Riksrevisjonen

Revisjonsrapport for 2017 om styringssystem for informasjonssikkerhet i Arbeidstilsynet

Mottaker: Arbeids- og sosialdepartementet

Revisjonen er en del av Riksrevisjonens kontroll av disposisjoner i henhold til *lov om Riksrevisjonen* § 9 første ledd og *instruks om Riksrevisjonens virksomhet* § 3b. Revisjonen er gjennomført i samsvar med ISSAI 400/4000, INTOSAIs internasjonale prinsipper og standarder for etterlevelsesrevisjon.

Forside-illustrasjon: Riksrevisjonen

Innhold

1 Sammendrag

Målet med revisjonen har vært å kontrollere om Arbeidstilsynet har et styringssystem for informasjonssikkerhet i henhold til kravene i eForvaltningsforskriften og som ivaretar krav i personopplysningsloven.

Betydningen av gode styringssystemer for informasjonssikkerhet og beskyttelse av sensitiv informasjon øker i takt med digitaliseringen av offentlig forvaltning. Det er viktig at offentlige virksomheter beskytter informasjon de forvalter, og sørger for at nettverk og systemer til enhver tid er sikre og stabile.

I sin tilsynsvirksomhet har Arbeidstilsynet rett til å få framvist opplysninger som anses som nødvendige for tilsynet,[1] og tilsynet forvalter blant annet sensitive personopplysninger om arbeidstakere, blant annet informasjon knyttet til personskade og sykdom som oppstår i arbeidssammenheng. Arbeidstilsynet er dermed avhengig av god informasjonssikkerhet for å sikre at informasjonen det forvalter ikke kommer på avveie.

Revisjonen har tatt utgangspunkt i følgende lover, vedtak og forutsetninger fra Stortinget:

- *Forskrift om elektronisk kommunikasjon med og i Forvaltningen* (eForvaltningsforskriften) § 15
- *Lov om behandling av personopplysninger* (personopplysningsloven)
- *Forskrift om behandling av personopplysninger* (personopplysningsforskriften)

Etter eForvaltningsforskriften § 15 andre ledd skal forvaltningsorganet «ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder[2] for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem». Forskriftens § 15 stiller videre krav til at intern kontrollen skal inkludere relevante krav som inngår i annen lovgivning. *Lov om behandling av personopplysninger* (personopplysningsloven) stiller krav til informasjonssikkerhet for informasjonssystemer som behandler personopplysninger.

Riksrevisjonen har også lagt til grunn anbefalinger fra Den internasjonale standardiseringsorganisasjonen (ISO), Nasjonal sikkerhetsmyndighet (NSM) og Center for Internet Security (CIS), ut fra den forutsetning om at dette er beste praksis for styring og gjennomføring av sikkerhetstiltak.

Revisjonen omfatter Arbeidstilsynets arbeid med styring av informasjonssikkerhet, herunder sikkerhetsmål og sikkerhetsstrategier, samt klassifisering og risikovurdering for sikring av informasjon. Videre at det, med bakgrunn i risikovurderinger, er etablert risikoreduserende sikkerhetstiltak som er effektive, og om tiltak blir løpende oppdatert tilpasset endringer i risikobildet. Det er også foretatt kontroll av om Arbeidstilsynet evaluerer og oppdaterer styringssystemet med bakgrunn i observerte sikkerhetshendelser og sikkerhetsrevisjoner.

Revisjonen er gjennomført ved dokumentanalyse, møter, observasjoner og analyse av uttrekk fra Arbeidstilsynets IKT-systemer.

Revisjonen viser at Arbeidstilsynet har innført et styringssystem for informasjonssikkerhet som delvis dekker kravene i eForvaltningsforskriften § 15 og personopplysningsloven.

- Arbeidstilsynet har et styringssystem for informasjonssikkerhet som definerer prosessene for arbeidet med informasjonssikkerhet og planlegging av sikkerhetstiltak, men ikke hvordan arbeidet med informasjonssikkerhet skal evalueres og forbedres.
- Arbeidstilsynet har klassifisert systemene, men ikke gjennomført risikovurderinger, slik det er beskrevet i styringssystemet, for alle systemene Tilsynet har heller ikke dokumentert hvilke sikkerhetstiltak som skal gjennomføres.
- Arbeidstilsynet har ikke utarbeidet policy, retningslinjer eller rutiner for sikkerhetstiltak, og har i varierende grad gjennomført og fulgt opp tiltak i henhold til beste praksis.
- Arbeidstilsynet har ikke et helhetlig system for registrering, håndtering og oppfølging av informasjonssikkerhetshendelser.
- Arbeidstilsynet har ikke fulgt opp om styringssystemet fungerer etter hensikten eller vurdert om det er behov for endringer.

[1] Arbeidsmiljøloven § 18-5.
[2] Anbefalinger gitt i NS-ISO/IEC 27001:2017 og NS-ISO/IEC 27002:2017

Revisjonen er basert på regelverk gjeldende i 2017. EU-forordning 2016/679 (personvernforordningen/GDPR) trer i kraft i 2018. Forordningen er en videreføring av tidligere regelverk, men inneholder flere detaljreguleringer og tilstramminger, i tillegg til noen nye prinsipper. Manglende etterlevelse av krav i lover og regler på tidspunktet for revisjonen, vil i like stor grad gjelde etter at den nye personvernloven er gjort gjeldende.

Utkast til rapport ble lagt fram for Arbeids- og sosialdepartementet ved brev 23. mars 2018. Departementet har i brev 23. april 2018 gitt kommentarer til rapportutkastet. Kommentarene er innarbeidet i endelig rapport.

