EUROPEAN UNION AGENCY FOR RAILWAYS

Et bedre fungerende jernbanesystem for samfunnet.

Veileder

Prinsipper for tilsyn

	Utarbeidet av	*Validert av*	*Godkjent av*
Navn	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
Stilling	Prosjektmedarbeider	Prosjektleder	Enhetsleder
Dato	29/06/2018	29/06/2018	29/06/2018
Underskrift			

Dokumentlogg

Versjon	*Dato*	*Kommentarer*
1.0	29/06/2018	Endelig versjon for publisering.

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

120 Rue Marc Lefrancq | BP 20392 | FR-59307 Valenciennes Cedex
Tlf. +33 (0)327 09 65 00 | era.europa.eu

1. Innledning

1.1 Formålet med veilederen

De nasjonale sikkerhetsmyndighetene (NSA-er) i Europa varierer i størrelse og kompleksitet. Denne veilederen beskriver først og fremst hvordan NSA-ene kan føre tilsyn med sine infrastrukturforvaltere og jernbanevirksomheter, men også enheter med ansvar for vedlikehold, der det er hensiktsmessig, på en konsistent måte i forhold til deres størrelse. Veilederen tar sikte på å gi NSA-er og andre berørte parter en forklaring på hvilken rolle tilsyn spiller i det europeiske jernbanesystemet og hvordan det er knyttet til sikkerhetsvurdering.

Husk at når det gjelder tilsyn med farlig gods på jernbanen kan nasjonal sikkerhetsmyndighet enten ha en direkte rolle eller en indirekte og koordinerende rolle sammen med annen relevant tilsynsmyndighet.

1.2 Hva er tilsyn?

Med tilsyn menes den framgangsmåten som er innført av NSA-en for å overvåke hensiktmessigheten til sikkerhetsstyringssytemet etter at det er blitt utstedt et felles sikkerhetssertifikat eller en sikkerhetstillatelse og at alle nødvendige krav er kontinuerlig oppfylt.

Dette tilsynet dekker NSA-ens handlinger for å sikre at en virksomhet som er tildelt et felles sikkerhetssertifikat eller en sikkerhetstillatelse opprettholder sikkerhetsstyringssystemet sitt, slik at det styrer risiko effektivt under hele gyldighetsperioden til sikkerhetssertifikatet, i tillegg til en rekke andre spesifikke oppgaver angitt i CSM Supervision (2018/761) (heretter kalt «felles sikkerhetsmetode for tilsyn»). For å utføre tilsyn bør NSA-en sikre at det benyttes kompetent personell og at deres kompetanse opprettholdes gjennom et kompetansestyringssystem.

Felles sikkerhetsmetoden for tilsyn følger kravene i sikkerhetsdirektivet (EU) 2016/798 om behovet for at NSA-ene fører tilsyn med jernbanevirksomheter innenfor sitt myndighetsområde når et felles sikkerhetssertifikat eller en sikkerhetstillatelse har blitt tildelt.

Artikkel 17 i direktiv 2016/798 krever at NSA-er kontinuerlig overvåker virksomhetenes overholdelse av myndighetskrav i henhold til artikkel 9 i samme direktiv om at jernbanevirksomheter bruker et sikkerhetsstyringssystem (SMS). Ved gjennomføring av tilsyn må NSA-ene sørge for at tilsynsaktivitetene inkluderer:

- *Overvåking av hensiktsmessigheten av jernbanevirksomhetenes bruk av SMS, delvis eller som en helhet*
- *Overvåking av korrekt anvendelse av relevante felles sikkerhetsmetoder (CSM-er) av jernbanevirksomhetene i deres SMS, inkludert tilfeller der jernbanevirksomheten er en enhet med ansvar for vedlikehold (ECM) av egne kjøretøyer som ikke er sertifisert i samsvar med ECM-forskriften*
- *Overvåking av at interoperabilitetskomponenter innen sitt virksomhetsområde overholder vesentlige krav i henhold til artikkel 8 i interoperabilitetsdirektivet, (EU) 2016/797, gjennom jernbanevirksomhetens SMS.*

Etter utfallet av tilsynet kan NSA-ene utføre forholdsmessig utøvelse av myndighet (f.eks. midlertidige sikkerhetstiltak) for å sikre juridisk overholdelse, identifisere muligheter for forbedring av nasjonal lovgivning, og informere interessentene om endringene i sikkerhetsregelverket, samt eventuelle nye risikoforhold eller økning av risiko i sine medlemsstater.

Tilsynet vil normalt bli utført på språket til den medlemsstaten der tilsynet finner sted, med mindre det er enighet mellom den relevante NSA-en for driftsområdet og virksomheten som får tilsyn om at et annet språk skal brukes.

1.3 Hvem er denne veilederen for?

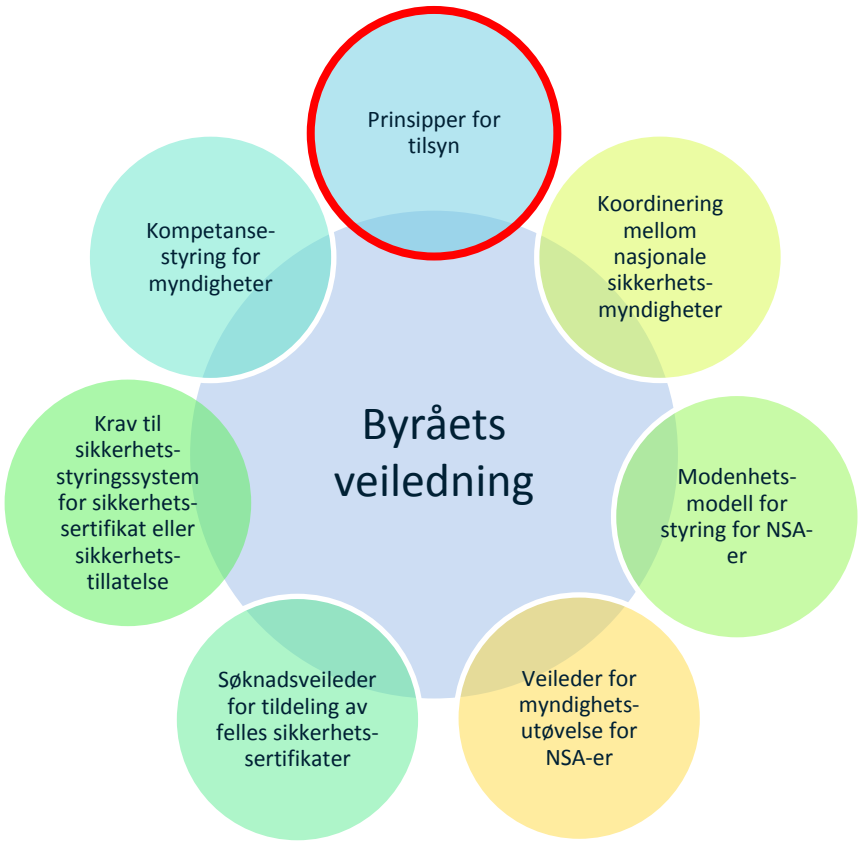
Denne veilederen er først og fremst ment for NSA-er for å hjelpe dem med å oppfylle kravene til den felles sikkerhetsmetoden for tilsyn etter tildeling av felles sikkerhetssertifikat eller sikkerhetstillatelse. Veilederen er også tilgjengelig for de som det føres tilsyn med, slik at de kan se hva de kan forvente under samarbeidet med en NSA, noe som vil hjelpe dem å planlegge og organisere seg i forhold til tilsynene.

1.4 Omfang

Denne veilederen gir detaljert praktisk informasjon for å øke forståelsen av kravene om tilsyn fastsatt i EUs juridiske rammeverk.

1.5 Veilederens struktur

Dette dokumentet er en del av Byråets samling av veiledere til hjelp for jernbanevirksomheter, nasjonale sikkerhetsmyndigheter og Byrået ved utføring av deres roller og oppgaver i samsvar med sikkerhetsdirektivet (EU) 2016/798.



Figur 1: Byråets samling av veiledere

1.6 Hvem skal det føres tilsyn med?

Det er NSA-ene som skal føre tilsyn med de virksomhetene som har et felles sikkerhetssertifikat eller en sikkerhetstillatelse. De gjør dette for å kontrollere at disse virksomhetene leverer i tråd med søknaden om et felles sikkerhetssertifikat eller sikkerhetstillatelse om å opprettholde et SMS som styrer risiko.

Innhold

2. Definisjoner

Følgende definisjoner brukes i denne veilederen:

Relevante interessenter

Relevante interessenter betyr alle som har en rolle i, eller er berørt av, jernbanedrift, og som har interesse for sikkerhetsresultater, f.eks. bransjeorganer, passasjerorganisasjoner eller lokale myndigheter.

