vegtilsynet

Tilsynsrapport - sak 2025-07

Styring av sikkerhet i digitale systemer

Statens vegvesen

vegtilsynet

Saksnummer	2025-07
Publiseringsdato	11.12.2025
Tilsynslag	Thomas Ruud Sollien, tilsynsleder Thomas Sjøflot, fagrevisor veg Iver Fiksdal, ekstern revisor, Deloitte
Tilsynspart	Statens vegvesen
Tilsynsform	Tilsynsmøte

Om rapporten

Rapporten er basert på tilsyn i Statens vegvesen. Tilsynssaken omhandler styring av sikkerhet i digitale systemer med betydning for sikkerheten i veginfrastrukturen.

Vegard Hansen
direktør

Thomas Ruud Sollien
tilsynsleder

Rapporten er godkjent elektronisk og har ingen signatur.

Sammendrag

Digitalisering og ny teknologi i vegsektoren gir både muligheter og nye risikoer, inkludert trusler mot trafikksikkerheten. Derfor er det viktig å ha kontroll på digitale systemer som styrer trafikk og beredskap

Målet med tilsynssaken har vært å undersøke om Statens vegvesen har et styringssystem som sikrer oppfyllelse av krav til digital sikkerhet knyttet til veginfrastrukturen. En sekundær hensikt har vært for Vegtilsynet å bygge kunnskap om tilsynspart sitt styringssystem for på en best mulig måte kunne gjennomføre eventuelle oppfølgende tilsyn.

Tilsynet ble gjennomført som et tilsynsmøte etter revisjonsprinsippene i NS-EN ISO 19011:2018. Bevisinnhentingen i tilsynssaken var avgrenset til informasjon fra møtet. Samlet sett er det Vegtilsynets vurdering at diskusjonen i tilsynsmøtet viser at tilsynspart har et styringssystem som i betydelig grad sikrer at krav til digital sikkerhet, knyttet til veginfrastrukturen, blir oppfylt.

Hovedfunn i tilsynet har vært:

- Tilsynspart sitt arbeid for å identifisere og vurdere risiko synes å være betryggende for alle systemer som omfattes av virksomhetens ledelsessystem for informasjonssikkerhet.
- Vegtilsynet er usikre på om alle digitale systemer med potensiell risiko håndteres i tråd med ovennevnte ledelsessystem.
- Tilsynspart sitt arbeid med kontrollaktiviteter og risikoreduserende tiltak vurderes som tilfredsstillende, men med enkelte forbedringspunkter.
- Tilsynspart har en god modenhet knyttet til behov for å drive kontinuerlig oppfølging og vurdering/effektevaluering av risikoreduserende tiltak.

Vegtilsynet har i saken gitt to observasjoner:

1. Statens vegvesen bør tydeliggjøre hvordan det kan sikres at alle digitale systemer med potensiell risiko blir identifisert.

2. Statens vegvesen bør vurdere hvordan tiltak som ligger utenfor det enkelte system eller mellom systemer best kan iverksettes. Dette er viktig for å legge til rette for en helhetlig risikostyring og iverksette relevante risikoreduserende tiltak.

Innhold

1. Bakgrunn

Digitalisering av vegsektoren og innføring av ny teknologi gir økte muligheter. Samtidig skaper digitalisering også nye og ukjente sårbarheter og risikoer – også for trafikantene sin sikkerhet. Å ha kontroll på de digitale systemene er viktig for at verdikjeden skal fungere, bl.a. knyttet til trafikkstyring og beredskap ved hendelser. I Nasjonal strategi for digital sikkerhet framheves viktigheten av forebyggende arbeid ved å foreta risikovurderinger og gjennomføre tilstrekkelige tiltak for å beskytte seg mot uønskede hendelser. Den senere tid har det kommet fram opplysninger fra Politiets sikkerhetstjeneste om at uvedkommende har skaffet seg tilgang til digitale systemer for bl.a. styring av luker i dammer i vassdrag.

Et styringssystem for informasjonssikkerhet skal gjennom en prosess for risikostyring bidra til at konfidensialiteten, integriteten og tilgjengeligheten til informasjon bevares.[1]

- Konfidensialitet dreier seg om at informasjon ikke blir kjent for uvedkommende.
- Integritet handler om at informasjon ikke blir endret av uvedkommende, eller på en utilsiktet måte.
- Tilgjengelighet betyr at informasjon skal være tilgjengelig for autoriserte brukere ved behov.

Vegtilsynet ønsker å undersøke sikkerhetsstyringen i digitale systemer med betydning for sikkerheten i veginfrastrukturen.

Forskrift om vegdata, trafikkinformasjon, trafikkberedskap og trafikkstyring m.m. for offentlig ved (vegdata- og trafikkinformasjonsforskriften), med ikrafttredelse 01.04.2025, stiller i §6-1 ulike typer krav til aktører i vegsektoren knyttet til digital sikkerhet.

[1] Jf. ISO/IEC 27001:2023

2. Mål

Målet med tilsynet har vært å undersøke om Statens vegvesen har et styringssystem for å sikre at krav til digital sikkerhet knyttet til veginfrastrukturen blir oppfylt.