Departementet hovedoppfatning er at revisjonsrapporten er dekkende for den faktiske situasjonen ved Arbeidstilsynet. På bakgrunn av funnene avdekket i revisjonen har departementet innhentet informasjon fra Arbeidstilsynet som viser at etaten planlegger å iverksette tiltak blant annet knyttet til:

- Krav til og gjennomføring av interne revisjoner, samt systematisk evaluering og kontinuerlig forbedring av styringssystemet
- Forankring av risikoarbeidet på informasjonssikkerhetsområdet som en del av den ordinære virksomhetsstyringen
- Dokumentere og følge systemsikkerhetsplaner, herunder en kontroll av gjennomførte risikovurderinger
- Gjennomgang og etablering av operasjonelle rutiner og retningslinjer på flere områder under IT-drift
- Tydeliggjøring om bruk av avvikssystemet og oppfølging av hendelser.

2 Innledning

Arbeidstilsynet er underlagt Arbeids- og sosialdepartementet. Arbeidstilsynets hovedoppgave er å føre tilsyn med at virksomheter følger kravene i arbeidsmiljøloven.[3] Etaten skal bidra til et seriøst, trygt og inkluderende arbeidsliv ved særskilt å følge opp to hovedprioriteringer:[4]

- useriøsitet, sosial dumping og arbeidslivskriminalitet
- manglende systematisk HMS-arbeid, som fører til høy risiko for helseskader

I gjennomføringen av primæroppgavene har Arbeidstilsynet rett til å få framvist opplysninger som anses som nødvendige for tilsynet,[5] og tilsynet forvalter blant annet sensitive personopplysninger om arbeidstakere, blant annet knyttet til personskade og sykdom som oppstår i arbeidssammenheng.

Det er viktig at offentlige virksomheter beskytter informasjon de forvalter, og sørger for at nettverk og systemer til enhver tid er sikre og stabile. Betydningen av gode styringssystemer for informasjonssikkerhet og beskyttelse av sensitiv informasjon[6] øker i takt med digitaliseringen av offentlig forvaltning.

Et styringssystem for informasjonssikkerhet skal hjelpe ledelsen og virksomheten for øvrig med å ha tilstrekkelig styring og kontroll på informasjonssikkerheten gjennom systematisk internkontroll på området. Styringssystemet skal bidra til at virksomheten velger riktige sikkerhetstiltak og sørge for at de valgte løsningene blir evaluert og om nødvendig forbedret. Manglende styring og ledelsesinvolvering kan føre til at virksomheten ikke gjennomfører nødvendige analyser av sikringsbehov før de iverksetter tiltakene. Svakheter i sikkerhetstiltak kan indikere at styringssystemet ikke fungerer på alle områder, enten ved at svakhetene ikke er identifisert, eller at korrigerende tiltak ikke er iverksatt. Manglende sikkerhetstiltak kan føre til uheldige konsekvenser for enkeltpersoner og for samfunnet og/eller skade omdømmet til offentlige virksomheter.

Arbeidstilsynet er organisert med ett direktorat og sju regioner med tilsynskontor over hele landet.[7] Direktoratet ligger i Trondheim og har ansvar for blant annet strategi, styring, utvikling, regelverk og kommunikasjon. Direktoratet er også systemeier for etatens fagsystemer. Regionkontorene har ansvar for tilsyn i virksomheter i regionen og gir veiledning og informasjon i sitt geografiske område og for sine nasjonale fagområder. Hver region ledes av en regionsdirektør. I 2016 hadde Arbeidstilsynet 662 ansatte.[8]

[3] Arbeidsmiljøloven § 18-1.
[4] Tildelingsbrev fra Arbeids- og sosialdepartementet til Arbeidstilsynet for 2017.
[5] Arbeidsmiljøloven § 18-5.
[6] Nasjonal strategi for informasjonssikkerhet har definert sensitiv informasjon til å være informasjon det av ulike hensyn er viktig å beskytte.
[7] Arbeidstilsynets hjemmeside (http://www.arbeidstilsynet.no/om/index.html?tid=207114#Regionene).
[8] Arbeidstilsynets årsrapport for 2016.

Behandlingen av sensitive personopplysninger skjer gjennom bruk av etatens fagsystem Betzy varsel og arkivsystemet ePhorte. I Betzy tilsyn dokumenterer tilsynet sin ordinære tilsynsvirksomhet. Innføringen av Betzy-systemene startet gradvis i 2012 og utgjør i dag Arbeidstilsynets primære fagsystem. Alle inspektører og tilsynsledere bruker fagsystemet til all tilsyns- og veiledningsaktivitet, i forberedelser, gjennomføring og oppfølging av tilsyn. Til kommunikasjon, herunder rapportering av tilsyn, og oppbevaring av annen arkivverdig informasjon bruker Arbeidstilsynet arkivsystemet ePhorte. Arbeidstilsynet drifter sin egen IKT-infrastruktur og egne systemer, og dette gjøres fra direktoratet i Trondheim.

3 Revisjonens mål og problemstillinger

Målet med revisjonen er å kontrollere om Arbeidstilsynet har et styringssystem for informasjonssikkerhet i henhold til kravene i eForvaltningsforskriften og som ivaretar krav i personopplysningsloven[9].

Revisjonen er gjennomført med utgangspunkt i tre problemstillinger:

1) Har Arbeidstilsynet etablert et grunnlag for å planlegge sikkerhetstiltak som skal bidra til tilfredsstillende informasjonssikkerhet?

2) Problemstillingen omfatter Arbeidstilsynets arbeid med styring av informasjonssikkerhet, herunder sikkerhetsmål og sikkerhetsstrategier, samt klassifisering og risikovurderinger for sikring av informasjon.

3) Har Arbeidstilsynet sikret at det gjennomføres systematiske tiltak som skal bidra til å sikre tilfredsstillende informasjonssikkerhet?

4) Problemstillingen omfatter et utvalg tiltak som påvirker sikkerheten for informasjonen i Betzy varsel, Betzy tilsyn og ePhorte med underliggende infrastruktur.

5) Følger Arbeidstilsynet opp at styringssystemet og tiltak gir tilfredsstillende informasjonssikkerhet?

