevirksomhet mot CSM om overvåking (forordning (EU) 1078/2012). Resultatene av denne overvåkingen må deretter formelt utveksles mellom begge de samarbeidende jernbanevirksomhetene.*
3. *Sikkerhetsstyringssystemet hos begge parter må inneholde tilstrekkelige prosesser og prosedyrer for å oppnå betingelsene 1 og 2 ovenfor.*

I andre tilfeller kan nasjonal lovgivning kreve at en bestemt type produkt eller tjeneste har et nasjonalt sertifikat (eller tilsvarende) som skal utstedes av et kompetent organ (for eksempel den nasjonale sikkerhetsmyndigheten), som også kan brukes som dokumentasjon på jernbanevirksomhetenes evne til å oppfylle de relevante kravene i kommisjonens delegerte forordning (EU) 2018/762 [*Forskrift om felles sikkerhetsmetode for sikkerhetsstyringssystemer (CSM SMS)*]. For eksempel kan nasjonale sertifikater utstedt til ECM og/eller vedlikeholdsverksteder som utfører vedlikehold på andre vogner enn godsvogner også gi en rimelig forsikring, i likhet med ECM-sertifikatet, om at vognene de utfører vedlikehold på er i sikker driftstilstand.

## Vedlegg 3 — sidesporsoperasjoner, avtaleordninger og samarbeid

### Sidesporsoperasjoner

I dette dokumentet forstås «sidespor» som en jernbaneinfrastruktur som er knyttet til et jernbanenett som er underlagt en infrastrukturforvalter (dvs. infrastrukturen av jernbanesystemet som omfattes av direktiv (EU) 2016/798). Sidespor kan eller kan ikke være en del av dette jernbanenettet, avhengig av gjennomføringen av ovennevnte Direktiv i hver enkelt medlemsstat.

Aktiviteter som gjøres på sidesporene, som lasting av vogner, er industrielle aktiviteter som i det etterfølgende samhandler med spesifikke jernbaneaktiviteter som sammensetning, klargjøring og kjøring av vogner som kan være tog eller bli brukt i tog. Dette inkluderer sammenkobling av ulike vogner for å danne vogngrupper eller tog, og kjøre dem.

Sidespor kan være (men er ikke begrenset til):

- *infrastruktur som brukes til å parkere jernbanevogner mellom operasjonene.*
- *intermodale terminaler;*
- *infrastruktur som brukes til tjenester på passasjervogner, som rengjøring eller lett vedlikehold;*
- *infrastruktur som tilhører og administreres av et vedlikeholdsverksted for jernbanevogner;*
- *industriområder eller anlegg der det utføres industrielle aktiviteter for lasting/lossing av godsvogner.*

Aktiviteten på sidesporene utføres av en «sidesporsoperatør». En sidesporsoperatør kan være et jernbaneforetak, en infrastrukturforvalter, en tjenesteleverandør (for eksempel for rengjøring av passasjervogner), et industriselskap (for eksempel et kjemikalieanlegg som laster og lossing tankvogner) eller en underleverandør til et slikt industriselskap. Sidesporsoperatøren har da påtatt seg rollen som et jernbaneforetak, eller er et jernbaneforetak som planlegger å utføre sidesporsaktiviteter i tillegg til gjeldende jernbaneaktiviteter. I sistnevnte tilfelle er infrastrukturforvalter den som er infrastrukturforvalteren for sidesporene, eller den som er jernbaneforetak under sikkerhetstillatelse.

«Sidesporsoperatøren» håndterer risiko forbundet med arbeidsmiljø og sikkerhet gjennom sitt foreliggende HMS-styringssystem i henhold til internasjonal og nasjonal lovgivning. Når «sidesporsoperatøren» ikke er et jernbaneforetak, må dette styringssystemet ta hensyn til HMS-forpliktelsene knyttet til eksterne arbeidere, særlig dem hos jernbaneforetakene, for eksempel når lokomotivførere kjører inn på et sidespor. Parallelt må jernbanevirksomheten håndtere risikoer forbundet med arbeidsmiljø og sikkerhet gjennom sitt HMS-styringssystem i henhold til internasjonal og nasjonal lovgivning.

#### **Eksempel 1: Sidesporsoperatøren er et jernbaneforetak «Y»**

Dette jernbaneforetaket håndterer, gjennom sitt sikkerhetsstyringssystem, risiko knyttet til sine jernbaneoperasjoner på sidesporene og på jernbanenettet under en infrastrukturforvalters ansvar. Denne risikostyringen inkluderer risiko forbundet med skade på vogner forårsaket av alle aktiviteter som utføres på sidesporet, herunder også sammensetning, klargjøring og kjøring av tog.

I praksis er det noen ganger vanskelig å fastslå hvem som er det ansvarlige jernbaneforetak. For eksempel ankommer et tog fra jernbaneforetak «X» et sidespor (lokfører og lokomotiv er innleid) og jernbaneforetak «Y», som driver sidesporet, tar det over som et nytt tog (lokfører og lokomotiv er innleid) og i mellomtiden må sidesporsoperasjoner utføres. I et slikt tilfelle gjelder ovennevnte sikkerhetsprinsipper. Det er felles samhandlingsrisiko som må vurderes i jernbaneforetak «Y»s sikkerhetsstyringssystem (for eksempel skader på vogner fra sidesporsoperasjoner, som lasting). I tillegg må utveksling av informasjon om kjøretøy fra jernbaneforetak «X» til jernbaneforetak «Y» også vurderes. Dette omfatter forsikring om at vognen er i sikker tilstand når jernbaneforetak «X» overfører den til sidesporsoperatøren, og likeledes når den overføres videre

via jernbaneforetak «Y». jernbaneforetak «Y» som er ansvarlig for sidesporaktiviteter, står fortsatt helt og fullt ansvarlig for håndtering av risikoer knyttet til vedlikeholdsaktiviteter som utføres deretter.