I tillegg til ovennevnte mål er det en hensikt med saken å styrke Vegtilsynets kunnskap om og innsikt i Statens vegvesen sitt styringssystem knyttet til digital sikkerhet. Dette for på en best mulig måte å kunne gjennomføre eventuelle oppfølgende tilsyn på området.

3. Metode og gjennomføring

Metode

Tilsynssaken er gjennomført som et tilsynsmøte. Dette er en av tilsynsformene Vegtilsynet har etablert for å føre tilsyn med at Statens vegvesen og Nye Veier AS. Tilsynsformen bygger på alminnelige revisjonsprinsipp, jf. ISO 19011:2018[2]. Vegtilsynet benytter tilsynsformen for å skaffe kunnskap om og ha dialog med tilsynspart om utvalgte trafikksikkerhetsmessige forhold. Tilsynsformen blir også benyttet innenfor andre områder, der Vegtilsynet ser at det kan være hensiktsmessig å gjennomføre et mer overordnet og dialogpreget tilsyn.

For denne tilsynssaken er det er fastsatt fem tilsynskriterier[3], utledet fra vegdata- og trafikkinformasjonsforskriften, jf. kap. 1.

Saken er avgrenset til sikkerhetsstyringen i digitale systemer med betydning for sikkerheten i veginfrastrukturen. Bevisinnhenting i saken er avgrenset til informasjon som kom fram i tilsynsmøtet.

Digitale systemer med betydning for sikkerheten i veginfrastrukturen omfatter blant annet (ikke uttømmende liste):

- Digitale systemer som umiddelbart kan endre objekter og veginfrastruktur
    - Trafikkstyring
    - Lys, signalanlegg, bommer, skilt, bevegelige broer, vifter, pumper, radiomeldinger, osv.
- Digitale systemer som er en del av en beredskapsfunksjon.
    - Overvåking av trafikk og veginfrastruktur
    - Kamera, Nødtelefoner, signal fra brannslokker, værstasjoner, CO2-målere, signal fra dører og porter osv.
- Digitale systemer som er nødvendig for å ivareta veginfrastruktur
    - Systemer med tilstand på objekter og veginfrastruktur
    - Systemer for registering av tilstand på objekter og veginfrastruktur

[2] ISO 19011:2018 Retningslinjer for revisjon av ledelsessystmer
[3] Se kap. 4 Tilsynsresultat

    - Systemer for oppfølging av feil og mangler på veginfrastruktur
    - Systemer med informasjon om objekter og veginfrastruktur, som type, alder, vedlikehold, oppfølging, tegninger, reservedeler, osv.
- Digitale systemer som er nødvendig for utføre og følge opp drift av veginfrastruktur

Gjennomføring

Vegtilsynet sendte varsel om tilsyn 02.09.2025 og gjennomførte tilsynsmøtet 31.10.2025. Representasjon fra tilsynspart sin side i tilsynsmøtet framgår av tabell 1.

Tilsynet har hatt slik framdrift:

Dato	**Framdrift**
29.09.2025	Varsel om tilsyn
31.10.2025	Åpningsmøte
31.10.2025	Tilsynsmøte der representanter fra følgende divisjoner deltok: IT, Transport og samfunn, Drift og vedlikehold, og Økonomi og virksomhetsutvikling i Vegdirektoratet
21.11.2025	Rapportutkast oversendt for faktasjekk. Frist for innspill 08.12.2025
05.12.2025	Sluttmøte
11.12.2025	Endelig tilsynsrapport

Tabell 1: Gjennomføring og framdrift av tilsynssaken

Utkast til rapport ble sendt tilsynspart for faktasjekk 21.11.2025. Funn ble gjennomgått i sluttmøte med tilsynspart 05.12.2025. Tilsynspart gav i brev datert 8. desember 2025 tilbakemelding på at det ikke var funnet faktafeil i utkast til rapport, og dette er lagt til grunn ved utarbeidelse av endelig tilsynsrapport.

Vegtilsynet opplever at det har vært god dialog mellom partene, der tilsynspart har lagt forholdene til rette for en effektiv og god gjennomføring av tilsynet.

4. Tilsynsresultat

Symboler som er brukt for å illustrere tilsynsfunnene i rapporten går fram av tabellen under.

Symbol	Vurdering av samsvar med tilsynskriterium
	Avvik: Manglende samsvar med krav
	Observasjon: Forhold der man gjennom tilsynet har sett at det er potensial for forbedring hos tilsynspart
	Undersøkelsen har ikke avdekket avvik eller observasjoner

Tabell 2: Illustrasjon på tilsynsfunn

Tilsynskriterium:
Virksomheten skal ha et styringssystem for digital sikkerhet. Sentrale krav knyttet til et slikt system for styring av digital sikkerhet vil være:
TK1: Virksomheten skal identifisere risiko
TK2: Virksomheten skal vurdere identifiserte risikoer
TK3: Virksomheten skal iverksette risikoreduserende tiltak/kontrollaktiviteter
TK4: Virksomheten skal evaluere effekten av iverksatte tiltak
TK5: Virksomheten skal justere/tilpasse risikoreduserende tiltak/kontrollaktiviteter

Utledning av tilsynskriterium:
Virksomheten må kjenne til eksterne krav for å kunne ha kontroll med at styringssystemet er innrettet slik at det sikrer oppfylling av relevante eksterne krav. Plikten til å sikre sammenheng mellom eksterne krav og styringssystemet går fram flere steder i Prop. 160 L (2015-2016) Endringar i veglova (Vegtilsynet) bl.a. kap. 2.2. I dette punktet er det presisert at eit styringssystem skal «innehalde ei beskriving av aktivitetar for å nå dei mål og for å sikre etterleving av dei krav som er satt til tryggleiken knytt til riksveg».