6) Problemstillingen omfatter rutiner for avviksbehandling samt hvordan Arbeidstilsynet følger opp at styringssystemet fungerer etter hensikten.

4 Metoder

Problemstillingene er besvart gjennom dokumentanalyse, møter, observasjoner og analyse av uttrekk fra Arbeidstilsynets IKT-systemer.

Det er tatt utgangspunkt i systemene Betzy tilsyn, Betzy varsel og ePhorte gjennom hele revisjonen. Dette er på bakgrunn av informasjon som lagres disse systemene.

Det er avholdt et oppsummeringsmøte med Arbeidstilsynet 16. februar 2018 hvor formålet var å avklare faktagrunnlaget for de enkelte problemstillingene. Resultatet av revisjonen ble presentert for Arbeids- og sosialdepartementet den 6. mars 2018.

4.1. Problemstilling 1 og 3 – planlegging og oppfølging av sikkerhetstiltak

For å besvare problemstillingen er det gjennomført dokumentanalyse og møter.

Dokumentanalyse
Dokumentanalyse er gjennomført for å kontrollere om Arbeidstilsynet har utarbeidet og dokumentert krav til informasjonssikkerhetsarbeidet i virksomheten. Dette inkluderer kontroll av om Arbeidstilsynet har utarbeidet rutiner for, og gjennomfører klassifisering av informasjonsaktiva, risikoanalyser og interne revisjoner.

[9] *Lov om behandling av personopplysninger* (personopplysningsloven) 14. april 2000 nr. 31.

Analysen omfatter:

- styrende dokumenter
  - *Policy for informasjonssikkerhet i Arbeidstilsynet*, datert 1. desember 2012
  - *Strategi for informasjonssikkerhet*, datert 28. mai 2013
  - *Retningslinjer for klassifisering av informasjonssystemer*, datert 18. mars 2014
  - *Sjekkliste for informasjonssikkerhet*, datert 17. august 2016
- klassifiseringsdokumenter
  - Betzy varsel, datert 23. mai 2015
  - Betzy tilsyn, datert 5. november 2014
  - ePhorte, datert 19. juni 2012
- risikoanalyser
  - Betzy varsel, datert 11. november 2015
  - Betzy tilsyn, datert 8. april 2015
  - ePhorte, datert 20. mars 2013

Andre aktuelle dokumenter er identifisert og beskrevet under det relevante området i rapportens punkt 6.1.

Møter
For å få utfyllende informasjon om hvordan Kartverket arbeider med de ulike områdene omfattet av problemstilling 1 og 3 er det gjennomført møter med nøkkelpersoner på informasjonssikkerhetsområdet.

Referatet fra møtet er verifisert av Arbeidstilsynet i e-post av 4. desember 2017.

4.2. Problemstilling 2 – gjennomføring av sikkerhetstiltak

For å besvare problemstillingen er det gjennomført møter, analyser av uttrekk fra Arbeidstilsynets systemer, observasjoner, gjennomgang av rutiner og styrende dokumenter.

Det er kontrollert et utvalg tiltak med utgangspunkt i systemene Betzy tilsyn, Betzy varsel og ePhorte samt underliggende infrastruktur. Sikkerhetstiltakene er valgt på bakgrunn av hva anerkjente aktører innenfor informasjonssikkerhet anser som viktigst for å redusere risiko på informasjonssikkerhetsområdet.[10] Det er lagt til grunn at Arbeidstilsynet gjennom styringssystemet har vurdert og håndtert risiko ved å implementere grunnleggende sikkerhetstiltak på følgende områder:

- tilgangskontroller
  - saksbehandlerrettigheter i applikasjonene
  - administratorrettigheter
- logging og oppføling av logger for applikasjon og underliggende infrastruktur
- oppdatering av operativsystem og programvare
- kontroll med programvare og enheter i nettverket

I tillegg er det vurdert om det foreligger policy, retningslinjer og rutiner, og om det er gjennomført etterkontroll/evaluering for det enkelte sikkerhetstiltak.

Revisjonen av de utvalgte sikkerhetstiltakene vil ikke gi et fullstendig bilde av sikkerhetstilstanden ved Arbeidstilsynet. Resultatene gir imidlertid en indikasjon på om styringssystemet fungerer etter hensikten.

Revisjonen beskriver situasjonen på tidspunktene for gjennomførte revisjonsbesøk og uttrekk av data per utgangen av november 2017.

[10] Kilder til tiltak for god informasjonssikkerhet:
- The Center for Internet Security (CIS), *CIS Controls for Effective Cyber Defense*
- Nasjonal sikkerhetsmyndighet, Ti viktige tiltak mot dataangrep
- Australian Signals Directorate, Top 4/Top 35 (Strategies to Mitigate Targeted Cyber Intrusions)

Dokumentanalyse
Det er gjennomført dokumentanalyse for å undersøke om Arbeidstilsynet har dokumentert krav til sikkerhetstiltak på områdene som er omfattet av revisjonen. Sikkerhetstiltak er på et overordnet nivå beskrevet i følgende dokumenter:

- *Retningslinjer for klassifisering av informasjonssystemer*, datert 18. mars 2014
- *Retningslinje for sikring av nettverk og infrastruktur*, datert 14. september 2012
- *Retningslinje for sikring av systemer og applikasjoner*, datert 15. oktober 2012

Underliggende og eventuelt andre dokumenter som belyser området, er identifisert og beskrevet under i rapportens punkt 6.2.1.

Møter
For å sikre korrekt forståelse av hvordan sikkerhetsarbeidet foregår i Arbeidstilsynet, gjøre observasjoner og gjennomgå data for analyse er det gjennomført møter med nøkkelpersoner fra Arbeidstilsynet 21. og 22. november 2017.

Dataanalyse og observasjoner
Det er gjort observasjoner for å få innsikt i hvordan ulike systemer hos Arbeidstilsynet blir brukt og fungerer, samt om aktuelle sikkerhetstiltak er innført.