**Eksempel 2: Sidesporoperatøren er ikke et jernbaneforetak**

Dette kan deles opp i fire undereksempler:

- **Eksempel 2.1** når sidesporoperatøren er infrastrukturforvalteren.
- **Eksempel 2.2 og 2.3** når sideoperatøren, som ikke er infrastrukturforvalter, kun driver aktiviteter på sin egen infrastruktur, men ikke på jernbanenettet underlagt infrastrukturforvalters ansvar.
- **Eksempel 2.4** omfatter jernbanedrift utført av en sidesporoperatør, som ikke er infrastrukturforvalter, på jernbanenettet underlagt infrastrukturforvalterens ansvar.

**Eksempel 2.1:** Når driften på sidesporene deles mellom jernbaneforetak og en infrastrukturforvalter (eller eventuelt en virksomhet som handler på vegne av den), må hvert jernbaneforetak informeres om alle sikkerhetsrelaterte hendelser som har oppstått under infrastrukturforvalterens drift gjennom avtaler. Dette inkluderer skader, ulykker og uønskede hendelser som involverer kjøretøy.

Disse avtalene kan håndteres gjennom hvert av jernbaneforetakenes sikkerhetsstyringssystem, og infrastrukturforvalterens sikkerhetsstyringssystem.

Gjennom sikkerhetsstyringssystemet håndterer jernbaneforetak risiko knyttet til egen drift basert på mottatt informasjon.

**Eksempel 2.2:** Togsammensetning og klargjøring gjøres av jernbaneforetak (kobling, klargjøring) på sidesporinfrastrukturen. Jernbaneforetaket må informeres om alle (sikkerhetsrelaterte) hendelser som har funnet sted i løpet av driften hos sidesporoperatøren (for eksempel lasting eller rengjøring) gjennom avtaler. Dette inkluderer skader, ulykker og uønskede hendelser som involverer kjøretøy.

Disse avtalene kan styres gjennom jernbaneforetakets sikkerhetsstyringssystem.

Gjennom sikkerhetsstyringssystemet håndterer jernbaneforetaket risiko knyttet til egen drift basert på mottatt informasjon.

**Eksempel 2.3:** Togsammensetningen utføres helt/delvis av sidesporoperatøren eller av en virksomhet som arbeider på vegne av sidesporoperatøren.

Etter at et tog er sammensatt, overføres det til en jernbaneforetak .

Akkurat som i eksempel 2.2, må jernbaneforetaket informeres om alle (sikkerhetsrelaterte) hendelser som har funnet sted i løpet av driften hos sidesporoperatøren (for eksempel lasting eller rengjøring) og ved togsammensetning gjennom avtaler. Slike hendelser inkluderer skader, ulykker og uønskede hendelser som involverer kjøretøy.

Disse avtalene kan styres gjennom jernbaneforetak sikkerhetsstyringssystem.

Gjennom sikkerhetsstyringssystemet håndterer jernbaneforetakets risiko knyttet til egen drift basert på mottatt informasjon.

**Eksempel 2.4:** Dette eksemplet supplerer eksempel 2.3. Således er kun jernbaneforetakets ytterligere forpliktelser beskrevet her.

Sidesporoperatøren kjører tog eller flytter vogngrupper fra jernbaneinfrastrukturen sin til jernbanenettet som er underlagt en infrastrukturforvalters ansvar.

Eksempel:

- *Tog eller vogngrepper flyttes fra et serviceverksted til plattformene ved en passasjerterminal eller til en parkeringsplass knyttet til en passasjerterminal;*
- *Tog eller vogngrepper flyttes fra et industrianlegg til et utvekslingssted knyttet til en fraktstasjon.*

Sidesporsoperatøren er verken en jernbaneforetak eller en infrastrukturforvalter, men aktivitetene som utføres på jernbanenettet til en infrastrukturforvalter, må dekkes av et felles sikkerhetssertifikat eller en sikkerhetstillatelse.

Jernbanedriften som sidesporsoperatøren har drevet på jernbanenettet som er underlagt en infrastrukturforvalters ansvar, er enten dekket av sikkerhetssertifikatet til et jernbaneforetak eller av sikkerhetstillatelse til en infrastrukturforvalter. Dette innebærer at jernbaneforetak eller infrastrukturforvalteren må håndtere risiko knyttet til aktiviteter utført av sidesporsoperatøren, gjennom ordninger for styring av underleverandører i sitt sikkerhetsstyringssystem.

Jernbaneforetakene og infrastrukturforvalteren må i alle tilfeller nøye beskrive omfanget av all sin jernbanedrift og sine aktiviteter som samhandler med annen jernbanedrift, slik at nasjonale sikkerhetsmyndigheters tilsyn av sikkerhetsstyringssystemet blir hensiktsmessig. Jernbaneforetakene og infrastrukturforvalters evne til å gi en klar og fullstendig beskrivelse av driften, samt andre aktiviteter som knytter seg til jernbanedriften, er avgjørende for å sikre hensiktsmessigheten av sikkerhetsstyringssystemet og hensiktsmessigheten av nasjonale sikkerhetsmyndigheters tilsyn.