For denne saken betyr dette at vegdata- og trafikkinformasjonsforskriftens krav til digital sikkerhet må være operasjonalisert og beskrevet i Statens vegvesens styringssystem på en slik måte at det legges til rette for at forskriften etterleves.

Det følger av forskriften § 6-1 første ledd at Statens vegvesen gjennom planlagte og systematiske tiltak skal, i henhold til nasjonale og europeiske sikkerhetsstandarder, normer og regelverk, sørge for tilfredsstillende behandling av data og informasjon. Av Vegdirektoratets veileder til forskriften[4] framgår det at dette medfører at «Det skal foreligge risikovurderinger av de digitale systemene som er i eller tilknyttet vegnettet og av systemene og løsningene for de nasjonale tjenestene.»

Av forskriften § 6-1, andre ledd framgår det at Statens vegvesen skal stille krav til sikkerhet og beskyttelse, inkludert tilgangsstyring, i henhold til sikkerhetsstandarder og normer for datasystemer og tjenester, samt til tilknytningspunkt, kommunikasjonsinfrastruktur og utstyr. I nevnte veileder trekkes ISO 2700-serien og IEC 62443-standardene fram som relevante sikkerhetsstandarder og normer.

Tilsynsbevis

Overordnet ansvars- og arbeidsdeling

I tilsynsmøtet ble tilsynspart innledningsvis bedt om å redegjøre kort for den overordnede organiseringen av arbeidet med sikkerhet i digitale systemer/informasjonssikkerhet. Det ble også etterspurt hvordan roller og ansvar for sikkerhet i det enkelte system er fastlagt, og hvordan systemspesifikk sikkerhet og det overordnede informasjonssikkerhetsarbeidet henger sammen.

Som svar på de innledende spørsmålene, viste tilsynspart til at:

- Det ligger en tydelig ansvarsfordeling knyttet til informasjonssikkerhet i Policy for informasjonssikkerhet.
    - Leder for IT-divisjonen, IT Digital sikkerhet, er ansvarlig for etatens ledelsessystem for informasjonssikkerhet og legger dermed premissene for sikkerhetsarbeidet.
    - Divisjonsdirektører har, som system- eller prosesseiere, et utøvende og operasjonelt ansvar for sikkerheten.
- Innenfor denne organiseringen har systemeier et ansvar for risikoene i det enkelte IT-system og de følges opp regelmessig fra IT-divisjonen med tanke på bl.a. gjennomføring av verdivurderinger, sikkerhetstiltak, avvik og lukking av avvik.

[4] Veiledning til forskrift om vegdata, trafikkinformasjon, trafikkberedskap og trafikkstyring m.m. på offentlig veg, datert 02.05.25

Vegtilsynet stilte videre spørsmål om det oppleves å ligge noen uklarheter knyttet til ansvarsdragningen mellom divisjonene som systemeiere og IT Digital sikkerhet sitt ansvar for ledelsessystem for informasjonssikkerhet.
På dette spørsmålet ble det vist til at:

- IT-divisjonen oppfatter ansvarsdelingen som tydelig, og at rollene som premissgivende og kontrollerende aktør er tilstrekkelig tydelig avgrenset mot systemansvaret for spesifikke system som ligger ute i de enkelte divisjonene.
- Fra fagdivisjonenes side oppleves ansvarsdragning og organisering å være god, og det pekes på at IT Digital sikkerhet og divisjonene jobber godt og metodisk på tvers for å sikre at risikoer identifiseres, vurderes og håndteres.
    - Det ble understreket at den støtte og oppfølging som fås fra IT Digital sikkerhet fungerer godt og at fagdivisjonene opplever å ha tilgang på et sterkt kompetansemiljø som systemeierne har god nytte av.

Egenvurdering av styring av sikkerhet i digitale systemer

Vegtilsynet utfordret tilsynspart til å gi en egenvurdering av i hvilken grad de vurderer at SVV har et tilstrekkelig system for styring av digitale systemer med betydning for sikkerhet i veginfrastruktur.