Unødvendig ulempe

Dette betyr ganske enkelt at hvis du reiser til en jernbanevirksomhet for å utføre tilsyn, blir arbeidet koordinert på en slik måte at jernbanevirksomheten ikke har to forskjellige sett med tilsyn som krever at de samme personene må intervjues på samme tid, eller at det ikke er flere tilsynsbesøk i samme tidsrom fra forskjellige personer fra samme avdeling. Dette handler om å planlegge nødvendige tiltak på den mest effektive måten, slik at arbeidet blir gjort innenfor en fornuftig tidsramme uten å forårsake større forstyrrelse av virksomheten som det føres tilsyn med.

Styring

Med styring menes prosessene og prosedyrene for sikkerhetsstyringssystemet som er innført av jernbanevirksomheten for å styre sikkerhet og for å oppnå sikkerhetsmål, samtidig som juridiske forpliktelser og andre krav som er relevante for sikkerhet overholdes.

Alvorlige avvik

Alvorlige avvik er et problem som er identifisert av en NSA der avviket fra det som forventes er slik at korrigerende tiltak må gjennomføres etter pålegg fra NSA-en. I tilfeller som berører den myndighet som har utstedt det felles sikkerhetssertifikat/-tillatelse må tilbakekall eller begrensning av det felles sikkerhetssertifikat vurderes.

Andre forhold som må vurderes

Andre forhold som må vurderes er forhold hvor NSA-en ved tilsyn har identifisert et avvik, uten at dette er alvorlig nok til at det må gjennomføres direkte tiltak, men er alvorlig nok til at NSA-en må registrere det de har funnet og varsle virksomheten som det føres tilsyn med om behovet for korrigering. Informasjonen i begge kategoriene identifisert av NSA-en skal sendes til den som har utstedt det felles sikkerhetssertifikat innen en forsvarlig tidsramme etter at en søknad om et enkelt sikkerhetssertifikat har blitt sendt, slik at eventuelle problemer rundt mangel på overholdelse kan vurderes av dette organet.

3. Risikobasert tilsyn

Det er mulig å identifisere noen hovedområder som er av betydning for at risikobasert tilsyn skal kunne fungere hensiktsmessig. Disse er:

- *NSA-en må ha en helhetlig forståelse av risikoene innenfor det nasjonale jernbanesystemet og hvilke av disse som er mest betydelige;*
- *NSA-en må ha en god forståelse av styringsevnen til jernbanevirksomheter (og tilhørende aktører) for å kontrollere risikoen;*
- *NSA-en må ha personale med kompetanse til å kunne dømme på tvers av punktene ovenfor, og fleksible nok til å tilpasse tilnærmelsesmåten sin hvis de ser at risikoen øker eller reduseres (se Byråets veileder om kompetansestyring for myndigheter);*
- *NSA-en bør hente informasjon fra et så bredt utvalg av kilder (både innen og utenfor jernbanen) som mulig når de skal fatte beslutninger om risikobasert tilsyn;*
- *NSA-en må kunne begrunne de beslutningene de tar i forhold til hva de fører tilsyn med og hva de ikke fører tilsyn med;*
- *NSA-en må kunne imøtekomme andre tilsynsdrivere i medlemsstaten, slik som politiske beslutninger eller samfunnsmessige bekymringer som kanskje ikke er risikobaserte;*
- *Tilsynet må være knyttet til prosessene ved tildeling av felles sikkerhetssertifikat og sikkerhetstillatelse slik at de operatørene eller aktivitetene innen drift som anses å ha større risiko, får mer tilsyn umiddelbart etter tildeling av felles sikkerhetssertifikat eller sikkerhetstillatelse.*
- *Tilsynet som utføres, må gjøre det mulig for NSA-en å forsikre seg om at jernbanevirksomhetens sikkerhetsstyringssytem er i stand til å håndtere risikoene de møter.*

Ved å implementere prinsippene beskrevet ovenfor bør NSA-ene ha tilstrekkelig kunnskap (kvantitative, semi-kvantitative eller kvalitative) til å forstå risikoen innenfor medlemsstaten. Dette er avgjørende for å utvikle tilsynsstrategien. Uten en klar idé om risikoen man står overfor, er det umulig å ta forholdsmessige og målrettede beslutninger om hva som bør føres tilsyn med og hvordan dette kan gjøres på best mulig måte. En manglende forståelse av risikoene i systemet innebærer også at man i samtaler mellom staten og NSA-en går glipp av muligheten til tilstrekkelig vurdering av hvilke forbedringer i sikkerheten som kan håndteres med tilgjengelige ressurser. NSA-ens evne til å klargjøre for medlemsstaten hvor forbedringer innen sikkerhet bør rettes vil være nyttig input til medlemsstaten i å skape rom for sikkerhetsforbedringer. Forståelsen av sikkerhetsrisikoen i systemet er effektivt utgangspunktet for en forretningssak for sikkerhetsforbedring for å redusere den risikoen.

Det er også verdt å merke seg at NSA-ens forståelse av risikoen i medlemsstaten ikke bør være for ulik den som nasjonal infrastrukturforvalter har. Man vil for eksempel forvente at infrastrukturforvalteren og NSA-en har en lignende oppfatning av nivået av samlet risiko fra planoverganger i medlemsstaten. Hvis infrastrukturforvalterens og NSA-ens oppfatning er svært forskjellig, kan dette være en indikasjon på feil i systemet som styrer risiko.

Med hensyn til måten man kommer frem til en oppfatning av risikoene i medlemsstaten, ville det være nyttig på et europeisk nivå om det var konvergens mot en standardmetode for å oppnå dette. På nåværende tidspunkt er det imidlertid detaljerte forskjeller, selv blant de landene som bruker lignende tilnærminger, som gjør det vanskelig å sammenligne på et europeisk nivå. Nåværende tilnærminger varierer fra ekstremt sofistikerte til svært enkle, og dette kan være en gjenspeiling av modenheten til medlemsstatens jernbanesystem når det gjelder bruk av den europeiske tilnærmingen, deres størrelser og ulike kulturelle forutsetninger.

For å vurdere evnen til de ulike aktørene i jernbanesystemet når det gjelder risikostyring, er det nødvendig at NSA-en er i stand til å bruke tilsyn for å avgjøre hvor effektive sikkerhetsstyringssystemene er i virksomhetene de fører tilsyn med. For de fleste NSA-er vil dette i praksis avhenge av ansettelse av opplærte og kompetente inspektører som er i stand til å utføre disse vurderingene.

NSA-ene må kunne bruke informasjon fra så mange kilder som mulig for å kunne kryssjekke informasjon og unngå å stole på ett datasett for å beslutte tilsynsprioriteringer. NSA-ene oppfordres også til å bruke informasjon om risikostyring fra utenfor jernbanebransjen der det er hensiktsmessig, for å bekrefte funn og fremdrive forbedringer innen sikkerhetsstyringsprosesser. Det vil være datasett eller informasjonskilder som vil være av særlig relevans, slik som ulykkes- eller hendelsesdata, selskapets daglige logger og utdata fra risikomodeller i medlemsstaten som kan benyttes hvis de er tilgjengelige. Annen informasjon fra klager eller bekymringer som kommer fra almenheten eller akademisk studier bør imidlertid også betraktes som nyttig informasjon ved utvkling av en risikobasert tilsynsstrategi og plan.

I samsvar med artikkel 7 i felles sikkerhetsmetode for tilsyn bør NSA-ene ha et sett med kriterier for hvem det skal føres tilsyn med og hvorfor. Dette settet med kriterier er knyttet til oppnåelse av strategien. Formålet med dette er å sørge for at det tas en konsekvent tilnærming for alle tilsynsaktiviteter, og at de ulike aktørene forstår hvorfor bestemte aktiviteter vurderes og hvilke kriterier de måles opp mot.

TSI OPE krever også at NSA-er, som en del av tilsynsstrategien og planen, fører tilsyn med hensiktsmessig overholdelse (ettersom TSI OPEomhandler prosessen og reglene som bidrar til sikker togdrift) i deres daglige utføring av tilsyn av SMS-ene til virksomhetene de regulerer. Veileder utgitt av Byrået om anvendelse av de grunnleggende driftsprinsippene (Fundamental Operating Principles) som er beskrevet i TSI OPE, skal bistå NSA-ene ved utføring av tilsyn innen dette området.