Avtalene i alle ovennevnte underseksempler må klart beskrive (men er ikke begrenset til):

- *hva som skal gjøres av hver av partene i avtalen;*
- *den forventede kvaliteten på resultater/tjenester;*
- *tildeling av roller og ansvar;*
- *hva, når og hvordan informasjon vil bli utvekslet mellom partene. Informasjonen må inkludere rapportering om hendelser som beskrevet i alle underseksemlene ovenfor, samt de spesifikke egenskapene til infrastrukturen for sidesporet, som fartsgrenser, vektgrenser eller hellingsforhold;*
- *kompetansekrav;*
- *HMS-krav (utledet fra risikovurdering, nasjonale krav osv.).*

## **Avtaler og samarbeid**

Jernbaneforetaket er ansvarlig for å sørge for sikker drift av toget, ved å koordinere og administrere togoperasjonene. Avtaleordninger (som regel bestående av rammeavtaler, særskilte avtaler og vedlegg) utgjør grunnlaget for et hensiktsmessig samarbeid mellom ulike jernbaneforetak, det være seg nye eller etablerte aktører, og må overholde bestemmelsene i europeisk og nasjonal lovgivning, samt eventuelle andre gjeldende krav.

Således må jernbaneforetaket håndtere risikoen ved driften, herunder samarbeid med samarbeidspartnere og bruken av (under)leverandører. NSA fører så tilsyn med at jernbaneforetaket oppfyller sine lovfestede forpliktelser transparent og grundig.

Jernbaneforetak kan ikke outsource sitt sikkerhetsansvar for å koordinere og håndtere en sikker drift av togene sine. Dette hindrer ikke at jernbaneforetakene kan samarbeide. Jernbaneforetaket som er ansvarlig for sikker togdrift, må være tydelig identifisert i alle avtaler mellom de involverte partene, og må besitte et felles sikkerhetssertifikat. Dette jernbaneforetaket kan enten forvalte ressursene direkte (bemanning, vogner) via sikkerhetsstyringssystemet, eller bestemme seg for å sette dem bort enten delvis eller helt (for eksempel leasing av vogner, ansettelse av lokførere) til en leverandør. I sistnevnte tilfelle sitter

---

The NSA NO 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.

jernbaneforetaket fortsatt med ansvaret for å håndtere risikoer knyttet til bruken av (under)leverandører ved å styre at avtalen gjennomføres i henhold til sikkerhetsstyringssystemet sitt og [forordning \(EU\) 1078/2012](#), og således må det kontrolleres at disse ressursene overholder lovfestede krav og andre gjeldende sikkerhetskrav (for eksempel at vogner er i sikker driftstilstand, rutekompatibilitet, personellutdanning, lokførere med gyldig lisens og sertifikat for en bestemt rute).

Et felles sikkerhetssertifikat som er utstedt av et sikkerhetssertifiseringsorgan (og overvåket av en NSA i henhold til dette) til avtaleparten (dvs. samarbeidspartneren eller underleverandøren), kan gi tilstrekkelig forsikring til jernbaneforetaket som er ansvarlig for sikker drift om at sikkerhetsstyringssystemet oppfyller de relevante kravene. Avtalene omfatter utveksling av informasjon som er relevant for sikkerheten (for eksempel tidligere hviletid for lokomotivførere) mellom avtalepartene.

Prinsippene for samarbeid mellom jernbaneforetakene forblir de samme uavhengig av samarbeidsregimer, dvs. samarbeid eller bortsetting av (delvis eller helt) av jernbanedrift nasjonalt eller grenseoverskridende. Arten og omfanget av tiltakene som skal gjennomføres av jernbaneforetakene, og i hvilken utstrekning NSA skal føre tilsyn med samarbeidsordningene, står imidlertid i forhold til samarbeidsomfanget mellom jernbaneforetakene.

For eksempel vil grenseoverskridende samarbeid mellom jernbaneforetak (dvs. bruk av eksterne vogner og/eller bemanning) trolig kreve større kontroll enn noen andre samarbeidsordninger, fordi driften blir satt bort til et annet jernbaneforetak med andre språk og driftsregler for kjøretøy, som kan variere fra medlemsstat til medlemsstat. I motsetning til dette vil det bare være behov for mindre kontroll og dermed mindre tilsynsaktiviteter fra NSA.

## Vedlegg 4 — sikkerhetskultur

### *Introduksjon til sikkerhetskultur*

Kultur oppstår fra samspillet mellom mennesker i hverdagen, og bidrar til å definere samfunnets atferdsmessige forventninger og normer. Kultur er et komplekst konsept som involverer en rekke faktorer som utvikler seg over tid, avhengig av omstendigheter, miljø og opplevelser i en nasjon, stat, samfunn og/eller virksomhet.

Sikkerhetskultur refererer til elementene i kulturen som spesifikt angår sikkerheten. Det er mulig å gi en beskrivelse av noen av faktorene som bidrar til en god sikkerhetskultur, men imidlertid umulig å samle sammen all informasjon som omfatter sikkerhetskulturen. Det finnes ingen enkel vitenskapelig måling av sikkerhetskulturen. Dette skyldes at faktorene som bidrar til den varierer, ikke bare mellom virksomheter, men også i dem. Ulike avdelinger har forskjellige sikkerhetskrav og behov, for eksempel driftsmessige og økonomiske, og den rådende sikkerhetskulturen vil utvikle seg ut fra disse. Eksterne faktorer som forskriftsmessige krav, utdanningsnivåer, samfunnsstrukturer og nasjonal kultur vil også bidra til en virksomhets sikkerhetskultur.