- Av positive egenskaper ved ledelsessystemet for informasjonssikkerhet trakk tilsynspart fram opplegget rundt systemeierskap, ansvars- og oppgavefordeling som noe som fungerer veldig godt. Det var også en oppfatning av at kulturen rundt arbeid med informasjonssikkerhet nå kan karakteriseres som solid og det er en viktig premiss for å komme videre i dette arbeidet. Det oppleves også at arbeidet med digital sikkerhet er ganske godt integrert i arbeidet med IT-systemer i virksomheten.
- Når det gjelder utfordringer ble ressurssituasjonen pekt på som sentral. For noen systemer er dette ikke problematisk eller kritisk, mens for andre systemer er dette en betydelig utfordring. Dette kan medføre at sikkerhetsrisikoen øker og det ble pekt på viktigheten av at arbeidet med informasjonssikkerhet ikke blir en salderingspost.
- Det er også en utfordrende faktor med stor kompleksitet, både organisatorisk og mellom systemer. Slik kompleksitet øker sannsynligheten for at ting «faller mellom to stoler» og at risiko ikke blir tatt tak i på en systematisk måte.

- Ulike aspekter knyttet til eksterne leverandører ble også trukket fram som en utfordrende faktor. Eksempler var mangel på teknisk personell hos leverandører og manglende risikovurderinger av endringer eller oppdateringer foretatt av leverandører i tilsynspart sine systemer.

TK1: Virksomheten skal identifisere risiko

Vegtilsynet stilte spørsmål om tilsynspart har definert mål for informasjonssikkerhetsarbeidet, om det er fastsatt en egen policy (e.l), og om det foreligger tydelige sikkerhetskrav og risikostrategi/-toleranse for arbeid med sikkerhet i digitale systemer.

- Tilsynspart bekreftet at det finnes en *Policy for informasjonssikkerhet* som setter de overordnede rammene og styrende prinsippene for styringssystemet.
    - Dette policydokumentet bygger på *Policy for sikkerhet og beredskap i Statens vegvesen* som gir rammene for et systematisk sikkerhets- og beredskapsarbeid i virksomheten og som bygger opp under etatens toppmål og virksomhetsstrategi.
- *Policy for sikkerhet og beredskap* definerer tydelig CISO[5], leder av IT Digital sikkerhet, som ansvarlig for arbeidet med informasjonssikkerhet og da på vegne av vegdirektøren.
    - I policydokumentet er det slått fast at etatens skal følge ISO27001-standarden[6] og ISF[7] – Standard of Good Practice (SOGP) i forvaltningen av sitt ledelsessystem for informasjonssikkerhet.
    - Ledelsessystemet inneholder ulike emnespesifikke retningslinjer som blant annet gjelder risikovurdering, tilgangsstyring, informasjonsklassifisering og sikkerhet i test og utvikling.
- Det påpekes fra tilsynspart at det ikke er stilt noe eksplisitt krav fra overordnet myndighet om overholdelse av ISO 27001, og at det heller ikke er noen ambisjon om å bli sertifisert etter standarden.
    - Det er derimot et klart mål å overholde standarden og å hente ut de effekter som følger av slik overholdelse.

[5] Chief Information Security Officer
[6] ISO/IEC 27001:2023 - ledelsessystem for informasjonssikkerhet
[7] Information Security Forum

    - I tillegg til de mer strategiske kravene i ISO-standarden om ledelsessystemer for informasjonssikkerhet legger IT Digital sikkerhet også til grunn krav i IEC 62443-standardene på et mer taktisk nivå, altså når mer detaljerte krav om premisser skal defineres.

Vegtilsynet stilte spørsmål om dette er dokumenter som er kjent og brukes aktivt ute i virksomheten.

- Det ble fra tilsynspart vist til at policydokumentet er på et overordnet nivå og en aktiv bruk av selve dokumentet antas å være begrenset til IT Digital sikkerhet.
- Når det gjelder prosesser, retningslinjer/prosedyrer og hjelpedokumenter i ledelsessystemet, som bygger på de overordnede mål og krav i policydokumentet, oppleves disse å være godt kjent ute i virksomheten.

Vegtilsynet stilte spørsmål om hvordan tilsynspart arbeider for å overholde krav i ISO 27001 og om det er på særlige områder det gjenstår arbeid før de kan si å overholde alle krav.

- Ved etableringen av det interne kravet om å følge ISO 27001 ble det foretatt en vesentlighets-/kritikalitetsvurdering. Arbeidet med de mest kritiske manglene ble prioritert først og det har siden blitt arbeidet systematisk og målrettet for å møte ISO-kravene.
    - Det ble påpekt at etaten ikke er helt i mål med å overholde alt i standarden, men de har kommet stadig lenger med å tette alle hull over de siste årene.
- Når det gjelder områder hvor det fremdeles er en jobb å gjøre før overholdelse kan sies å være på plass, ble det trukket fram flere ulike eksempler.
    - Enkelte eksempler var fra områder hvor utviklingen de siste årene har gått veldig hurtig, og det dermed er behov for justeringer og oppdateringer (sikkerhetsregler ved bruk av kunstig intelligens).
    - Andre eksempler var knyttet til temaer som «alltid» vil være krevende å håndtere og holde tilstrekkelig kontroll på (tilgang).

Vegtilsynet stilte spørsmål ved om det har blitt gjennomført systematiske risikovurderinger for å identifisere og vurdere informasjonssikkerhetsrisikoer for alle systemer som er vesentlige for trafikksikkerheten på vegene.