NSA-er kan også oppleve press fra eksterne kilder som ikke er risikobaserte. Disse kan skyldes en bekymring fra offentligheten om et aspekt av jernbanedriften, slik at det blir politisk nødvendig å løse problemet. Det er mulig at dette stemmer overens med tilsynsstrategien og tilsynsplanen, eller at det ikke gjør det, men det må gjøres rede for i begge. Slike problemer kan ha stor positiv innvirkning på sikkerheten. En medlemsstat kan for eksempel bestemme seg for å fjerne alle planoverganger innenfor sitt territorium innen 10 år, mens den risikobaserte tilnærmingen kanskje ikke ser alle overgangene fjernet, men oppgradert med moderne beskyttelsessystemer. Det er klart at hvis overgangene forsvinner helt om ti år, vil dette være en betydelig økning i sikkerheten for medlemsstaten. Omvendt kan en NSA oppleve press på grunnlag av anvendelse for å beholde planoverganger der en risikobasert tilnærming vil tilsi at de fjernes.

Det er avgjørende at risikobasert tilsyn er knyttet til resultatene fra vurderingene for sikkerhetssertifikatet og sikkerhetstillatelsen. Dette fordi vurderingen for sertifikatet bare gjelder teoretisk bruk av sikkerhetsstyringssystemet for aktiviteten til en jernbanevirksomhet. Hvorvidt bruken fungerer i praksis er et tema som må tas opp under tilsynet. For eksisterende jernbanevirksomheter med lang historie i bransjen kan tilsynet struktureres likt over sertifikatets levetid. For nye deltakere i systemet kan det være hensiktsmessig å øke tilsynet ved starten av sertifikatets levetid eller å målrette aktiviteter på bestemte elementer i sikkerhetsstyringssystemet for å sikre at det som er skrevet på papir virkelig blir satt i bruk på en hensiktsmessig måte. For både eksisterende selskaper og nyinntredere er det viktig at overvåkingsvirksomheten blir utsatt for risiko på grunnlag av risiko.

Siden ressursene for tilsyn i NSA-ene ofte er knappe, er det avgjørende at spørsmålet om hvor tilsynet vil være mest verdifullt er adressert ved å bestemme hva som skal føres tilsyn med og hvorfor på et risikobasert grunnlag. For eksempel kan det være at infrastrukturforvalteren er oppmerksom på problemer rundt ødelagte skinner og har et program på plass for å ta hånd om dette. Det er kanskje ikke den beste bruken av ressurser at NSA-en bruker mye tid på dette. I stedet kan NSA-en velge å sette fokus på et område der det oppfattes at infrastrukturforvalteren ikke ser ut til å styre problemet.

4. Tilsynsstrategi

Artikkel 3 i felles sikkerhetsmetode for tilsyn krever at NSA-ene har en tilsynsstrategi som inneholder elementene som er angitt i vedlegg I til den felles sikkerhetsmetoden. En foreslått mal for en tilsynsstrategi er angitt i Vedlegg til denne veilederen. Overskriftene i malen muliggjør en konsistent tilnærming til utviklingen av tilsynsstrategier på tvers av alle medlemsstatene for å utvikle tillit mellom NSA-ene om at sikkerhetsnivåene opprettholdes. I tillegg, ettersom Byrået spiller en rolle i overvåkingen av NSA-enes ytelse, vil en felles struktur for slike strategier hjelpe ved utøvelsen av denne funksjonen.

4.1 Bakgrunn

Når bakgrunnen skal beskrives vil det være tilstrekkelig med en grunnleggende beskrivelse av størrelsen på jernbanenettet i medlemsstaten, inkludert antall jernbanevirksomheter. Dette avsnittet bør også omtale varigheten til tilsynsstrategien og rutinen for å gjennomgå den.

4.2 Mål

Målet bør referere til formålet med strategien, for eksempel «å jobbe med bransjen for kontinuerlig å forbedre resultatene til sikkerhetsstyringen». Dette avsnittet bør også inkludere referanse til hvordan målet oppnås.

4.3 Tilsynsprinsipper

Prinsippene er en gjentagelse av NSAs forpliktelse til nøkkelverdiene som sikrer at beslutningstakingen under tilsynet er tydelig, men rettferdig. Vedlegg I til felles sikkerhetsmetode for tilsyn beskriver at ved opprettelsen av tilsynsstrategien og planen(e) som følger av den, skal NSA-en samle og analysere data/informasjon fra en rekke kilder. Kilder inkluderer informasjon fra vurdering av sikkerhetsstyringssystemer, resultater fra tidligere tilsynsaktivitet, relevant informasjon fra kjøretøytillatelser, rapporter fra havarikommisjonen (NIB-er), andre ulykkes- eller hendelsesdata, årlige sikkerhetsrapporter fra jernbanevirksomheter, rapporter fra enheter med ansvar for vedlikehold, klager fra offentligheten og andre relevante kilder. I hovedsak bør NSA-en ta relevant informasjon fra ethvert sted den er å få tak i for å finne ut hvor de viktigste risikoområdene er innenfor medlemsstatens jernbane. De må vurdere og analysere tilgjengelig informasjon for å avgjøre hvilke problemer som er mest betydelige, og deretter utarbeide en strategi som adresserer disse problemene med en plan for å identifisere hvordan og over hvilken periode strategien skal leveres. NSA-en må både utarbeide hvilke ressurser som kreves for å levere denne foreslåtte strategien og planen, og tildele tilstrekkelige ressurser for å levere den. Til slutt må NSA-en adressere eventuelle problemer i strategien og planen som vedrører drift over grenser eller infrastruktur, og koordinere med andre NSA-er etter behov.

Tilsynsprinsippene som NSA-en bør bruke kommer hovedsakelig fra vedlegg I i felles sikkerhetsmetode for tilsyn. NSA-ene bør planlegge tilsynsaktivitetene gjennom en framgangsmåte basert på tydelighet og rettferdighet. Tilsynsprinsippene er utformet for å hjelpe NSA-ene å oppnå dette.

NSA-ene bør anvende **proporsjonalitetsprinsippet** mellom myndighetsutøvelse og risiko. Tiltak som tas av en NSA for å oppnå overholdelse eller holde jernbanevirksomheter og infrastrukturforvaltere ansvarlig for manglende oppfyllelse av juridiske forpliktelser, bør stå i forhold til eventuell sikkerhetsrisiko eller den potensielle alvorlighetsgraden av den manglende overholdelsen, inkludert eventuell faktisk eller potensiell skade. Dette prinsippet er avgjørende for NSA-er da de ved å vedta denne tilnærmingen demonstrerer overfor dem de regulerer at de bruker loven på en tydelig og rettferdig måte. Dette reduserer den potensielle

frykten i regulerte virksomheter om at feil vil bli utsatt for drakonisk straff fra NSA-en, noe som igjen skaper en kultur for hemmelighold og frykt som ikke fremmer robust risikostyring.

NSA-ene bør anvende prinsippet om en **konsekvent** tilnærming for å sikre at en NSA tar en lik tilnærming under like omstendigheter for å oppnå like mål. Jernbanevirksomheter ønsker å bli behandlet på samme måte av forskjellig personell som utfører tilsyn innen en NSA, og av forskjellige NSA-er der det er grenseoverskridende ordninger. Dette gir dem pålitelighet og lar dem planlegge bedre. Det adresserer også problemer rundt sikkerhetskulturen, og reduserer jernbanevirksomhetenes frykt overfor NSA-ene.

NSA-enes tilsynsaktivitet bør hovedsakelig **rettes** mot de aktiviteter som en NSA mener medfører størst risiko eller hvor farene er minst styrte. For å gjøre dette bør den nasjonale sikkerhetsmyndigheten ha metoder og verktøy for å vurdere resultatene av sikkerhetsstyringen til jernbanevirksomhetene. I en situasjon der ressursene er knappe og kravene til NSA-ene er mange, er det viktig at fokus legges på de største risikoene. Metodene for dette er NSAs analyse av resultatene av sikkerhetsstyringen til jernbanevirksomhetenes ledelse.

NSA-ene bør avgjøre hva de vil prioritere, slik at de bruker **ressursene** hensiktsmessig, men avgjørelsen om hvordan dette gjøres best bør være hver enkelt NSAs ansvar. Oppfølgingen bør fokusere på dem som er ansvarlige for risikoen og som er best egnet til å kontrollere den. NSA-ene har knappe ressurser, så det er viktig at disse brukes klokt for å maksimere NSA-enes effektivitet ved å sørge for at de ansvarlige styrer risiko på en hensiktsmessig måte.

NSA-ene bør anvende prinsippet om **åpenhet** for å hjelpe jernbanevirksomhetene å forstå hva som forventes av dem (inkludert hva de bør eller ikke bør gjøre), og hva de kan forvente fra NSA-en. For jernbanevirksomhetene er det ekstremt viktig at de forstår hvordan en NSA tar beslutninger, slik at de kan forstå hva det sannsynlige resultatet vil være dersom de ikke styrer risiko på en hensiktsmessig måte.