Det er mottatt data og gjennomført analyser av uttrekk av:

- Active Directory (AD), katalogtjenesten Arbeidstilsynet bruker til å håndtere brukere, brukerrettigheter og ressurser
- installert programvare, oppdateringer av operativsystem og programvare, samt brukere med administratorrettigheter fra applikasjonsservere for Betzy (varsel og tilsyn) og ePhorte og 60 aktive PC-er i nettverket
- tilgangsrettigheter, innstillinger og oppdateringer fra databasene for Betzy (varsel og tilsyn) og ePhorte

Det er oversendt oppfølgingsspørsmål om resultatene fra analysene, som Arbeidstilsynet har gitt tilbakemelding på i e-post av 30. januar 2018.

5 Revisjonskriterier

I dette kapitlet presenteres overordnede krav til informasjonssikkerhet i staten og felles krav for behandling av personopplysninger. Videre vil anerkjente standarder bli presentert, samt revisjonskriterier knyttet til hver av revisjonens problemstillinger.

Forskrift om elektronisk kommunikasjon med og i forvaltningen 25. juni 2004 nr. 988 (eForvaltningsforskriften)[11] er et virkemiddel for å styrke informasjonssikkerheten. Formålet er å legge til rette for sikker bruk av elektronisk kommunikasjon og å sikre hensiktsmessige tekniske løsninger.

Forskriften stiller krav til styring og kontroll med informasjonssikkerhet i statlige forvaltningsorganer. Styringssystemet skal etter § 15 fjerde ledd bokstav g) også inkludere krav som er fastsatt i og i medhold av personopplysningsloven. *Lov om behandling av personopplysninger* 14. april 2000 nr. 31 (personopplysningsloven) § 13 stiller krav til informasjonssikkerhet for informasjonssystemer som behandler personopplysninger. Nærmere krav om organisatoriske og tekniske sikkerhetstiltak går fram av *forskrift om behandling av personopplysninger* 15.desember 2000 nr. 1265 (personopplysningsforskriften) [12] kapittel 2.

Etter eForvaltningsforskriften § 15 andre ledd skal forvaltningsorganet «ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem».

[11] Hjemlet i *lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker* (forvaltningsloven) § 15 a mfl.
[12] Fastsatt ved kgl.res. 15. desember 2000 med hjemmel i lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

Som anerkjente standarder vil revisjonen ta utgangspunkt i anbefalinger gitt i NS-ISO/IEC 27001:2017 (ISO 27001) og NS-ISO/IEC 27002:2017 (ISO 27002).[13] Bruk av standardene må tilpasses virksomhetens egenart.

For å oppfylle kravene i personopplysningsloven viser Datatilsynet i *Skjema for internkontroll* til at virksomheter som et minimum må følge alle obligatoriske krav i NS-ISO/IEC 27001. Videre viser Datatilsynet til at NS-ISO/IEC 27002 gir beste praksis for å oppfylle disse kravene.[14]

Av lovforarbeidene til personopplysningsloven[15] går det fram at tilfredsstillende informasjonssikkerhet forutsetter etablering av både organisatoriske og tekniske sikkerhetstiltak. En vurdering av hvilke tiltak som må til for å oppnå lovkravene om tilfredsstillende informasjonssikkerhet, skal gjøres på bakgrunn av risikoanalysen. Sikringen av konkrete personopplysninger avhenger av hvilke trusler disse er utsatt for.

Revisjonskriteriene under punktene 5.1–5.3 er ytterligere spesifisert under de aktuelle områdene i rapportens kapittel 6 *Funn*.

De foreløpige revisjonskriteriene er lagt fram for Arbeids- og sosialdepartementet i brev av 22. september 2017. Departementet hadde ingen merknader til de foreløpige revisjonskriteriene.

Revisjonen har tatt utgangspunkt i gjeldende regelverk i 2017. EU-forordning 2016/679 (personvernforordningen/GDPR) trer i kraft i 2018. Forordningen er en videreføring av tidligere regelverk, men inneholder flere detaljreguleringer og tilstramminger, i tillegg til noen nye prinsipper. Manglende etterlevelse av krav i lover og regler på tidspunktet for revisjonen vil gjelde i like stor grad etter at den nye personvernloven er gjort gjeldende.

5.1. Problemstilling 1 – grunnlag for og planlegging av sikkerhetstiltak

eForvaltningsforskriften § 15 stiller blant annet følgende krav til planlegging av sikkerhetstiltak:

- Første ledd: «Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.)»

- Tredje ledd: «Omfang og innretning på internkontrollen skal være tilpasset risiko.»

Krav til internkontroll på informasjonssikkerhetsområdet forutsetter etablering av både organisatoriske og tekniske sikkerhetstiltak.[16]

Etter personopplysningsforskriftens § 2-3 skal formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi beskrives i et sikkerhetsmål. Videre skal valg og prioriteringer i sikkerhetsarbeidet beskrives i en sikkerhetsstrategi.

Etter personopplysningsforskriften § 2-4 skal det føres oversikt over hva slags personopplysninger som behandles. Sikringen av konkrete personopplysninger avhenger av hvilke trusler opplysningene er utsatt for. En vurdering av hvilke tiltak som er nødvendig for å oppfylle kravene til behandling av personopplysninger etter personopplysningsloven § 13 og personopplysningsforskriften kapittel 2, skal gjøres på bakgrunn av risikoanalysen.

[13] http://standard.difi.no/forvaltningsstandarder/referansekatalogen-html-versjon/.
14 Datatilsynet.no, *Skjema for internkontroll*. <https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/etablering-internkontroll/Internkontroll-skjema-egenkontroll/> (Hentedato 15.12.2017)
[15] Ot.prp. nr. 92 (1998–99) Kapittel 16 *Kommentarer til enkeltparagrafer*, § 13.
[16] Ot.prp. nr. 92 (1998–99) Kapittel 16 *Kommentarer til enkeltparagrafer*, § 13.