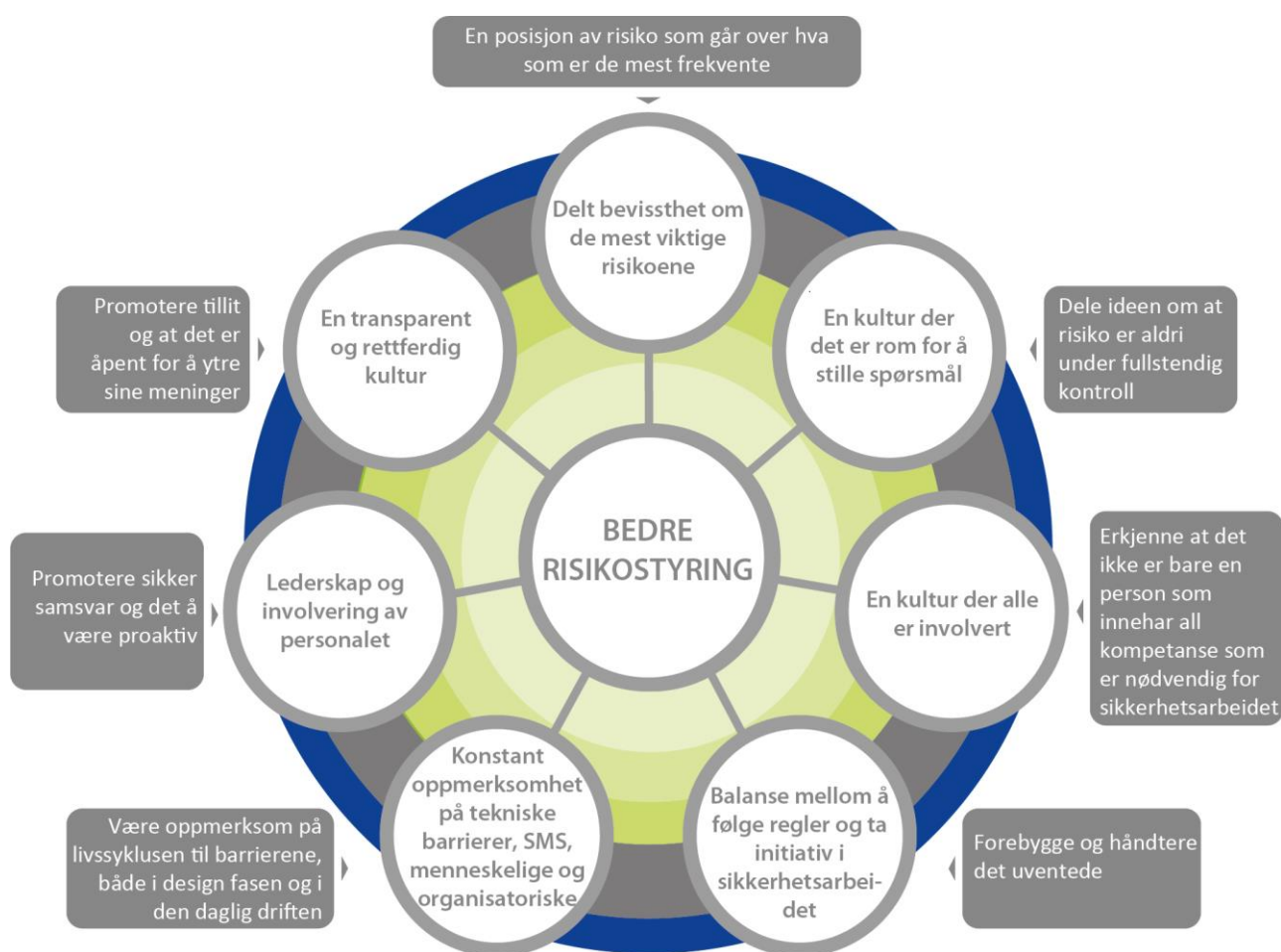
Sikkerhetskultur er et etablert konsept. Konseptet mangler imidlertid en definisjon man enes om. Mangelen på en definisjon har medført at det har blitt et skille mellom teori og praksis, og det som i hovedsak er en sosial forestilling har blitt omgjort til egenskaper for en god sikkerhetskultur.

Når det er sagt, er en enkel måte å beskrive sikkerhetskulturen på å se på faktorene som bidrar til atferden. Sikkerhetsstyringssystemet danner grunnlaget ved å definere og pålegge hva som kreves, gjennom retningslinjer og prosedyrer. I utopien vil sikkerhetsstyringssystemet være perfekt, og all ledelse og alt personell vil etterleve det. Utopi er dessverre bare utopi, og det som skjer er at ledelse og personell prøver å gi innholdet i sikkerhetsstyringssystemet mening basert på verdier, holdninger og meninger på grunnlag av en kombinasjon av personlig erfaring, arbeidsstandarder og arbeidsforholdene på arbeidsplassen og i samfunnet. Hvis sikkerhetsstyringssystemet gir mening og det er en kultur for etterlevelse, vil korrekt atferd følge av dette. Hvis ikke dette er tilfellet blir det gjort individuelle tolkninger, og det vil bli anvendt alternative løsninger. Disse vil være basert på en individuell risikovurdering som veier opp faktorer som påvirker avgjørelser som er truffet. Risikovurderingen vil ikke bare fokusere på den faktiske risikoen, men omfatte forhold knyttet til anvendelighet, risikoen for å bli tatt, ledelsens ord og handling, etc. Gjensidig avhengighet mellom sikkerhetsstyringssystemet, det at det gir mening, samt atferd, definerer derfor sikkerhetskulturen.