NSA-ene bør være **ansvarlige** for sine vedtak i samsvar med artikkel 18(3) i sikkerhetsdirektivet. NSA-ene skal derfor ha interne retningslinjer som sørger for at de bør kunne holdes ansvarlig. Videre skal NSA-ene også ha en klageprosedyre. NSA-ene må ta beslutninger, og noen av disse vil ha en negativ virkning på jernbanevirksomheter som ikke styrer risiko på en hensiktsmessig måte. Det er viktig at NSA-ene har klare kriterier for hvordan disse beslutningene skal tas, slik at det klart fremkommer hvordan de ble tatt. Det er også svært viktig at det er en prosess for å utfordre slike avgjørelser der en virksomhet føler at NSA-en har gått utover det de har rett til eller ikke har fulgt den rette prosessen.

NSA-ene bør utvikle **samarbeidsordninger** med andre kompetente myndigheter for å dele informasjon og utvikle enhetlige tilnærminger til problemer som påvirker jernbanesikkerheten. NSA-ene må ha prosesser for å dele relevant informasjon med hverandre og med andre kompetente myndigheter. Dette er avgjørende for å sikre at riktig handling tas av rett organ der det er nødvendig.

Hvis en NSA følger disse prinsippene, vil dem det føres tilsyn med behandles rettferdig og, der det er hensiktsmessig, med strenghet. Det bør også påpekes at disse prinsippene er komplementære, dvs. de fungerer sammen for å vise at NSA-en til de virksomhetene den regulerer som en kompetent og tydelig myndighet som tar gode beslutninger på en åpen og ærlig måte. Det skal bemerkes at tilsynsstrategimalen i vedlegget til denne veilederen også beskriver disse prinsippene. Dette er fordi denne strategien er ekstremt viktig for å sette standarden på hvordan tilsynet skal utføres, og ved å reprodusere prinsippene her vil NSA-en styrke sin forpliktelse og kunne fremlegge bevis på åpenhet i tilnærmingen sin.

Byrået har også laget en *veileder for myndighetsutøvelse* som kan brukes av dem som utfører tilsyn. Den reflekterer prinsippene som er beskrevet ovenfor. Veilederen tar prinsippene og bruker dem i en matrise som er ment å være til veileder for dem som utfører tilsyn, vedrørende beslutninger om hvordan myndighetsutøvelse bør være ut fra en analyse av risikogapet. Jo større risikogapet er, dvs. mellom det som forventes av en virksomhet dersom alle var oppfylt og den faktiske oppfyllelsen, desto større bør man forvente beslutningen om myndighetsutøvelse å være.

4.4 Organisering av tilsyn

Organiseringen av tilsyn bør generelt dekke NSA-ens styringsstruktur og bemanning, inkludert hvordan samhandlingen med sikkerhetssertifisering og sikkerhetstillatelse styres. NSA-en bør være åpen om styringsstrukturen sin og måten tilsynsproblemer eskaleres etter behov, fra operasjonell til et høyere nivå, inkludert, hvor det er hensiktsmessig, for beslutninger om myndighetsutøvelse. NSA-en bør også være åpen om hvordan beslutninger tas om å regulere risiko innen ett område mer enn et annet. NSA-en bør angi bemanningen og generelt sett hvordan den vedlikeholder kompetansen (se *Byråets veileder om kompetansestyring for myndigheter*), samt på hvilket grunnlag personalet anvendes. NSA-en bør også angi hvordan den har til hensikt å måle ytelsen av sikkerhetsstyringssystemene som en del av tilsynsaktivitetene, for eksempel ved bruk av en modenhetsmodell for styring eller sikkerhetskultur eller andre metoder. Byrået har utviklet en veileder for modenhetsmodell for styring som kan benyttes av både myndigheter og virksomheter til dette formål (se også *Byråets veileder om modenhetsmodell for styring*).

Ett av hovedproblemene for NSA-en er måten nye aktører på markedet styres på, da det ikke foreligger historisk informasjon om kvaliteten til deres sikkerhetsstyringssystem. Dette har ført til at noen NSA-er gir nye aktører på jernbanemarkedet et sikkerhetssertifikat med kortere gyldighetsperiode enn 5 år. Andre NSA-er har besluttet å utføre en mer omfattende revisjon av en ny aktør før de utsteder et sikkerhetssertifikat eller å utføre en slik revisjon umiddelbart etter utstedelsen. Enhver begrenset gyldighetsperiode må begrunnes med at det er nødvendig for å sikre effektiv kontroll av risikoer som påvirker jernbanevirksomhetens sikkerhet. NSA-ene kan utføre en mer detaljert undersøkelse av nye aktører etter sertifisering for å sikre at organiseringen av sikkerhetsarbeidet deres er egnet til formålet. NSA-en bør klart angi dette i sin tilsynsstrategi og sine planer for tilsyn.

4.5 Risikonivå innenfor medlemsstaten

Det neste avsnittet om risikonivå i medlemsstaten bør omhandle grunnlaget for hvordan man har kommet fram til det, f.eks. ved bruk av risiko- og/eller modenhetsmodeller, samt eventuelle problemer med at visse risikoer er dekket i strategien, og andre ikke er det.

4.6 Strategiske prioriteringer for tilsyn

Følgende avsnitt bør omhandle hvordan strategiske prioriteringer fastsettes. Disse bør dekke:

- *Hvordan det skal føres tilsyn med sikkerhetsstyringssystem. Her bør NSA-en beskrive tilsynsformene (se avsnitt 4.7 nedenfor) som mest sannsynlig vil bli brukt, og hvorfor noen områder prioriteres fremfor andre.*
- *Hvordan samordnet og/eller felles tilsyn med andre NSA-er vil bli utført, hvis hensiktsmessig (se avsnittet om samordnet tilsyn og samarbeid nedenfor);*
- *Risiko på høyere nivå. For dette punktet forventes det at NSA-en synliggjør det de mener er de høyeste sikkerhetsrisikoene i systemet og hvordan de har kommet frem til disse;*
- *For lavere risikonivå vil det gjennomføres generelle tilsyn. For dette punktet forventes det at NSA-en synliggjør det den vurderer å være risikoer på neste (lavere) nivå, samt angi hvorfor de har kommet frem til disse.*

4.7 Tilsynsmetodikk

Artikkel 4 i felles sikkerhetsmetode for tilsyn krever at NSA-ene tilpasser hensiktsmessige metoder og synliggjør disse metodene ved planlegging av tilsynsaktivitetene. Tilsynsmetoder har en bred betydning som omfatter både innsamling av informasjon (en relatert aktivitet) for å undersøke sikkerhetsresultatene fra styringssystemet, og refererer direkte til bestemte aktiviteter, slik som å intervjue personer. Ettersom tilsyn med jernbanevirksomheter når det gjelder å sikre overholdelse med EUs og nasjonal lovgivning er en bred oppgave for NSA-en, finnes det tilsvarende mange forskjellige tilnærminger som kan brukes til å samle inn opplysninger om nivå av overholdelsen. Alle disse tilnærmelsene involverer imidlertid innhenting av informasjon på ulike måter, etterfulgt av en analyse av hva den forteller om sikkerhetsstyringssystemet til virksomheten som det føres tilsyn med og dens nivå av overholdelse av loven.