5.2. Problemstilling 2 – gjennomføring av sikkerhetstiltak

Med utgangspunkt i eForvaltningsforskriften § 15 fjerde ledd bokstav g) stiller personopplysningsloven § 13 blant annet følgende krav til sikkerhetstiltak ved behandling av personopplysninger:

- Den behandlingsansvarlige[17] og databehandleren[18] skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

- For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene.

Nærmere krav til regler om organisatoriske og tekniske sikkerhetstiltak går fram av personopplysningsforskriften kapittel 2. Vurdering av hvilke tiltak som må gjennomføres for å oppfylle lovkravene om tilfredsstillende informasjonssikkerhet, skal gjøres på bakgrunn av risikoanalyser. Sikring av konkrete personopplysninger avhenger av hvilke trusler disse er utsatt for. Revisjonen har tatt utgangspunkt i følgende krav:

- I henhold til § 2-7 skal informasjonssystemet konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås, og konfigurasjonen skal dokumenteres.

- I henhold til § 2-8 første ledd skal medarbeidere hos den behandlingsansvarlige bare bruke informasjonssystemet til å utføre pålagte oppgaver og selv være autorisert for slik bruk. Videre krever § 2-8 tredje ledd at autorisert bruk av informasjonssystemet skal registreres.

- I henhold til § 2-11 skal det treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er viktig. Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten.

- I henhold til § 2-13 skal det treffes tiltak mot uautorisert endring i personopplysninger hvor integritet er viktig. Sikkerhetstiltakene skal også hindre uautorisert endring i annen informasjon med betydning for informasjonssikkerheten. Videre skal det treffes tiltak mot ødeleggende programvare.

- I henhold til § 2-14 skal sikkerhetstiltakene gjøre det mulig å oppdage forsøk på uautorisert bruk. Forsøk på uautorisert bruk skal registreres. Sikkerhetstiltakene skal dokumenteres.

- I henhold til § 2-16 skal rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten dokumenteres.

ISO 27002 gir detaljerte anbefalinger for gjennomføring av sikkerhetstiltak.

Revisjonen er også basert på anbefaling fra Nasjonal sikkerhetsmyndighet (NSM), Center for Internet Securitys (CIS) Critical Security Controls og andre anbefalinger fra relevante aktører og leverandører.

5.3. Problemstilling 3 – oppfølging og evaluering av styringssystemet

Med utgangspunkt i eForvaltningsforskriften § 15 fjerde ledd bokstav g) og personopplysningsloven § 13 stiller personopplysningsloven § 14 krav om internkontroll for å vedlikeholde informasjonssikkerheten:

- Den behandlingsansvarlige skal etablere og holde ved like planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

Nærmere krav til vedlikehold av tiltak går fram av personopplysningsforskriften. I § 2-3 framgår det at den daglige ledelsen har ansvar for at bestemmelsene i forskriftens kapittel 2 er fulgt. Videre framgår det at bruk av informasjonssystemet jevnlig skal gjennomgås for å klarlegge om det er hensiktsmessig for virksomheten og gir

[17] Jf. personopplysningsloven § 2 nr. 4, «behandlingsansvarlige: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes».
[18] Jf. personopplysningsloven § 2 nr. 5, «databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige».

tilfredsstillende informasjonssikkerhet. Av personopplysningsforskriften § 2-5 går det videre fram at det jevnlig skal gjennomføres sikkerhetsrevisjon av bruk av informasjonssystemet.

Av forskriftens § 2-6 går det fram at bruk av informasjonssystemet som er i strid med fastlagte rutiner og sikkerhetsbrudd, skal behandles som avvik. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse. Resultatet av avviksbehandlingen skal dokumenteres.

Videre gir ISO-standardene mer detaljerte anbefalinger for vedlikehold av informasjonssikkerheten.

6 Funn

I dette kapitlet presenteres revisjonskriterier og funn for hver av områdene under de tre problemstillingene revisjonen dekker.

I tillegg til beskrivelsen i dette kapitlet er det utarbeidet et vedlegg med en mer detaljert framstilling av revisjonens funn for problemstilling 2.