- IT Digital sikkerhet har ansvar for systemene for verdi- og risikovurderinger. Alle systemer som kommer inn i denne kjeden, skal verdivurderes (alt som kommer inn i CMDB[8]), og alt som verdivurderes skal også risikovurderes.
    - Kravet til å gjennomfør vurderingene ligger tydelig hos den enkelte systemeier. Det er også krav om at begge typer vurderinger skal oppdateres minst på årlig basis. Fra IT Digital sikkerhet sin side blir etterlevelsen av disse kravene monitorert og det blir tatt ut statistikk for å følge med.
    - Det blir framhevet at den kontrollen de opplever å ha på at risikovurderinger blir foretatt kommer av at det har blitt jobbet aktivt med å skape en sikkerhetskultur som bygger på en forståelse for behov for og bruk av risikovurderinger. Også kvaliteten på risikovurderingene oppleves som god.
- Vurderingene fra IT Digital sikkerhet ble bekreftet av systemeiere. Dette er systemer som følges og som de ikke ser bort fra i sin oppfølging, hverken på mer overordnet nivå eller når det gjelder det mer systemspesifikke arbeidet.
- Selv om IT Digital sikkerhet eier prosessen og systemeiere har ansvaret for gjennomføring benyttes fagkompetansen i IT Digital sikkerhet også ute i virksomheten.
    - IT Digital sikkerhet opplyser at de er involvert i gjennomføringen av mange/de fleste verdivurderinger og risikovurderinger, for å gi råd og være sparringpartner.
- Når det gjelder systemer som har betydning for trafikkstyring og -sikkerhet, opplever tilsynspart å ha god kontroll og at de i stor grad er i mål når det gjelder verdi- og risikovurderinger.
- Tilsynspart oppgir også å ha god oversikt over de områder og systemer hvor de ikke gjennomfører verdi- og risikovurdering i samsvar med etablerte krav.

Vegtilsynet stilte oppfølgingsspørsmål om noen av disse systemene er vesentlige eller av stor trafikksikkerhetsmessig betydning.

[8] En CMDB (Configuration Management Database) er en database som samler og organiserer informasjon om alle IT-komponentene og deres relasjoner i en organisasjon.

- Tilsynspart framholder at dette ikke er avdekt. Tilsynspart oppgir å ha flere ulike tilnærminger for å følge opp at vurderingene faktisk gjennomføres, holdes ajour og at krav blir ivaretatt.
    - For de viktigste systemene, også knyttet til trafikksikkerhet, oppgis gjennomføringen av risikovurderinger å være på plass, og at det har vært tilfelle over lengre tid.
- Flere systemeiere påpekte at oppfølging også skjer ute i divisjonene og avdelingene, hvor det fra de respektive ledere blir gitt betydelig oppmerksomhet på eventuell manglende gjennomføring av verdi- og risikovurderinger.

Vurdering

Vegtilsynet vurderer, på grunnlag av den presentasjon som ble gitt i tilsynsmøtet, at tilsynspart sitt arbeid for å identifisere risiko synes å være betryggende for alle systemer som inngår i CMDB. Den presentasjonen som ble gitt av prosesser, prosedyrer, retningslinjer og andre hjelpedokumenter fra ledelsessystem for informasjonssikkerhet viste en god systematikk, og diskusjon i møtet tilsier at krav til arbeidsoppgaver ute i virksomheten blir fulgt opp.

I tilsynsmøtet ble det i liten grad presentert noen systematisk tilnærming til å holde oversikt over alle digitale systemer og om det foretas noen overordnede risikovurderinger av alle systemer. Kriterier for å bli omfattet av ledelsessystemet ble i svært liten grad presentert for Vegtilsynet. Etter Vegtilsynet sin vurdering vil en svak systematikk for overordnet risikovurdering og uklare kriterier for hvilke systemer som omfattes av ledelsessystem for informasjonssikkerhet medføre risiko for at systemer som burde blitt fulgt opp i tråd med ledelsessystemets krav, faller utenfor. Dette vil igjen kunne innebære en risiko for uønskede hendelser.

Funn 1 – observasjon

Statens vegvesen bør tydeliggjøre hvordan det kan sikres at alle digitale systemer med potensiell risiko blir identifisert.

TK2: Virksomheten skal vurdere identifiserte risikoer

Vegtilsynet stilte spørsmål om hvordan gjennomførte risikovurderinger blir dokumentert.

- Tilsynspart opplyste at slike vurderinger dokumenteres og arkiveres systematisk både i CMDB og i andre systemer i hele systemenes livssyklus.

Vegtilsynet stilte spørsmål om det foreligger noen utfordringer eller svakheter i arbeidet med å identifisere og vurdere informasjonssikkerhetsrisikoer i de mest vesentlige systemene.