Måling av sikkerhetskulturen krever innsikt i de tre faktorene og deres gjensidige avhengighet. Som nevnt tidligere, finnes det ingen enkel vitenskapelig måling av sikkerhetskulturen. I stedet kan egenskaper som påvirker sikkerhetskulturen analyseres i lys av de tre faktorene.

For eksempel kan retningslinjer som «Sikkerheten først» følges opp ved å undersøke hva de betyr for medarbeiderne: Har de tro på dem? Går ledelsen i bresjen? Hvordan tas beslutninger og på hvilke grunnlag? Hvordan reagerer virksomheten når den er under press? osv. Lignende undersøkelser kan gjøres for andre faktorer, som kontinuerlig læring og en kritisk holdning. Når resultatene av analysen settes sammen, vil det dannes et bilde av tilstanden på kulturen. Over tid kan et mer omfattende bilde dannes, slik at det trekkes mer kvalifiserte konklusjoner.

For å forstå sikkerhetskulturen i en virksomhet, har eksperter og forskere utviklet modeller, som vanligvis innebærer et sett med egenskaper for en positiv sikkerhetskultur. Figur 4 er et eksempel på en slik modell, basert på arbeid nylig utført av Institute for an Industrial Safety Culture (ICSI).



Figur 4: Egenskaper for en sikkerhetskultur

Basert på ICSI-modellen kan man finne en sammenheng mellom de fleste elementene i sikkerhetsstyringssystemet og de overordnede egenskapene ved en sikkerhetskultur, som vist i tabell 6.

Tabell 6: Forhold mellom sikkerhetsstyringssystemkrav og egenskapene ved en sikkerhetskultur

SMS-elementer	CSM SMS- krav	Egenskaper for en sikkerhetskultur
Ledelse og forpliktelse	2.1	<ul style="list-style-type: none"> <li>Spørrende kultur</li> <li>Transparent og rettferdig kultur</li> <li>Lederskap og involvering av medarbeidere</li> </ul>
Sikkerhetspolitikk	2.2	Lederskap og involvering av medarbeidere
Struktur og ansvar	2.3	Integrert kultur (alle er involvert)

<i>SMS-elementer</i>	<i>CSM SMS- krav</i>	<i>Egenskaper for en sikkerhetskultur</i>
Bemanning og andre parter involvering	2.4	<ul style="list-style-type: none"> <li>• Transparent og rettferdig kultur</li> <li>• Integrert kultur (alle er involvert)</li> <li>• Lederskap og involvering av medarbeidere</li> </ul>
Risikovurdering	3.1	<ul style="list-style-type: none"> <li>• Felles fokusering på de viktigste risikoene</li> <li>• Alltid ha i bakhodet tekniske barrierer, sikkerhetsstyringssystemet, menneskelige og organisatoriske faktorer</li> <li>• Fornuftig balanse mellom å følge regler for sikkerhet og ta initiativ til sikkerhet</li> </ul>
Sikkerhetsmål og planlegging	3.2	-
Ressurser	4.1	Integrert kultur (alle er involvert)
Kompetanse	4.2	<ul style="list-style-type: none"> <li>• Transparent og rettferdig kultur</li> <li>• Integrert kultur (alle er involvert)</li> </ul>
Bevissthet	4.3	Felles fokusering på de viktigste risikoene
Informasjon og kommunikasjon	4.4	Transparent og rettferdig kultur
Dokumentert informasjon/dokumentasjon i sikkerhetsstyringssystemet	4.5	Alltid ha i bakhodet tekniske barrierer, sikkerhetsstyringssystemet, menneskelige og organisatoriske faktorer
Integrasjon av menneskelige og organisatoriske faktorer	4.6	-
Driftsaktiviteter	5.1	<ul style="list-style-type: none"> <li>• Felles fokusering på de viktigste risikoene</li> <li>• Spørrende kultur</li> <li>• Fornuftig balanse mellom å følge regler for sikkerhet og ta initiativ til sikkerhet</li> </ul>
Forvaltning av eiendeler	5.2	Felles fokusering på de viktigste risikoene

The NSA NO 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>SMS-elementer</i>	<i>CSM SMS- krav</i>	<i>Egenskaper for en sikkerhetskultur</i>
Entreprenører, partnere og leverandører	5.3	<ul style="list-style-type: none"> <li>• Transparent og rettferdig kultur</li> <li>• Integrert kultur (alle er involvert)</li> </ul>
Endringsstyring	5.4	-
Håndtering av nødsituasjoner	5.5	Fornuftig balanse mellom å følge regler for sikkerhet og ta initiativ til sikkerhet
Overvåking	6.1	En kultur der det er rom for å stille spørsmål
Internrevisjon	6.2	-
Ledelsens gjennomgåelse	6.3	-
Erfaringer fra ulykker og hendelser	7.1	<ul style="list-style-type: none"> <li>• En kultur der det er rom for å stille spørsmål</li> <li>• Transparent og rettferdig kultur</li> </ul>
Kontinuerlig forbedring	7.2	<ul style="list-style-type: none"> <li>• En kultur der det er rom for å stille spørsmål</li> <li>• Transparent og rettferdig kultur</li> </ul>

Mer informasjon om ICSI-modellen finner du på deres nettsted (<http://www.icsi.eu.org>).