6.1. Problemstilling 1 – grunnlag for og planlegging av sikkerhetstiltak

6.1.1. Sikkerhetsmål og sikkerhetsstrategi

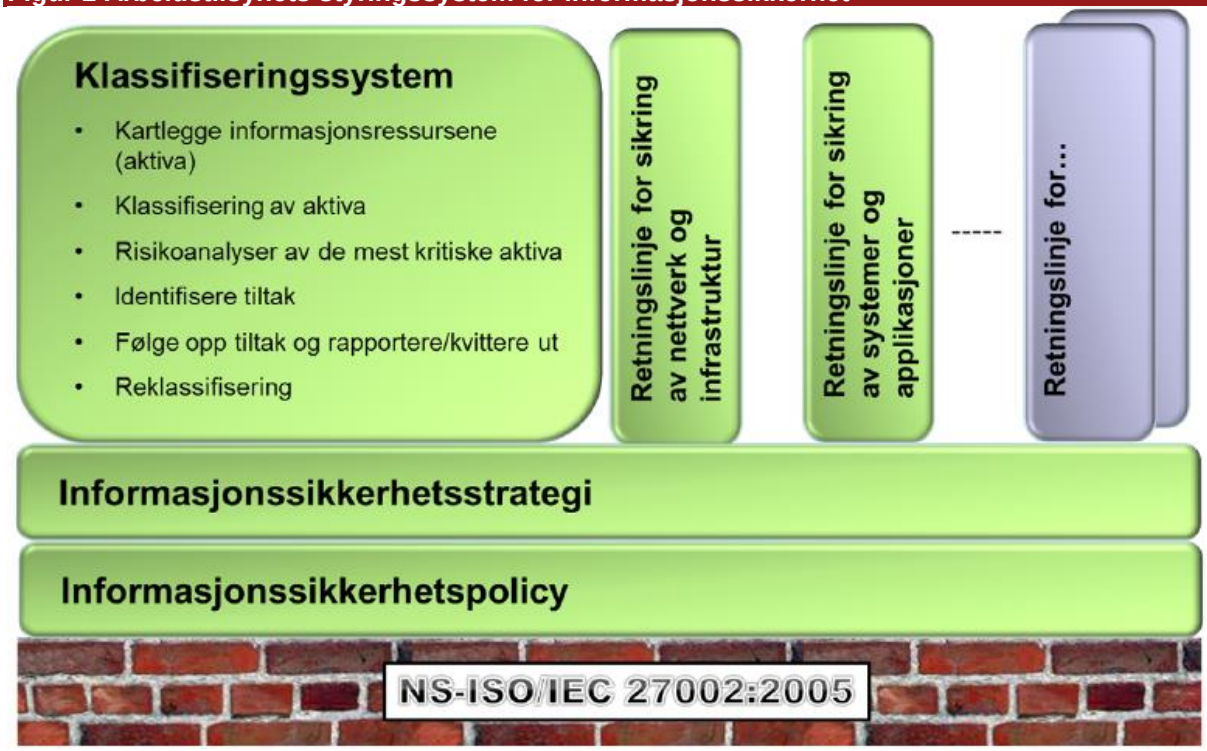
Ifølge eForvaltningsforskriften § 15 første ledd skal mål og strategi for informasjonssikkerhet i virksomheten være beskrevet (sikkerhetsmål og sikkerhetsstrategi) og danne grunnlaget for virksomhetens internkontroll (styring og kontroll) på informasjonssikkerhetsområdet.

ISO 27001 anbefaler i punkt 5.2 at virksomhetens øverste ledelse utarbeider en sikkerhetspolicy som definerer rammene for arbeidet med informasjonssikkerhet i virksomheten. En policy bør videre inneholde en forpliktelse til å oppfylle aktuelle krav til informasjonssikkerhet, og en forpliktelse til kontinuerlig forbedring av styringssystemet. Videre er det i punkt 5.2 anbefalt at policyen kommuniseres og gjøres tilgjengelig innad i virksomheten og til aktuelle parter.

ISO 27002 punkt 5.1.1 anbefaler at virksomheten beskriver formål og ansvar for styring av informasjonssikkerhet, samt prinsipper for vesentlige aktiviteter. Revisjonen legger til grunn at prinsipper for klassifisering, risikostyring, hendelseshåndtering, interne revisjoner, evaluering og kontinuerlig forbedring bør gå fram av styringssystemet.

Sikkerhetsmål og strategier
Arbeidstilsynet opplyser at de har bygget opp styringssystemet for informasjonssikkerhet på bakgrunn av anbefalinger i NS-ISO/IEC 27002:2005. Styringssystemet er bygget opp som vist i figur 1.

Figur 1 Arbeidstilsynets styringssystem for informasjonssikkerhet



Kilde: Arbeidstilsynet

Styringssystemet for informasjonssikkerhet består av følgende dokumenter:

- *Policy for informasjonssikkerhet i Arbeidstilsynet datert* 1. desember 2012
- *Strategi for informasjonssikkerhet*, datert 28. mai 2013
- *Retningslinjer for klassifisering av informasjonssystemer*, datert 18. mars 2014
- *Retningslinje for sikring av nettverk og infrastruktur*, datert, 14. september 2012
- *Retningslinje for sikring av systemer og applikasjoner,* datert, 15. oktober 2012
- veiledninger

Revisjonen viser at Arbeidstilsynet har satt mål for arbeidet med informasjonssikkerhet. Videre har Arbeidstilsynet definert prinsipper, roller og ansvar for informasjonssikkerhetsarbeidet. Av dokumentene framgår også relevante lovkrav, samt prinsipper for klassifisering, risikostyring og at sikkerhetsbrudd skal registreres og følges opp. Styringssystemet skal fungere etter «plan-do-check-act»-prinsippet[19]. Arbeidstilsynet har imidlertid ikke definert prinsipper for interne revisjoner, evalueringer av og kontinuerlig forbedring av styringssystemet.

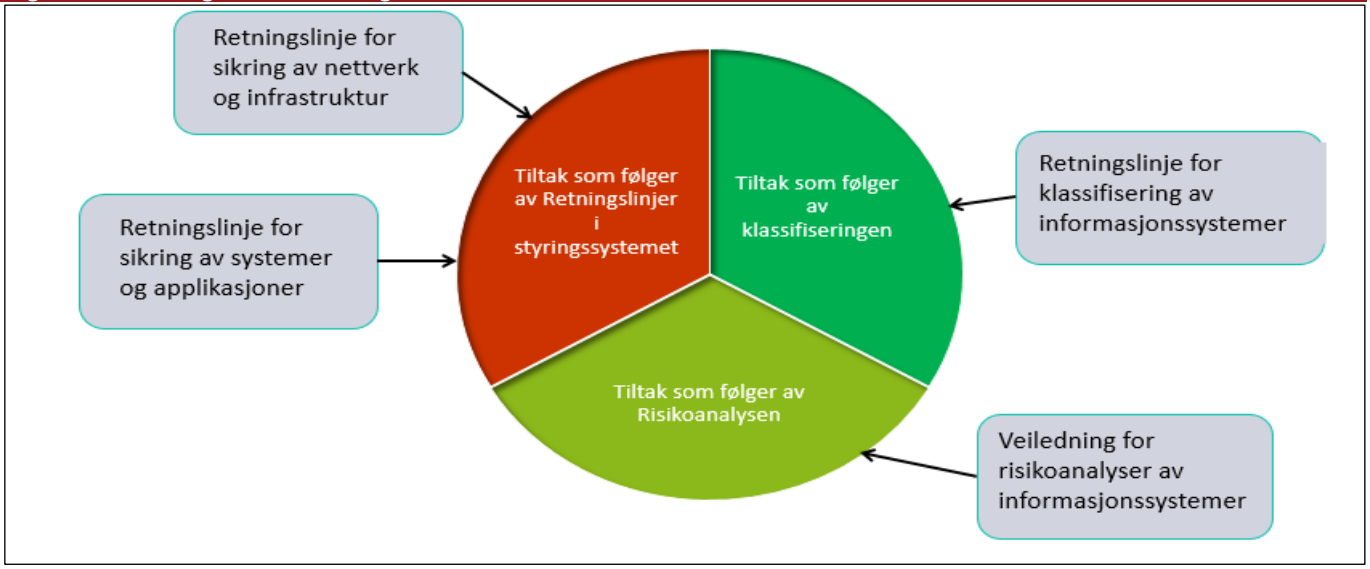
Revisjonen viser at det er avvik mellom styringssystemet og hvordan Arbeidstilsynet praktiserer arbeidet med informasjonssikkerhet. Et eksempel på dette er at ansvarsforholdene som er beskrevet i *informasjonssikkerhetspolicyen*, ikke synes være i samsvar med hvordan informasjonssikkerhetsarbeidet i Arbeidstilsynet er organisert.