- Tilsynspart kvitterte med at de ikke er kjent med at det foreligger systematiske, store svakheter.
    - Det jobbes aktivt med å teste egen sikkerhet, eksempelvis om tiltak knyttet til tilganger faktisk fungerer og om operativ sikkerhet er på plass.
- Fra IT Digital sikkerhet sin side har det over tid blitt jobbet aktivt mot systemeierne med å «ufarliggjøre» risikovurdering, og for å få forståelse for at dette er gode verktøy for å håndtere usikkerhet og utrygghet.
    - Det har ute i virksomheten over tid blitt bygget erfaring og modenhet, og det er en oppfatning av at utviklingen har vært betydelig de siste årene.
- Samtidig fremheves det at tilsynspart er en stor organisasjon med mange ulike fagfelt, og at de fleste ikke jobber med digital sikkerhet i hverdagen.
    - Dette har som naturlig konsekvens at mange systemeiere ikke har den spisskompetansen som det mer spesialiserte fagmiljøet i IT-divisjonen har. Det oppfattes derfor som viktig at IT Digital sikkerhet er koblet tett på, men at det fremdeles må jobbes videre med å sikre at nok kompetanse inngår i alle relevante arbeidsprosesser hos systemeierne.

Vegtilsynet stilte spørsmål ved om systemer, prosesser og prosedyrer er fleksibelt nok til å fange alle ulike behov knyttet til de forskjellige systemene.

- Her svarte tilsynspart at dette oppfattes å være tilfelle. Dette ble uttrykt både fra miljøet som har ansvar for ledelsessystemet med dets prosesser og prosedyrer og systemeierne som har det utøvende ansvaret for den digitale sikkerheten.
    - Det ble trukket fram at etatens ledelsessystem for informasjonssystem gir et godt bilde av hvilke sikkerhetsnivå det enkelte systemet har, og hvor

tiltak og oppfølging skal iverksettes og at dette er gode prosesser for å sikre hensiktsmessig sikkerhetsarbeid mot hvert enkelt system, og disse systemenes konkrete sikkerhetsbehov.
    - Spesielt verdivurderingsprosessen, der man ser på skadepotensial og kritikalitetsvurdering, ble trukket fram som positiv. På bakgrunn av disse vurderingene, får man ut kritikalitetsklasser, som skiller på hva som er mest kritisk vs. mindre kritisk.

Vurdering

I tråd med vår vurdering knyttet til tilsynskriterium 1, vurderer Vegtilsynet at tilsynspart sitt arbeid for å vurdere risiko synes å være systematisk for alle systemer som inngår i CMDB. Dette gjelder både de krav som ligger i ledelsessystem for informasjonssikkerhet og den bruk av ledelsessystemet som foregår ute i virksomheten hos eierne av de respektive digitale systemene.

Også for dette tilsynskriteriet vil Vegtilsynet påpeke en usikkerhet ved om alle systemer med potensiell risiko faktisk blir fanget opp av tilsynspart sitt arbeid med å håndtere risiko.

Undersøkelsen har ikke avdekket avvik eller observasjoner

TK3: Virksomheten skal iverksette risikoreduserende tiltak/kontrollaktiviteter

Vegtilsynet ønsket å bli presentert for hvordan det arbeides med å finne tiltak for å håndtere identifisere risikoer, og sikre at tiltak iverksettes for å redusere identifiserte risikoer til et akseptabelt nivå. I denne sammenheng ble det stilt spørsmål om hvordan dette arbeidet er forankret i etatens ledelsessystem for informasjonssikkerhet og hvordan ansvar er fordelt.

- Tilsynspart opplyste at det i retningslinjer i ledelsessystemet er definert nivåer for akseptabel risiko og at risiko vurderes i en 5x5-matrise. Retningslinjene definerer også hvem som har mandat til å akseptere restrisiko og for å iverksette tiltak der det er behov for dette.
    - Et typisk eksempel kan være at systemeier har en viss myndighet, en avdelingsdirektør har en viss myndighet, og trinnvis videre oppover til vegdirektøren. Prinsippet er at risikoer over en fastsatt toleransegrense alltid skal løftes til neste nivå.

- Det er systemeierne på divisjonsnivå som har ansvar for gjennomføring av konkrete risikovurderinger og etableringer og oppfølging av slike risikomatriser som beskrevet over. Ved behov, og da gjerne knyttet til komplekse eller kompliserte risikoforhold, bistår IT Digital sikkerhet.
    - Slik involvering oppgis å ha et forholdsvis avgrenset omfang og handler ofte om hvorvidt divisjonen har brukt skalaene for sannsynlighet og konsekvens riktig. Fra IT Digital sikkerhet ble det poengtert at de opplever at divisjonene over tid har blitt gode og at de i stor grad er selvgående i arbeidet for å ta ned risikoen i henhold til de skalaene og vurderings- og akseptkriterier som er definert.
- Fra systemeiernes side ble det uttrykt at strukturen og systematikken er god og fungerer for å sikre at de identifiserer og iverksetter tiltak for å redusere risiko. De opplever at det er satt betydelig fokus på digital sikkerhet de siste årene og at det over tid har vært en profesjonalisering av dette arbeidet.
    - Det er god hjelp og støtte fra fagmiljøet i IT Digital sikkerhet. Det ble også trukket fram godt fagnettverk på sikkerhet også internt i en divisjon. Dette fremhever de som viktige faktorer som medvirker til at sluttresultatet på systemnivå for de enkelte system blir gode.
- Fra systemeiersiden ble det trukket fram viktigheten av å fortsette arbeidet for en god sikkerhetskultur og ytterligere øke modenheten knyttet til risikohåndtering.
- En gjennomgående utfordring som ble påpekt er at det ikke alltid er åpenbart hvem som eier en risiko, noe som kan gjøre det vanskelig å finne tiltak. Det kan også være utfordringer knyttet til tilfeller hvor andre enn systemeier er ansvarlig for de relevante risikoreduserende tiltakene.