Det finnes flere spesifikke teknikker som kan brukes ved gjennomføring av tilsyn på eller utenfor virksomhetens geografiske plassering. Disse inkluderer:

- *Inspeksjon av fysiske aktiva på området, slik som kjøretøy eller infrastrukturelementer;*
- *Inspeksjon av sikkerhetsstyringsprosedyrer og dokumentasjon for å sikre at de er tilpassede og hensiktsmessige;*
- *Intervjuer med ansatte på alle nivåer i en jernbanevirksomhet for å identifisere deres forståelse av hvordan prosedyrer og regler etterleves i praksis, og å gjøre en vurdering av virksomhetens sikkerhetskultur;*
- *Revisjoner av en definert styringssystemstandard, f.eks. OHSAS 18001:2007;*
- *Revisjoner av en modell definert av NSA-en;*
- *Revisjoner/inspeksjoner av en aktivitet eller prosess etter en hendelse;*
- *Sikkerhetsstyringsevne-/modenhetsrevisjoner;*
- *Dataanalyse;*
- *Stikkprøver av produkter eller aktiviteter;*
- *Oppgaveobservasjon (f.eks. reise i førerhus for å observere føreradferd);*
- *Deltakelse av NSA på viktige møter i ledelsen i -en jernbanevirksomhet (f.eks. om planoverganger eller nye infrastrukturprosjekter).*
- *Undersøkelser av virksomheter som krever ferdigstillelse av spørreskjemaer for selvvurdering, f.eks. for vurdering av sikkerhetskultur eller overholdelse av lovgivning eller sjekklister;*
- *Eventuelle andre relevante aktiviteter som skal legges til summen av NSAs kunnskap om en bestemt jernbanevirksomhet, deres sikkerhetsstyring og sikkerhetskultur.*

I denne veiledning menes med:

- ***Inspeksjon** betyr bruk av autoriserte og kompetente personer innen NSA-en for å undersøke et bestemt og begrenset aspekt av aktiviteten til en jernbanevirksomhet. En inspeksjon skal ha til formål å fastslå overholdelse med europeisk og nasjonal lovgivning, eller for å verifisere at det som er opplyst eller registrert i dokumenter som støtter sikkerhetsstyringssystemet, faktisk skjer i praksis. En inspeksjon i denne sammenhengen både verifiserer at prosessen er etablert og hvor godt den fungerer. Det betyr ikke «avkrysningsboks-verifisering» for at bestemte dokumenter eller utstyr ettersom dette kun kan fortelle inspektøren at noe eksisterer men at det ikke brukes i praksis*
- ***Revisjoner** betyr strukturelle inngripener hvor jernbanevirksomheten undersøkes mot en bestemt sikkerhetsstyringsstandard eller revisjonskriterier.*

- ***Revisjoner av modenhetsmodell for sikkerhetsstyringsevne*** *er en strukturert metode for å utføre en revisjon av sikkerhetsstyringssytemet til virksomheten ved hjelp av en styringsevne-/modenhetsmodell for å undersøke hvor hensiktsmessig sikkerhetsstyringen er (se også Byråets veileder om modenhetsmodell for styring). En slik modell kan gi et bilde av ytelsen til sikkerhetsstyringssystemet hvis den brukes riktig av kompetent tilsynspersonale. Den kan være et nyttig verktøy for en NSA å bruke for å gi informasjon om hvordan et bestemt sikkerhetsstyringssytem fungerer til sikkerhetssertifiseringsorganet når en søknad om fornyelse blir vurdert.*

Metodene som benyttes, slik som intervjuer, dokumentgjennomgang eller verifikasjoner, kan utføres i større eller mindre dybde over et mindre eller større utvalg av prosesser og blandes for å gi et bilde av virksomhetens sikkerhetsresultat, så vel som å identifisere underliggende mangler.

Intervjuer med enkeltpersoner, undersøkelser av dokumenter og verifikasjonsinspeksjoner kan da brukes til å danne en vurdering av virksomhetens styringsmodenhet og systemets evne til å kontrollere risikoen det står overfor. Den kompetente personen som utfører revisjonen bruker deretter sin egen vurdering ved hjelp av en styringsevne- eller modenhetsmodell for å vurdere hvor godt virksomhetens sikkerhetsstyringssystem er til å styre sikkerhet.

Oppgaveobservasjon og deltakelse på styremøter er aktiviteter som øker NSA-ens kunnskap om en bestemt jernbanevirksomhet og dens sikkerhetskultur.

For en NSA foreslås bruk av en blanding av tilsynsmetoder som det ideelle. Hver NSA bør ta sikte på å oppnå en god balanse mellom top-down-aktivitet (revisjon av sikkerhetsstyringssystemet) og bottom-up-aktivitet (inspeksjoner på området for å observere hva som skjer). Tilsynstilnærminger kan trekke sammen eksisterende inspeksjonsaktiviteter og blande dem med revisjoner av sikkerhetsstyringssystemer for å innhente informasjon om styringen. Dette vil oppheve noen av svakhetene med enkelte metoder og skape et mer realistisk samlet bilde av hvordan resultatet til den det føres tilsyn med fungerer i praksis.

Metodene beskrevet ovenfor kan også brukes av NSA-en til å utføre undersøkelser på tvers av grensesnittene mellom jernbanevirksomheter for å få et samlet bilde på medlemsstatsnivå av hvordan ulike problemer styres innen jernbanen.

Tabellen og figuren nedenfor viser hvordan generelle inspeksjoner og styringssystemrevisjoner henger sammen, spesielt intervjuteknikker, gjennomgang av dokumentasjon og observasjon. Disse metodene finnes i standarder, slik som ISO 19011 om «Retningslinjer for revisjon av styringssystemer», og NSA-ene kan fritt velge om de ønsker å oppfylle kravene i standarden eller ikke. Tabellen nedenfor viser hvilke metoder som er knyttet til ulike typer aktiviteter.

Tabell 1 : Forholdet mellom on- og off-site i styringssystemrevisjoner og inspeksjoner

	Aktivitet on-site	*Aktivitet off-site*
Interaksjon med mennesker	Gjennomføre intervjuer. Utfylle sjekklister og spørreskjemaer med deltakelse fra revidert part. Utføre dokumentgjennomgang med deltakelse fra revidert part. Prøvetaking	Via interaktiv kommunikasjon betyr: • gjennomføre intervjuer; • utfylle sjekklister og; • spørreskjemaer; • utføre dokumentgjennomgang med deltakelse fra revidert part.
Begrenset/Ingen interaksjon med mennesker	Utføre dokumentrevisjon (f.eks. registreringer, dataanalyse). Observasjon av arbeid utført. Besøk on-site. Utfylle sjekklister. Prøvetaking (f.eks. produkter).	Utføre dokumentrevisjon (f.eks. registreringer, dataanalyse). Observasjon av arbeid utført med metode for overvåking som tar sosiale og juridiske krav i betraktning. Analysere data.

4.8 Tilsynsplan(er)

Tilsynsplanen(e) bør levere den praktiske anvendelsen av tilsynsstrategien for gyldighetsperioden til denne strategien. Fordi tilsynsplanen er avledet fra tilsynsstrategien, bør den være basert på risikoene som er identifisert og som behøver følges opp ved bruk av tilsyn i tilsynsstrategien. Tilsynsplanen bør også fremheve hvordan tilknytningen mellom vurderingsprosessen for sikkerhetssertifiseringen og -tillatelsen og tilsynsprosessen for jernbanevirksomheter sikkerhetssertifikatets eller -tillatelsens levetid vil fungere, inkludert, om nødvendig, behovet for å samordne med Byrået når det er sikkerhetssertifiseringsorganet og med andre NSA-er. Tilsynsplanen bør inneholde informasjon om prosessen for hvordan den opprettes og gjennomgås, og tilknytningen til tilsynsstrategien, inkludert hvordan resultatene fra planen resulterer i endringer i strategien. Tilsynsplanen bør spesifisere hvilke jernbanevirksomheter det skal føres tilsyn med i det året planen gjelder, samt begrunnelsen for dette tilsynet. Ressursene som skal tildeles tilsyn bør spesifiseres i tilsynsplanen. Tilsynsformene/-metodene som skal brukes under tilsynet bør også angis. Der

tilsynsplanen adresserer problemer rundt menneskelige faktorer, bør NSA-en se i jernbanevirksomhetenes SMS-er på hvordan disse sakene styres.

4.9 Myndighetsutøvelse

De felles sikkerhetsmetodene for tilsynet nevnt i artikkel 7 (1) at den nasjonale sikkerhetsmyndigheten må ha kriterier for håndtering av manglende overholdelse som er påvist i sikkerhetsstyringssystemet til jernbaneforetaket eller infrastrukturforvaltningen, og i vedlegg 1 fastslår at en nasjonal sikkerhetsmyndighet bør treffe håndhevingstiltak dersom det er relevant. Dette tiltaket vil avhenge av hvilke sanksjoner hver enkelt nasjonal lovgivning tillater for å ta. I forbindelse med de felles sikkerhetsmetodene for tilsyn vil feil være tilfeller der jernbaneforetakets eller infrastrukturforvaltningens SMS ikke oppfyller det viktigste kravet om å kontrollere risikoer. De sanksjonene som en nasjonal sikkerhetsmyndighet kan få anvendelse på, bør bygge på de sentrale prinsippene for tilsyn (se nr. 4.3).Den nasjonale sikkerhetsmyndigheten skal vise at alle tiltak de tar opp i forhold til, står i forhold til målet og rettet mot den antatt risiko. De felles sikkerhetsmetodene for tilsynet (artikkel 5 (2) a) som skiller spørsmål fra den nasjonale sikkerhetsmyndigheten bør ta hensyn til større tilfeller av manglende overholdelse og andre områder. De sanksjoner som en nasjonal sikkerhetsmyndighet kan søke å pålegge, bør gjenspeile nivået av manglende overholdelse eller bekymring. At organisasjonen håndheves på en måte som må kunne forstå hvorfor en sanksjon anvendes, og hvordan den kan forbedre seg. De nasjonale sikkerhetsmyndigheter kan bruke alle håndhevingstiltak som dekker de viktigste prinsippene for tilsyn for å gi en strukturert og åpen prosess for å treffe håndhevingstiltak i henhold til nasjonal lovgivning eller EU-lovgivning. For å bistå nasjonale sikkerhetsmyndigheter skal Byrået ha utviklet en veiledning, en forvaltningsmodell som kan brukes sammen med ulike nasjonale regler.(se Byråets veiledning om håndhevingen).