Revisjonen viser at Arbeidstilsynets rammeverket for styringssystemet for informasjonssikkerhet er tilgjengeliggjort på tilsynets intranett. Arbeidstilsynet har utarbeidet dokumentet *Styringssystem for informasjonssikkerhet i Arbeidstilsynet – Introduksjon*[20] *for å* øke bevisstheten og gjøre styringssystemet kjent i organisasjonen.

Grunnlag for sikkerhetstiltak
Av Arbeidstilsynets styringssystem for informasjonssikkerhet går det fram at sikkerhetstiltak skal følge av retningslinjer i styringssystemet, av klassifiseringen og som følge av risikoanalysen.

[19] Etablere, iverksette og forvalte, overvåke og revidere samt vedlikeholde og forbedre.
[20] *Styringssystem for informasjonssikkerhet i Arbeidstilsynet - Introduksjon*, versjon 2.1 datert 23.1.2015.

Figur 2 Grunnlag for etablering av sikkerhetstiltak



Kilde: Arbeidstilsynet

Retningslinje for sikring av nettverk og infrastruktur definerer tiltak som skal etableres i Arbeidstilsynets nettverk, herunder sikker sone[21]. Av *Retningslinje for sikring av systemer og applikasjoner* følger tiltak som skal etableres på system- og applikasjonsnivå.

Avsnittet «Implementering av tiltak» i *Retningslinjer for klassifisering av informasjonssystemer* angir hvilke krav som stilles til etablering av tiltak, ut fra hvilken sikkerhetsklasse systemet er plassert i. Sikkerhetsklasse A stiller de strengeste kravene til tiltak, blant annet ved at systemet plasseres i sikker sone i Arbeidstilsynets nettverk. Tilsynet opplyser at alle sensitive personopplysninger lagres og oppbevares i en sikker sone, hvor kun autoriserte brukere skal ha tilgang.

Av informasjonssikkerhetsstrategien går det fram at det skal utarbeides en systemsikkerhetsplan på bakgrunn av gjennomførte risikoanalyser. Planen skal vise summen av tiltak som skal iverksettes som følge av retningslinjer i styringssystemet, klassifiseringen og risikoanalysen.

6.1.2. Identifisering og klassifisering av informasjonsaktiva/-verdier

Ifølge eForvaltningsforskriften § 15 fjerde ledd bokstav g) skal sikkerhetsstrategien og internkontrollen også stille nødvendig krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon etter personopplysningsloven § 13, og personopplysningsforskriften kapittel 2. Personopplysningsforskriften § 2-4 stiller krav om at det skal føres oversikt over hvilke personopplysninger som behandles.

ISO 27002 punkt 8.1 anbefaler at aktiva tilknyttet informasjon eller behandling av informasjon identifiseres og registreres, og at det utpekes en eier som har ansvar for det enkelte aktiva. For å sikre at informasjonen får et tilstrekkelig beskyttelsesnivå, anbefales det i punkt 8.2 at informasjon klassifiseres i henhold til juridiske krav, verdi, kritikalitet og sensitivitet.

Revisjonen viser at Arbeidstilsynet, i dokumentet *Behandling av personopplysninger i ATIL – juni 2017,* har en oversikt over hvilke personopplysninger tilsynet behandler. Dokumentet inneholder informasjon om hvilke systemer som behandler personopplysninger, lovgrunnlag, hvilke opplysninger som behandles, og om disse er sensitive eller ikke.

Arbeidstilsynet har utarbeidet *Retningslinjer for klassifisering av informasjonssystemer*[22], hvor formålet med dokumentet er å gi retningslinjer for klassifisering og risikoanalyse av informasjonssystemer. Retningslinjene beskriver blant annet når klassifisering og risikoanalyser skal gjennomføres, og når det skal vurderes om det er behov for reklassifisering. Videre beskrives sikkerhetsklassene (A-D), hvordan klassifiseringen skal gjennomføres og hvem som er ansvarlig.

[21] Datatilsynet (2011) *Veileder i sikkerhetsarkitektur*. <https://www.datatilsynet.no/globalassets/global/regelverk-skjema/veiledere/sikkerhetsarkitektur_veil.pdf>, s. 20.
[22] *Retningslinjer for klassifisering av informasjonssystemer, versjon 1.4 datert 18.3.2014.*

I tillegg til retningslinjene har Arbeidstilsynet utarbeidet dokumentet *Hjelpespørsmål for Arbeidstilsynets Systemklassifisering – versjon 1.0*. Prosesseier skal besvare hjelpespørsmål under områdene økonomi, omdømme, avhengighet, rammekrav og forventninger og sikkerhetsprofil og vurdere i hvilken grad systemet påvirkes, ut fra en skala fra 1 til 5. Arbeidstilsynet har ikke definert kriterier for bruk av skalaen. Vurderingene er grunnlaget for klassifisering av systemet. Sikkerhetsleder legger til rette for prosessen for å sikre en enhetlig klassifisering og sammenlignbare resultater.