Vegtilsynet stilte spørsmål om i hvilken grad tilsynspart vurderer at det blir identifisert og iverksatt tilstrekkelige risikoreduserende tiltak for å forhindre at uakseptable informasjonssikkerhetsrisikoer inntreffer.

- Tilsynspart uttrykte noe mindre trygghet på om de har god nok kontroll på om tiltak som iverksettes er tilstrekkelig og dekkende på tvers av ulike divisjoner og systemer.
    - De har et inntrykk av at det jobbes godt med tiltak, både identifisering, iverksetting og evaluering, så lenge dette er hensiktsmessig og i tråd med

den tidligere presenterte matrisen knyttet til myndighet for aksept av restrisiko.
    - Tilsynspart var kjent med kun en sak som hadde gått helt opp til vegdirektøren når det gjelder å akseptere restrisiko.

Vegtilsynet stilte spørsmål om de ser noen utfordringer eller svakheter i arbeidet med å identifisere risiko og iverksette risikoreduserende tiltak.
Enkelte områder ble her trukket fram:

- Det ene området er knyttet til sikkerhet på fysisk utstyr med lang levetid.
    - Det oppleves her som krevende å skule iverksette tiltak med lang nok levetid.
    - Dette kan være knyttet til utfordringer med finansiering eller at løsninger kan være vanskelig å finne for gamle systemer eller gammelt utstyr.
- Ett annet område som ble trukket fram er knyttet til informasjonssikkerhetsarbeidet mellom systemer og for oppfølging av tiltak som krever noe av noen utenfor det gitte systemet. Slike tilfeller forutsetter i dag manuelle prosesser og reguleres ikke av ledelsessystemet.

Vurdering

Ut fra den informasjon som ble gitt i tilsynsmøte vurderer Vegtilsynet at tilsynspart sitt arbeid med kontrollaktiviteter og risikoreduserende tiltak som tilfredsstillende. Krav, ansvar og myndighet synes å være tydelig definert knyttet til de ulike systemer og oppleves å bli etterlevd i praksis.

Samtidig registrerer Vegtilsynet at det finnes utfordringer knyttet til å definere eierskap. Dette gjelder både til selve risikoen i en del tilfeller og at det kan oppstå utfordringer i de tilfeller risikoreduserende tiltak involverer andre deler av virksomheten enn den som eier systemet eller risikoen.

Vegtilsynet vurderer at risiko eller ansvar for risikoreduserende tiltak som ligger utenfor egen kontroll vanskeliggjør en helhetlig risikostyring.

Funn 2 – observasjon

Statens vegvesen bør vurdere hvordan tiltak som ligger utenfor det enkelte system eller mellom systemer best kan iverksettes. Dette er viktig for å legge til rette for en helhetlig risikostyring og iverksette relevante risikoreduserende tiltak.

TK4: Virksomheten skal evaluere effekten av iverksatte tiltak

Vegtilsynet ønsket å få presentert hvordan det arbeides med å måle og evaluere om informasjonssikkerhetsarbeidet knyttet til de ulike systemer fungerer tilfredsstillende og stilte spørsmål om dette arbeidet er beskrevet i ledelsessystemet.

- Det ble fra systemeierne vist til at evaluering ligger som en del av oppgaven med å iverksette tiltak å bekrefte at risiko er redusert, enten ved testing eller øving.
    - Dette skal være en integrert del av gjennomføringen av tiltakene som identifiseres og iverksettes. Det er også slik at tiltak skal gjøres målbare.
- Tilsynspart understreket samtidig at risikovurdering er en repeterende og gjentakende (iterativ) aktivitet, ikke en statisk hendelse.
    - Om kort tid kan det ha åpnet seg andre risikoer og samme risiko vurderes annerledes.
    - At risiko kontinuerlig er i endring og at risikovurderingene derfor må være iterative medfører også at effektvurdering og -måling må ta høyde for disse iterasjonene.
- Tilsynspart orienterte også om at det er etablert støttefunksjonalitet rundt å følge opp og bistå systemeiere på om de klarer å ta ned risikoer som er identifisert, og særlig når det gjelder nye risikoer som kommer til.
    - Dette kan for eksempel være via ekstern bistand, input/intel fra NSM og andre leverandører, slik at risikovurderinger kan suppleres og oppdateres.

Vegtilsynet stilte spørsmål om hvordan tilsynspart arbeider med å måle og evaluere om det samlede ledelsessystemet for informasjonssikkerhet har den forventede og ønskede effekten.

- IT Digital sikkerhet orienterte om at det i virksomhetens mål- og resultatstyringssystem rapporteres på KPI-er som er satt innenfor informasjonssikkerhet.