5. Henvisning av tilsynsinformasjon og gjensidig avhengighet til vurdering av felles sikkerhetssertifikat og kjøretøytillatelse

Det er klart at tilsyn er den måten en NSA forsikrer seg at en jernbanevirksomhets SMS er i tråd med det som er beskrevet i den opprinnelige søknaden om felles sikkerhetssertifikat eller sikkerhetstillatelse. Artikkel 17(5) i direktiv (EU) 2016/798 og vedlegg I til CSM om tilsyn beskriver dette tydelig, at hvis en NSA under tilsyn avdekker at en innehaver av felles sikkerhetssertifikat ikke lenger tilfredsstiller vilkårene for sertifisering, kan sikkerhetssertfikatet enten begrenses eller inndras eller be om at Byrået gjør det dersom det er Byrået som har tildelt sikkerhetssertifikatet (en strukturert metode for å arbeide gjennom dette er beskrevet i Byråets veileder for myndighetsutøvelse). I henhold til artikkel 17 (7) i samme direktiv skal den nasjonale sikkerhetsmyndigheten sikre at de strukturelle delsystemene er i samsvar med de grunnleggende krav og sikkerhetsgodkjenning til en infrastrukturforvaltning, kan begrenses eller tilbakekalles av det eller kontrollorganet dersom vilkårene for det ble utstedt, ikke lenger er oppfylt.

Artikkel 5 i CSM om tilsyn forklarer behovet for å utveksle informasjon som er innhentet under tilsyn med den delen av NSA-en som er ansvarlig for vurderingen av sikkerhetssertifikatet eller med Byrået for å fornye eller oppdatere et felles sikkerhetssertifikat eller sikkerhetstillatelse. Samme artikkel sier også at NSA-en skal sende til den myndigheten som har tildelt felles sikkerhetssertifikat eller NSA-en for grenseoverskridende infrastruktur relevant informasjon, inkludert minst:

a) *En beskrivelse av større mangel på overholdelse som kan påvirke sikkerhetsytelsen eller innebære alvorlige sikkerhetsrisikoer, samt ethvert annet problemområde identifisert under tilsynsaktiviteter. Denne informasjonen kan hentes fra rapporter fra revisjoner, Sikkerhet Management modenhet modell og inspeksjoner, og oppsummeres med henblikk på revurdering.*

b) *Status for handlingsplanen (eller planene) etablert av jernbanevirksomheten eller infrastrukturforvalteren for å løse større mangel på overholdelse, henvist til i punkt (a), og relevante tiltak som er tatt av den nasjonale sikkerhetsmyndigheten for overvåke løsning av disse problemene. Denne informasjonen kan hentes fra oppfølgingsrevisjoner, Sikkerhet Management modenhet modell og inspeksjoner;*

c) *En oversikt over sikkerhetsresultatene til jernbanevirksomheten som opererer i sin medlemsstat. Denne informasjonen kan hentes fra en modenhetsmodell (hvis aktuelt) eller fra en ekspertvurdering, som evaluerer sikkerhetsstyringssystemets ytelse og evne (dvs. hvor godt de oppfyller sine juridiske forpliktelser og kontinuerlig forbedrer håndtering av risikoene);*

d) *Statusen på handlingsplanen eller -planene som er fastsatt av jernbanevirksomheten for å løse gjenstående bekymringer fra tidligere vurdering.*

NSA-en gir den myndigheten som tildeler sikkerhetssertifikatet informasjon som er relevant for å forstå hvor godt SMS-et fungerer i praksis og om det finnes svake områder. Dette vil gjøre det mulig for å spisse vurderingsaktiviteten.

For å oppfylle disse kravene må NSA-en vurdere hvilken informasjon om virksomheten som reguleres er relevant under de fire overskriftene ovenfor. For punkt (a) er det klart at informasjonen skal inneholde problemer som er identifisert av NSA-en som er viktige for å styre risikoen (gjennom sikkerhetsstyringssystemet), og fra punkt (b) og (d) tiltakene og tidsplanene som er avtalt mellom partene for å løse problemene, enten frivillig av virksomheten selv eller gjennom tiltak fra NSA-en for å få virksomheten å rette opp i situasjonen. Punkt (c) krever at NSA-en leverer en detaljert beskrivelse av virksomhetens sikkerhetsytelse til sikkerhetssertifiseringsorganet eller NSA-en for grenseoverskridende infrastruktur. Dette kan gjøres for eksempel via en rapport om tilsyn som er utført på den aktuelle virksomheten eller ved å gi resultatene fra en styringsmodenhetsmodell for virksomheten som vil gi en oversikt over SMS-ets relative ytelse.

I tillegg til listen ovenfor kan følgende også gi en indikasjon på hvilken type informasjon som også kan være nyttig for den myndigheten som tildeler et sikkerhetssertifikat når det gjelder hvordan et SMS fungerer:

a) *Oversikt over de ulike tilsynene utført siden det tidligere tildelte sikkerhetssertifikatet eller sikkerhetstillatelsen, og oppfølging av NSAs anbefalinger som ble tatt opp som følge av tilsynsaktiviteten. Denne informasjonen kan hentes fra NSAs tilsynsplan(er) og oppfølgingstabell over NSAs anbefalinger til den aktuelle jernbanevirksomheten.*

b) *Oversikt over NSAs fremtidige tilsynsaktiviteter som er planlagt for den aktuelle jernbanevirksomheten. Denne informasjonen kan hentes fra NSAs potensielle tilsynsplan(er)*

c) *Eventuelle resultater fra innsamling og analyse av ulykker/hendelser og klager oversendt NSA som vedrører sikkerhetsstyringssystemets ytelse, inkludert en kort oppsummering av hver hendelse og eventuelle tiltak som NSA har tatt for å følge opp løsning av problemene som har oppstått. Denne informasjonen kan samles inn og analyseres fra jernbanevirksomhetens årlige sikkerhetsrapport, rapportering av hendelser/ulykker fra jernbanevirksomheten til NSA, og også fra databaser eller registre, slik som ERAIL for jernbaneulykker og undersøkelser av hendelser;*

d) *Informasjon om alvorlig sikkerhetsrisiko som fremkommer under internrevisjon og andre overvåkingsaktiviteter av jernbanevirksomheten, status på handlingsplanen for å avslutte påpekte forhold og eventuelle tiltak som NSA-en har tatt for å kontrollere ferdigstillelse og effektivitet siden det forrige sikkerhetssertifikatet eller sikkerhetstillatelsen ble tildelt. Denne informasjonen kan samles inn og analyseres fra jernbanevirksomhetens eller infrastrukturforvalterens årlige sikkerhetsrapport (dvs. rapport om bruk av CSM for overvåking);*

e) *Informasjon som er rapportert av relevant NIB om pågående undersøkelser av hendelser knyttet til jernbanevirksomhetens aktiviteter, og anbefalinger fra tidligere undersøkelser som fortsatt er åpne og som ikke er fulgt opp av jernbanevirksomheten. Denne informasjonen kan samles inn og analyseres fra jernbanevirksomhetens årlige sikkerhetsrapport, men også fra databaser eller registre, slik som ERAIL for undersøkelser av jernbaneulykker og -hendelser. I samsvar med artikkel 8(3) i CSM om tilsyn skal NSA-en også samordne med NIB. Det bør forventes at relevant informasjon deles mellom NSA-en og NIB under denne samordningen;*

f) *Oversikt over eventuelle sanksjoner utført av NSA, som angitt i nasjonal lovgivning og som vedrører sikkerhetsstyringssystemets ytelse, mot jernbanevirksomheten siden det forrige sikkerhetssertifikatet eller sikkerhetstillatelse ble tildelt. Denne informasjonen gjelder handlinger utført av NSA-en for å håndheve sine vedtak, f.eks. forbedrings/forbudsvarsel, straffer, midlertidige sikkerhetsforanstaltninger (i henhold til artikkel 17 i direktiv 2016/798).*

g) *Eventuell ytterligere informasjon som NSA anser som viktig for vurderingen. Ytterligere informasjon kan samles inn og analyseres fra jernbanevirksomhetens årlige sikkerhetsrapport og fra NSA-ens årsrapport.*

Den generelle forventningen er at informasjon ovenfor vil bli gitt til myndigheten som tildeler sikkerhetssertifikat av NSA ved tidspunktet for søknaden om å fornye felles sikkerhetssertifikat. Hvis NSA-en under tilsynet bestemmer seg for å iverksette sanksjoner, herunder påtale av en jernbanevirksomhet, og den mener at myndigheten som tildelte sikkerhetssertifikatet bør vurdere å oppheve det enkelte sikkerhetssertifikatet, bør saken henvises direkte til myndigheten som tildeler sikkerhetssertifikat og ikke vente til søknaden om fornyelse av et felles sikkerhetssertifikat foreligger.