## Vedlegg 5 — menneskelige og organisatoriske faktorer

### Introduksjon til menneskelige og organisatoriske faktorer

Menneskelige og organisatoriske faktorer (MOF) er et tverrfaglig felt som fokuserer på hvordan man kan øke sikkerheten, forbedre ytelsen og øke brukertilfredsheten. MOF er basert på forståelse av brukere, oppgaver og miljøer. Utgangspunktet er alltid brukerens evner og begrensninger, og hvordan disse påvirkes og samhandler med systemene som brukes når arbeidsoppgaver utføres. Målet er å identifisere hvordan man best kan utføre arbeidsoppgavene på en sikker og hensiktsmessig måte. Det legges vekt på anvendelighet. MOF brukes forebyggende for å sikre gode designprosesser, og tilbakevirkende for å identifisere årsaker når noe har gått galt.

Når man for eksempel skal designe et nytt kjøretøy, er det ikke nok bare å bruke designstandardene. Lokomotivførere, ledere og vedlikeholdspersonell bør være involvert for å få frem deres erfaringer og forståelsen av hvordan de skal utføre arbeidsoppgavene sine sikkert og hensiktsmessig. Dette kan for eksempel være knyttet til spesifikke stasjons- eller strekningsproblemer, tilgjengelighet og tilgang til vedlikeholdspersonell, oppgaveprioriteringer i førerrommet, kommunikasjonskrav eller passasjeratferd på stasjoner.

Man kan innhente kunnskap og erfaring fra ulike operatører på best mulig måte gjennom en iterativ prosess, der brukeren kontinuerlig evaluerer design og utvikling av toget. Dette bidrar til å forhindre feil i designprosessen, altså å fokusere på menneskets samspill med individuelle systemer i stedet for å vurdere oppgaver generelt. Ulike leverandører har for eksempel ulikt syn på hvordan alarmer skal prioriteres, og uten et helhetlig perspektiv ender ofte brukeren opp med å bli overlesset med informasjon som har begrenset relevans for å utføre oppgaven. Dette er fordi teknisk design gir muligheten til å vise informasjonen, men der brukeren kanskje ikke har behov for den. MOF-analyse kan hjelpe til å skille mellom behovet for å vite og «kjekt å ha».

MOF innebærer å ha et systematisk perspektiv, det vil si ikke bare å se på de menneskelige, teknologiske og organisatoriske faktorene i seg selv, men også fokusere på spillet mellom de ulike faktorene. Hvis for eksempel en lokomotivfører har vært involvert i en passhendelse, omfatter de foreslåtte granskningspunktene relevante problemer (ikke en uttømmende liste), for eksempel tretthet, kognitiv overbelastning, kompetanse osv. (menneskelig), teknologisk innvirkning på yteevnen, som for eksempel grensesnitt mellom menneske og system, layout, signalplassering (teknologi), virksomhetens innflytelse på yteevnen, som opplæring, sikkerhetsstyringssystem, virksomhetsprioriteringer (virksomhet) og spillet mellom de tre områdene som innflytelse på anskaffelser med hensyn til design eller endringsstyring med innføring av nytt design.

Metodene er hentet fra en rekke forskjellige felt, for eksempel eksperimentall psykologi, industriteknikk, virksomhetspsykologi, sosiologi, ledelsesvitenskap, kognitiv teknikk, ergonomi, datavitenskap og sikkerhetsteknikk. Siden MOF fokuserer på brukeren, er en oppgaveanalyse en vanlig anvendt metode. En oppgaveanalyse gir designeren en forståelse av oppgavene som skal utføres, og hvordan de knytter seg til systemer som brukeren samhandler med og organisatoriske faktorer som har innvirkning på yteevnen. Basert på oppgaveanalysen kan det gjennomføres videre analyser, som for eksempel analyser av samhandling mellom menneske og system, arbeidsbelastning og menneskelig pålitelighet/risiko. Nøkkelen er å sikre at brukeren har best mulig arbeidssituasjon for en sikker og hensiktsmessig prestasjonsevne.

Følgende referanser inneholder ytterligere informasjon om menneskelige og organisatoriske faktorer:

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

---

The NSA NO 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.

## **Strategi for å støtte integrering av menneskelige og organisatoriske faktorer i sikkerhetsstyringssystemet**

Virksomheten skal ha en strategi for menneskelige og organisatoriske faktorer, fagkunnskap og metoder. Tilnærmingen skal være systematisk og konsekvent anvendes i alle relevante prosesser i virksomheten. En slik tilnærming innebærer først å vurdere behovene, evnene og atferden til mennesker i forbindelse med arbeidsoppgaver som skal utføres, og deretter å utarbeide en strategi for å imøtekomme behov, evner og atferd i forhold til arbeidsoppgaven.