- Det arbeides med å få på plass kontrollsystem som tilsvarer SoA (ISO27001)[9]. Etaten har ikke kommet så langt ennå, og bruker per i dag ISF sin SOGP for å teste hvordan man ligger an i henhold til dette kontrollrammeverket.
- Funnene fra «helsesjekken» i ISF brukes aktivt i styring av arbeid og aktivitet.

- Det ble også opplyst at det er mulig at tilsynspart i en periode framover vil kombinere SoA på strategisk nivå og SOGP på taktisk og operativt nivå.

Vurdering

Vegtilsynet vurderer, på grunnlag av diskusjonen i tilsynsmøtet, at tilsynspart har en god modenhet knyttet til behov for å drive kontinuerlig oppfølging og vurdering/effektevaluering av de tiltak de iverksetter og jobber med. Systemet for styring av risiko, herunder evaluering av effekt av de enkelte tiltak som settes i verk og målinger av selve ledelsessystemet reflekterer at tilsynspart forstår at risikobildet er dynamisk og i stadig endring.

Undersøkelsen har ikke avdekket avvik eller observasjoner

TK5: Virksomheten skal justere/tilpasse risikoreduserende tiltak/kontrollaktiviteter

Vegtilsynet stilte spørsmål ved om det har blitt avdekket behov for å gjøre justeringer eller tilpasninger i iverksatte tiltak. Dersom slike behov har blitt avdekket ønsket Vegtilsynet også å bli orientert om hvilke justeringer eller tilpasninger og for hvilke systemer.

- Tilsynspart orienterte om at de områder der det vurderes å være behov for oppfølging er på enkeltområder der ISF har oppdaterte krav, samt når det gjelder retningslinjer for bruk av kunstig intelligens.
  - Det ble videre vist til at «helsesjekken» i ISF viser at styringssystemet stadig blir bedre og at risikovurderingene og -håndteringen også stadig forbedres.

[9] En SoA (Statement of Applicability) er et obligatorisk dokument for ISO 27001-sertifisering som lister opp alle kontrollene i standardens vedlegg A, angir hvilke som er relevante for organisasjonen, og begrunner hvorfor de enten er inkludert eller utelatt. SoA vil dermed fungerer som en kobling mellom risikovurderingen og de faktiske sikkerhetstiltakene, og dokumenterer organisasjonens valg av kontroller for å håndtere informasjonssikkerhetsrisikoer.

Vurdering

Ut fra diskusjonen i tilsynsmøtet vurderer Vegtilsynet at tilsynspart sitt ledelsessystem for informasjonssikkerhet i all hovedsak fungerer godt når det gjelder risikostyring innen de enkelte systemer. Det er imidlertid, som en del løpende evalueringer av selve styringssystemet, identifisert forbedringspunkter som det arbeides fortløpende med å forbedre. Etter Vegtilsynet sin vurdering synes dette å være en indikasjon på at tilsynspart sitt system for styring av digital sikkerhet fungerer på et overordnet nivå.

Undersøkelsen har ikke avdekket avvik eller observasjoner

5. Konklusjon

Samlet sett er det Vegtilsynets vurdering at diskusjonen i tilsynsmøtet viser at tilsynspart har et styringssystem som i betydelig grad sikrer at krav til digital sikkerhet, knyttet til veginfrastrukturen, blir oppfylt.

Tilsynspart sitt arbeid for å identifisere og håndtere risiko synes å være betryggende og velfungerende for de systemer som omfattes av virksomhetens ledelsessystem for informasjonssikkerhet.

Ut fra hva som kom fram i tilsynsmøtet stiller Vegtilsynet likevel spørsmål ved om tilsynspart har en tilstrekkelig systematisk tilnærming til å holde oversikt over alle digitale systemer og om det foretas overordnede risikovurderinger av alle systemer. Dersom tilsynspart ikke har tilstrekkelig oversikt over digitale systemer som ikke håndteres innenfor ledelsessystemet vil dette kunne innebære en risiko for uønskede hendelser.

Videre registrerer Vegtilsynet at det i enkelte tilfeller finnes utfordringer knyttet til å definere eierskap både til risiko og håndteringen av denne. Som eksempler på slike tilfeller ble det trukket situasjoner hvor risikoreduserende tiltak involverer andre deler av virksomheten enn den som eier systemet eller risikoen. Dette er forhold som etter Vegtilsynets vurdering vanskeliggjør en helhetlig risikostyring.

Tilsynspart sitt ledelsessystem for informasjonssikkerhet fungerer etter Vegtilsynets vurdering altså i all hovedsak godt når det gjelder risikostyring innen de enkelte systemer som inngår i ledelsessystemet. De forbedringspunkter Vegtilsynet påpeker virker imidlertid i stor grad å være sammenfallende med hva tilsynspart selv også har identifisert som forbedringspunkter. Etter Vegtilsynet sin vurdering synes dette å være en indikasjon på at tilsynspart sitt system for styring av digital sikkerhet fungerer på et overordnet nivå.

Det er i tilsynssaken gitt to observasjoner.