Dette innebærer derfor en viss samordningsaktivitet mellom de som utfører tilsyn og de som utsteder sikkerhetssertifikat. Det er selvfølgelig viktig å sørge for at relevant informasjon deles mellom de som utfører tilsyn og de som tildeler sikkerhetssertifikat, slik at problemer knyttet til en jernbanevirksomhets SMS behandles skikkelig av den aktuelle parten. NSA-ene bør ha framgangsmåter for å styre dette i sine tilsynsstrategier og -planer.

Artikkel 11(3) i Kommisjonens gjennomføringsforordning (EU) 2018./763 *[praktiske ordninger for utstedelse av enkelt sikkerhetssertifikat]* sier klart at myndigheten som tildeler sikkerhetssertifikat etter vurderingen skal avgjøre sammen med NSA-en hvilke gjenværende problemstillinger som er utestående fra vurderingen og kan utsettes til senere vurdering i forbindelse med gjennomføring av tilsyn.

For kjøretøytillatelser er det viktig at det også finnes en mekanisme for at de som utsteder kjøretøystillatelser deler relevant informasjon med de som utfører tilsyn, spesielt når det gjelder begrensninger av bruksvilkårene for kjøretøy. Likeledes bør NSA-ene ha en mekanisme for at de som utfører tilsyn sender informasjon tilbake til de som har gitt tillatelse til et bestemt kjøretøy der det er problemstillinger om hvorvidt det kjøretøyet fortsatt oppfyller vilkårene for tillatelse gitt til kjøretøystypen eller kjøretøytillatelse for bruk på markedet ble gitt. Det skal bemerkes at under drift av et kjøretøy kan det være at det oppdages feil som påvirker alle kjøretøyene av den typen eller serien. I så fall kan et sikkerhetsvarsel opprettes ved hjelp av Safety Information System (SIS). NSA-en bør også følge opp hvordan jernbanevirksomheten håndterer risikoen og varsler ECM.

6. Koordinering mellom NSA(-er)

Artikkel 8 i CSM for tilsyn krever at NSA-ene koordinerer tilsynsaktivitetene sine med andre NSA-er der det er grensekryssende drift. Denne koordineringen er nødvendig for å unngå duplisering av innsats fra NSA-er og å unngå å belaste virksomheter det føres tilsyn med med flere kontakter fra ulike lands sikkerhetsmyndigheter. Den er også til for å sikre at de ulike NSA-ene som fører tilsyn med grensekryssende drift deler relevant informasjon slik at de kan utføre tilsynet på en effektiv måte. Ved koordinering av tilsynsaktiviteter vil det være nødvendig for NSA-ene å avgjøre seg imellom hvem som skal være «ledende» NSA. I denne sammenhengen er «ledende» NSA den som opptrer som overordnet koordinator for tilsynsaktivitetene og hovedkontaktpunktet for jernbanevirksomheten det gjelder. «Ledende» NSA kan være NSA-en fra den MS-en der det største aktivitetsvolumet foregår eller hvor virksomheten som blir ført tilsyn med er registrert. NSA-ene skal sammen bestemme hvilke deler eller tema som er viktigst å undersøke under tilsynet over gyldighetsperioden til det felles sikkerhetssertifikatet eller sikkerhetstillatelsen, og utarbeide en plan for å levere det de sammen har blitt enige om. NSA-ene bør også være enige om en voldgiftsprosess for tvister for å håndtere eventuelle uenigheter mellom NSA-ene som utfører tilsynsaktiviteten.

Vedlegg II til felles sikkerhetsmetode for tilsyn gir et rammeverk for koordinert og felles tilsyn som kan brukes av NSA-ene som en veileder for å styre denne prosessen. Viktige punkter er at tilsynet skal koordineres på en slik måte at det ikke oppstår unødvendig ulempe for jernbanevirksomheten, for eksempel ved å sørge for at nøkkelpersonale i jernbanevirksomheten ikke forespørres av ulike NSA-er samtidig, eller at det samme stedet er gjenstand for flere tilsyn i løpet av kort tid. Dersom NSA-ene opererer i henhold til lovbestemmelser som ikke forutsetter eller tillater «felles tilsyn», bør dette gjenspeiles i avtalene dem imellom. I dette tilfellet vil det være nødvendig for den «ledende» (eller koordinerende) NSA-en sammen med de andre involverte NSA-ene å utvikle en felles plan for å utføre de nødvendige tilsynsaktivitetene i hver medlemsstat.

Der det finnes en samarbeidsavtale (eller kontrakt) mellom jernbaneselskaper som gjør det mulig for et tog fra en medlemsstat å bli et tog fra en annen når det krysser grensen (selv om mannskapet og toget er fra jernbaneselskapet i den første medlemsstaten), bør de berørte NSA-ene koordinere seg imellom for å sikre at risikoen forbundet med saker på grensesnittet mellom jernbaneselskapene, slik som opplæring i relevant nasjonalt eller internasjonalt regelverk og vedlikehold av togene som er involvert, styres på riktig måte. Hvis en NSA oppdager problemer med ordningene med et jernbaneselskap under slike omstendigheter, bør de kontakte den aktuelle nabo-NSA-en om tiltak de har til hensikt å ta for å håndtere saken.

Det finnes mer informasjon i *Byråets veileder om koordinering mellom nasjonale sikkerhetsmyndigheter – en felles tilnærming til tilsyn*.

7. Menneskelige faktorer og sikkerhetskultur

For både vurderinger i forbindelse med tildeling av sikkerhetssertifikat og tilsyn bør NSA-ansatte kunne identifisere menneskelige faktorer og sikkerhetskulturstrategi, og hvordan virksomheten som det føres tilsyn med innlemmer slike problemer i sitt SMS (se felles sikkerhetsmetode for sikkerhetstyringssystem vedlegg I og vedlegg II). Som følge av dette bør den nasjonale sikkerhetsmyndigheten bygge opp kunnskap om hvordan menneskelige faktorer og sikkerhetskultur skal tas i betraktning, som kan brukes til å underrette tilsynsstrategien og tilsynsplanen (e) (se også Byråets veiledning om SMS ogByråets retningslinjer for forvaltningsmodell med løpetid).

8. Samarbeid med andre kompetente myndigheter eller organer

Det forventes at en NSA som fungerer som sikkerhetsmyndighet i en medlemsstat, vil ha anledning til å samarbeide og samordne med andre kompetente myndigheter eller organer under utførelsen av sine funksjoner.

I artikkel 8 (3) av de felles sikkerhetsmetodene for tilsyn er det fastsatt at den nasjonale sikkerhetsmyndigheten skal utarbeide samarbeidsordninger med relevante andre organer som nib, sertifiseringsorgan for ECA eller andre vedkommende myndigheter slik at relevante opplysninger er felles, og at det behandles alvorlig sikkerhetsrisiko. Formålet med denne bestemmelsen er å sikre at de som har et mål på myndigheten, og som kan ha behov for å treffe særlige tiltak, blir behørig informert og kan reagere på dette.

Det kan for eksempel være behov for å samarbeide med myndigheter som har i oppdrag å være i samsvar med reglene for farlig gods, brukerinspektorater, politi (strafferettslige sanksjoner), miljøregulatorer, reguleringsmyndighetene med ansvar for utstedelse av sertifikater, sertifikater til jernbaneforetak, tillatelse til utstedelse eller utstedelse av sertifikater.

Følgende er illustrative eksempler på slikt samarbeid. NSA-ene bør, om nødvendig, sørge for at deres strategi og planer tilpasses etter behov.