Strategien menneskelige og organisatoriske faktorer (MOF) kan inneholde elementer som knytter seg til:

### **Lederskap**

- *Lederskap og forpliktelse*
  - *Ledelsens forpliktelse for MOF er tydelig beskrevet i retningslinjer og mål*
  - *Det foreligger en prosess/veileder som viser hvordan MOF skal anvendes i prosjekter*
  - *MOF er en integrert del av designprosessen og prosjektstyringen*
- *Sikkerhetspolitikk*
  - *Sikkerhetspolitikken definerer klart at det bør anvendes et MOF-perspektiv i alle sikkerhetsrelaterte prosesser*
- *Roller, ansvar og myndighet i virksomheten*
  - *Klart definerte roller, ansvar og myndighet hos MOF-ekspertisen*
  - *Det foreligger en prosess for hvordan MOF-ekspertisen jevnlig deltar i prosjekter og prosesser.*

### **Planlegging**

- *Tiltak for å fokusere på risiko*
  - *En beskrivelse av hvordan MOF-perspektivet tas i betraktning i risikoanalyser*
  - *MOF-eksperter involveres i risikoanalyser*

### **Støtte**

- *Ressurser og kompetanse*
  - *En systematisk tilnærming for å sikre at det foreligger MOF-kompetanse i relevante roller basert på behovsanalyse*
  - *Det tilordnes tid og ressurser for å sikre at MOF-kravene er imøtekommet*
- *Bevissthet*
  - *Det foreligger kunnskap på tvers av virksomheten om den systematiske tilnærmingen for å sikre MOF-kompetanse i relevante roller*

### **Drift**

- *Driftsplanlegging og styring*
  - *MOF er tatt hensyn til i driftsplanleggingen*
- *Forvaltning av eiendeler*
  - *Virksomheten har tatt hensyn til MOF i forbindelse med forvaltning av eiendeler*
- *Endringsstyring*
  - *MOF skal alltid vurderes som en del av håndteringen av endringsprosessen*

### **Ytelseevaluering**

- *Overvåking*

---

The NSA NO 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.

- *Sikkerhetsresultat vurderes systematisk i lys av MOF-strategien.*

**Forbedring**

- *Erfaringer fra ulykker og hendelser*
  - *MOF-ekspertise og metoder brukes ved granskning av ulykker*
  - *Det foreligger en metode for å gjennomføre granskning basert på MOF-kunnskap og metoder*
  - *Det foreligger et opplæringsprogram for dem som gransker uønskede hendelser og ulykker, der man anvender et MOF-perspektiv*
- *Kontinuerlig forbedring*
  - *Prosess for kontinuerlig forbedring av virksomhetsprosessene for styring av MOF*

**Vedlegg 6 – definisjoner**

Bruken av ordene eller begrepene i dokumentet, for eksempel «må», «bør» eller «skal», indikerer at det foreligger et lovfestet krav som må etterleves.

Jernbaneulykke	En uønsket eller utilsiktet plutselig hendelse eller en bestemt rekke slike hendelser som har skadelige følger, herunder som medfører at noen dør eller blir alvorlig skadet, som medfører betydelig skade på jernbanemateriell, på jernbaneinfrastruktur, på eiendom utenfor jernbanen eller på miljø, og alle andre lignende ulykker(direktiv (EU) 2016/798).
Driftsområde	Ett eller flere nett i én eller flere medlemsstater, hvor en jernbanevirksomhet har til hensikt å drive sin virksomhet (direktiv (EU) 2016/798).
Forvaltning av eiendeler	Tilnærmingen som brukes av en virksomhet for å sikre at fysiske eiendeler forblir sikre, egnet til bruk og kommersielt levedyktige fra design og konstruksjon, og gjennom hele levetiden og frem til avvikling.
Revisjon	En systematisk, uavhengig og dokumentert prosess for å skaffe revisjonsbevis og evaluere dette objektivt, for å fastslå at omfanget av revisjonskriteriene er oppfylt (ISO 9000).
Driftens art	Utforming og oppbygging av infrastrukturen, vedlikehold av infrastruktur, trafikkplanlegging, trafikkstyring og kontroll, og bruk av jernbaneinfrastruktur, inkludert konvensjonelle linjer og/eller høyhastighetslinjer, passasjertransport og/eller godstransport
Kompetanse	Evnen til å anvende kunnskaper og ferdigheter for å nå ønskede resultater (ISO 9000).
Kontinuerlig forbedring	Gjentakende aktivitet for å forbedre ytelsen (dvs. målbart resultat) (ISO 9000).
Dokumentstyring	Proessen (eller prosedyren) for identifisering, utarbeiding, vedlikehold, styring, lagring og oppbevaring av dokumentert informasjon.
Driftens omfang	I forbindelse med jernbanedriften som utføres av jernbaneforetakene, betegnes omfanget av passasjerantall og/eller godsvolum og den beregnede størrelsen på et jernbaneforetak med hensyn til antall ansatte som arbeider i jernbaneforetaket, inkludert innleid personell (dvs. som små, mellomstore eller store bedrifter) (direktiv (EU) 2016/798).  I forbindelse med jernbanedriften som utføres av infrastrukturforvaltere, omfanget som betegnes av lengden på jernbanesporet og infrastrukturforvalterens anslåtte størrelse med hensyn til antall ansatte som arbeider hos infrastrukturforvalteren, inkludert innleid personell (forordning (EU) 2018/762 [CSM SMS]).
Fare	Et forhold som kan føre til en ulykke (forordning (EU) 402/2013).
Menneskelige og organisatoriske faktorer	Alle menneskelige ytelsesegenskaper og organisatoriske aspekter som må vurderes for å ivareta sikkerheten og hensiktsmessigheten til et system eller en virksomhet gjennom hele levetiden.
Menneskelig sentrert tilnærming	En tilnærming som innebærer først å vurdere behovene, evnene og atferden til mennesker, og deretter å utarbeide en strategi for å imøtekomme slike behov, evner og atferd.

The NSA NO 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.