8.1 Godkjennings- eller sertifiseringsorganer

NSA-ene forventes å samarbeide med andre godkjennings- (feks. organer som er ansvarlig for å gi tillatelse av kjøretøy) eller sertifiseringsorganer (feks. organer som er ansvarlige for sertifisering av opplæringssentre for lokomotivførere) etter behov. Fra et tilsynsperspektiv bør en NSA som utfører tilsyn akseptere sertifikater eller tilltatelser som fremlegges som bevis på overholdelse av EUs eller andres forskrifter i den grad de dekker saken som er under tilsyn. Dersom NSA-en under tilsynsaktiviteten blir oppmerksom på at det foreligger et alvorlig sikkerhetsproblem som involverer en sak som er innvilget en tilltatelse eller et sertifikat, bør den ta midlertidige korrigerende tiltak (f.eks. suspensjon av kjøretøybruk) etter behov, og henvende seg til det aktuelle organet som er ansvarlig for utstedelsen av sertifikatet eller tillatelsen.

8.2 Sikkerhetsproblemer på arbeidsplassen

Noen NSA-er er ansvarlige for sikkerhet på arbeidsplassen i deres medlemsstats lovverk, mens andre NSA-er ikke er det. I det første tilfellet, der sikkerhetsproblemer på arbeidsplassen oppstår under tilsyn, bør disse behandles av de som utfører tilsynet. I det andre tilfellet, når NSA-personalet som utfører tilsyn blir oppmerksom på sikkerhetsproblemer på arbeidsplassen, bør de gjøre virksomheten de fører tilsyn med oppmerksom på at de har sett noe bekymringsverdig, og deretter henvise saken til relevant myndighet for

oppfølging. NSA-en bør også koordinere og samordne, som hensiktsmessig, med ansvarlig k myndighet for sikkerhet i arbeidsmiljøet for å sikre at deres respektive strategier og planer samsvarer med hverandre.

8.3 Lokomotivfører, arbeid, kjøring og hviletidsregler

Artikkel 17(4) i direktiv (EU) 2016/798 krever at en kompetent myndighet er ansvarlig for å sikre overholdelse av regelverk for arbeids-, kjøre- og hviletid for lokomotivførere. Hvor denne kompetente myndigheten ikke er NSA-en, bør denne myndigheten samarbeide med NSA-en slik at NSA-en kan utføre sine tilsynsaktiviteter. Det følger av dette at hvis NSA-en ikke er den kompetente myndigheten for overholdelse av slike regler, men den blir oppmerksom på problemer som gjelder dem gjennom sine tilsynsaktiviteter i en bestemt virksomhet, bør den informere den kompetente myndigheten så snart som mulig etter funnet.

8.4 Samarbeid mellom en NSA og andre myndigheter

Artikkel 56(3) i direktiv 2012/34/EU sier følgende:

Det regulatoriske organet skal også samarbeide tett med den nasjonale sikkerhetsmyndigheten i henhold til Europaparlamentets og Rådets direktiv 2008/57/EF av 17. juni 2008 om interoperabilitet av jernbanesystemet i Fellesskapet og lisensmyndigheten innenfor betydningen av dette direktivet.

Medlemsstatene skal sørge for at disse myndighetene i fellesskap utvikler et rammeverk for informasjonsdeling og samarbeid for å hindre negative virkninger på konkurranse eller sikkerhet i jernbanemarkedet. Dette rammeverket skal omfatte en mekanisme slik at reguleringsorganet kan gi de nasjonale sikkerhets- og lisensmyndighetene anbefalinger om problemer som kan påvirke konkurransen i jernbanemarkedet, og at den nasjonale sikkerhetsmyndigheten kan gi reguleringsorganet og lisensmyndigheten anbefalinger om problemer som kan påvirke sikkerhet. Uten at det berører hver myndighets uavhengighet innenfor sitt respektive kompetanseområde, skal den relevante myndigheten undersøke enhver slik anbefaling før bestemmelsene vedtas. Hvis den aktuelle myndigheten bestemmer seg for å avvike fra disse anbefalingene, skal den begrunne dette i vedtakene.

I praksis kan dette bety:

a) *I en situasjon hvor et reguleringsorgan ber et etablert jernbaneforetak om å «åpne» tjenester for konkurranse, og det nekter og oppgir «sikkerhet» som en grunn, bør reguleringsorganet spørre NSA-en, som «sikkerhetsregulator», for dens oppfatning av om dette er en berettiget grunn til ikke å åpne tjenestene. Reguleringsorganet bør da ta hensyn til NSA-ens syn når det tar en avgjørelse om hvilke tiltak som skal tas;*

b) *I en situasjon der en infrastrukturforvalter har til hensikt å søke NSA-en for tillatelse til å sette i bruk et ETCS Level 1 delsystem på sporsiden som implementerer noen av de valgfrie funksjonene (f.eks. innfyllingsfelt, radiofylling) som krever at kjøretøyene må være utstyrt med relevant utstyr for å kunne kjøre på denne linjen, bør NSA-en be reguleringsorganet om å bekrefte at dette ikke diskriminerer mot jernbanevirksomheter, og at relevant informasjon er gjort tilgjengelig for alle interesserte parter og gir dem nok tid til å tilpasse kjøretøy tilsvarende.*

8.5 Samarbeid mellom en NSA og en lisensmyndighet

Direktiv 2012/34/EU sier følgende:

Art. 24(3): *Til tross for paragraf 1, der en lisens suspenderes eller tilbakekalles på grunn av manglende overholdelse av kravet om økonomisk egnethet,* ***kan lisensmyndigheten innvilge en midlertidig lisens*** *i*

påvente av omorganisering av jernbanevirksomheten, ***forutsatt at sikkerheten ikke settes på spill****. En midlertidig lisens skal imidlertid ikke være gyldig i mer enn seks måneder etter utstedelsesdatoen.*

Art. 24(5): *I tilfeller der en endring som påvirker en virksomhets juridiske situasjon, og særlig i tilfeller av fusjon eller overtakelse,* ***kan lisensmyndigheten beslutte at lisensen skal sendes til ny godkjenning. Den aktuelle jernbanevirksomheten kan fortsette driften, med mindre lisensmyndigheten beslutter at sikkerheten blir satt på spill.*** *I så fall skal begrunnelsene for en slik avgjørelse oppgis.*

For at lisensmyndigheten i praksis skal kunne avgi en lisensavgjørelse, må den konsultere NSA-en som sikkerhetsmyndighet. Spørsmålet lisensmyndigheten må svare på er om det er sannsynlig at sikkerheten vil bli satt på spill. Hvis den ber en jernbanevirksomhet om å operere under en midlertidig lisens (se artikkel 24(3)). Et annet spørsmål som må vurderes, er om en lisenssøknad må sendes til ny godkjenning (se artikkel 24(5)). Når avgjørelsen tas skal lisensmyndigheten ta hensyn til NSAs formening, som sikkerhetsregulator.

8.6 Samarbeid mellom en NSA og et ECM-sertifiseringsorgan

NSA-er og ECM-sertifiseringsorganer bør samarbeide for å unngå duplisering av aktiviteter. Dette betyr at når en NSA under utføring av tilsynet kommer over et kjøretøy (godsvogn) som er dårlig vedlikeholdt, og det dermed oppstår tvil om den aktuelle ECM-ens evne til å overholde kravene for sertifiseringen, bør NSA-en sende denne informasjonen til det relevante ECM-sertifiseringsorganet, som angitt i artikkel 9 i ECM-forordningen. Likeledes, hvis ECM-sertifiseringsorganet nekter å sertifisere en eksisterende ECM, bør de sende denne informasjonen til de relevante NSA-ene. Slik informasjon vil hjelpe NSA-ene å justere tilsynsstrategiene sine og planlegge tilsvarende.

9. Rammeverk for styring av kompetanse

I samsvar med artikkel 6 i felles sikkerhetsmetoder skal de nasjonale sikkerhetsmyndigheter sikre at personalet som deltar i tilsynet, har den nødvendige kompetanse. Den nasjonale sikkerhetsmyndigheten bør velge ut, tog og vedlikeholde kompetansen til det personalet gjennom et kompetansestyringssystem. Det er opp til hver enkelt nasjonal sikkerhetsmyndighet å opprette og bygge sin egen kompetanseledelse i samsvar med artikkel 6 i felles regelverk for felles sikkerhetsmetoder. For å hjelpe den nasjonale sikkerhetsmyndighet til å forvalte dette spørsmålet, har Byrået opprettet en veiledning for kompetanseledelse, og det vil gi råd om hva som utgjør et egnet kompetansestyringssystem, og hvilke spørsmål den nasjonale sikkerhetsmyndigheten må vurdere å ta i utvikling én (se Byråets veiledning om forvaltningsrammer for kompetanse).Veiledningen vil imidlertid ikke angi nøyaktig hva kompetansestyringssystemet ser ut til å være et spørsmål for hver enkelt nasjonal sikkerhetsmyndighet.

Vedlegg Foreslått mal for en tilsynsstrategi

Innholdsfortegnelse