Uønsket hendelse	Enhver hendelse, unntatt en ulykke eller alvorlig ulykke, som påvirker sikkerheten ved jernbanedriften (direktiv (EU) 2016/798). Dette inkluderer nestenulykker.
Infrastrukturforvalter	Ethvert organ eller foretak som er ansvarlig særlig for å opprette, forvalte og vedlikeholde jernbaneinfrastruktur, herunder trafikkstyring og styring, kontroll og signal. Infrastrukturforvalters oppgaver på et nett eller en del av et nett kan tildeles forskjellige organer eller foretak (direktiv 2012/34/EU).
Interessent	Person eller virksomhet som enten kan påvirke, bli påvirket av eller som oppfatter seg selv som påvirket av en beslutning eller aktivitet (ISO 9000) som er knyttet til sikkerhetsstyringssystemet.
Granskning	En prosess som gjennomføres for å forebygge ulykker og uønskede hendelser, som omfatter innsamling og analyse av informasjon, komme frem til konklusjoner, herunder å fastslå årsak, og når det er hensiktsmessig, utarbeide sikkerhetsanbefalinger (direktiv (EU) 2016/798).
Styringssystem	Et sett med elementer i en virksomhet for å fastsette retningslinjer og mål, og prosessene for å nå disse målene, og som er forbundet med eller samhandler med hverandre (ISO 9000).
Overvåking	Ordninger som jernbanevirksomheter eller enhet med ansvar for vedlikehold innfører for å kontrollere at styringssystemet anvendes riktig og er hensiktsmessig (forordning (EU) 1078/2012).
Nasjonale regler	Alle bindende regler vedtatt i en medlemsstat, uavhengig av hvilket organ som utsteder dem, som inneholder andre krav til jernbanesikkerhet eller tekniske krav enn de som er fastsatt i EØS-regelverket eller internasjonale regler, og som får anvendelse i den aktuelle medlemsstaten på jernbanevirksomheter eller tredjepart (direktiv (EU) 2016/798).
Prosess	Et sett av aktiviteter som er forbundet med eller samhandler med hverandre, og som gjør teori om til praksis (ISO 9000).
Jernbaneinfrastruktur	Fasiliteter som er nødvendige for at en jernbane skal kunne fungere, herunder: <ul style="list-style-type: none"> <li>• jernbanespor og tilknyttede sporstrukturer</li> <li>• sidespor, signalanlegg, kommunikasjonssystemer, kjøretøy</li> <li>• kontrollsystemer, togledersentraler og databehandlingssystemer</li> <li>• varsler og skilting</li> <li>• elektrisk kraftforsyning</li> <li>• tilknyttede bygninger, verksteder, depoter og driftsbanegårder</li> <li>• anlegg, maskiner og utstyr</li> </ul>
Jernbaneforetak	Ethvert offentlig eller privat foretak som har som virksomhet å yte tjenester for transport av gods og/eller passasjerer med jernbane, der foretaket forplikter seg til å sørge for trekkraften, herunder foretak som bare sørger for trekkraften
Risiko	Hyppigheten av forekomsten av ulykker og uønskede hendelser som medfører skade (som følge av fare) og alvorlighetsgraden av skadene (forordning (EU) 402/2013, CSM RA).

The NSA NO 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.

Risikoanalyse	Systematisk anvendelse av all tilgjengelig informasjon for å identifisere farer og anslå risikoer (forordning (EU) 402/2013, CSM RA).
Risikovurdering	Den samlede prosessen som omfatter en risikoanalyse og en risikovurdering (forordning (EU) 402/2013).
Risikoevaluering	En prosedyre basert på risikoanalysen for å fastslå om det er oppnådd et akseptabelt risikonivå (forordning (EU) 402/2013).
Risikostyring	Systematisk anvendelse av styringspolicyer, prosedyrer og praksis for arbeidsoppgaver, for å analysere, evaluere og håndtere risikoene (forordning (EU) 402/2013).
Sikkerhetskultur	Består av felles oppfatninger, praksis og holdninger som finnes ved en bedrift.  Hvordan sikkerhet oppfattet, verdsatt og prioritert i en virksomhet. Gjenspeiler forpliktelse og engasjement til sikkerhetsarbeidet på alle nivåer i virksomheten. Blir også beskrevet som «Hvordan en virksomhet oppfører seg når ingen ser på».
Sikkerhetsmål	Resultatene som skal oppnås.  Et sikkerhetsmål må være spesifikt, målbart, oppnåelig, realistisk og tidsbasert. Det må også angis for relevante funksjoner og nivåer i virksomheten.
Partner	En virksomhet som en annen virksomhet har inngått samarbeid med. Dette forholdet kan være en avtalebasert, der begge virksomhetene forplikter seg til ikke å samarbeide med noen tredjeparter.
Samarbeid mellom partnere	En ordning der partene, også kalt samarbeidspartnere, blir enige om å samarbeide for å fremme felles interesser.
Sikkerhetsstyringssystem	Den organisasjonen, de tiltakene og de framgangsmåtene som en jernbanevirksomhet har opprettet med sikte på en sikker drift av sin virksomhet (direktiv (EU) 2016/798).
Toppledelse	Person eller gruppe som styrer og håndterer en virksomhet på høyeste nivå (ISO 9000).
Driftstype	Typen kjennetegnes ved passasjertransport, inkludert eller ekskludert høyhastighetstjenester, godstransport, inkludert eller ekskludert farlig gods, og kun skiftetjenester (direktiv (EU) 2016/798).