Arbeidstilsynet har definert ulike tiltak som skal implementeres, avhengig av hvilken sikkerhetsklasse systemet blir klassifisert i (se for øvrig rapportens punkt 6.1.1. om grunnlag for sikkerhetstiltak).

Dokumentet *Klassifiserte informasjonssystemer i ATIL – juni 2017* gir en oversikt over klassifiserte systemer i Arbeidstilsynet. Av dokumentet framgår sikkerhetsklasse (A–D), tidspunkt for klassifisering og prosesseier/behandlingsansvarlig for alle klassifiserte systemer. Dette skal gi Arbeidstilsynet grunnlag for å gjennomføre risikoanalyser og etablere sikkerhetstiltak.

Revisjonen viser at Arbeidstilsynet har dokumentert klassifiseringer for systemene Betzy varsel, Betzy tilsyn og ePhorte.

6.1.3. Risikostyring

Ifølge eForvaltningsforskriften § 15 tredje ledd skal omfang og innretning på internkontrollen være tilpasset risiko.

ISO 27001 punkt 5.1 om *Lederskap og forpliktelse* anbefaler i punkt b at ledelsen skal sikre at kravene i ledelsessystemet for informasjonssikkerhet integreres i organisasjonens prosesser. Revisjonen legger til grunn at risikostyring på informasjonssikkerhetsområdet skal inngå i Arbeidstilsynets ordinære prosess for virksomhetsstyring, og at risikoanalyser skal gjennomføres på et nivå som viser risiko for informasjonssikkerhet i Arbeidstilsynet som helhet.

ISO 27001 punkt 6.1.2 og 6.1.3 anbefaler at det defineres og etableres en dokumentert prosess for risikovurdering og risikohåndtering av informasjonssikkerheten. Prosessen bør inneholde kriterier for akseptabel risiko samt identifisering, analyse og evaluering av risikoer. Resultatet av risikoanalysen bør sammenlignes med valgte kriterier. Videre anbefales det at risikoene prioriteres og at virksomheten utarbeider en plan for håndtering av informasjonssikkerhetsrisikoene.

ISO 27001 punkt 8.2 anbefaler at en virksomhet gjennomfører risikovurderinger av informasjonssikkerhet ved planlagte intervaller eller ved større endringer. I henhold til 8.3 anbefales det at risikoen på informasjonssikkerhetsområdet håndteres i tråd med en fastsatt plan.

I informasjonssikkerhetsstrategien stiller Arbeidstilsynet krav om at risikoprosessene skal bidra til å underbygge ledelsens strategiske beslutninger og prioriteringer.

Arbeidet med risiko på informasjonssikkerhetsområdet har ikke vært en del av den ordinære virksomhetsstyringen ved Arbeidstilsynet. Helhetlig risiko på området har ikke vært vurdert siden 2014.

Arbeidstilsynet har definert prinsipper for arbeidet med risikoanalyser i dokumentet *Retningslinjer for klassifisering av informasjonssystemer*. Videre har Arbeidstilsynet utarbeidet dokumentet *Veiledning for risikoanalyse av informasjonssystemer*[23], som beskriver hva en risikoanalyse er, og rammeverket/metodikken som Arbeidstilsynet har besluttet å benytte på området. Av dokumentet går det fram at det skal gjennomføres risikoanalyser på systemnivå i etterkant av klassifisering/reklassifisering, og vurdere behov for å oppdatere risikoanalysen ved innføring av nye systemversjoner.

Arbeidstilsynet har i dokumentet *Veiledning for Risikoanalyse av informasjonssystemer*[24] utarbeidet en risikomatrise hvor konsekvens og sannsynlighet vurderes med tall fra 1 til 4, hvor produktet angir verdien for

[23] *Veiledning for risikoanalyse av informasjonssystemer*, versjon 1.0, datert 14.9.2012.
[24] *Veiledning for Risikoanalyse av informasjonssystemer*, versjon 1.0 datert 14.9.2012.

risikofaktoren. Direktoratet har bestemt at hendelser med risikofaktor 9 eller høyere krever at det iverksettes tiltak. Hendelser med risikofaktor fra 3 til 8 skal vurderes for tiltak.[25]

Risikoanalysen for ePhorte[26] viser at risikoer er identifisert og analysert. Det er iverksatt tiltak, og ny risikovurdering er utarbeidet etter at disse er gjennomført. Behovet for ytterligere tiltak er også vurdert.

Risikoanalysene for Betzy varsel[27] og Betzy tilsyn[28] er ikke ferdigstilt og mangler blant annet tiltak for flere identifiserte risikoer. Status for tiltak som er identifisert, går ikke fram av risikoanalysene, og risiko er ikke evaluert for tiltakene som er iverksatt.

Revisjonen viser at det ikke er utarbeidet en systemsikkerhetsplan for alle systemer hos tilsynet, og. Betzy varsel, Betzy tilsyn og ePhorte er blant systemene som ikke har fått utarbeidet en slik plan. Se rapportens punkt 6.1.1.

Se for øvrig punktet om grunnlag for sikkerhetstiltak i rapportens punkt 6.1.1, og punkt 6.2 om gjennomføring av sikkerhetstiltak.

6.2. Problemstilling 2 – gjennomføring av sikkerhetstiltak

For sikkerhetstiltakene som er omfattet av revisjonen, er funnene gruppert i følgende faser i sikkerhetsarbeidet: (1) dokumentere vedtatte sikkerhetstiltak (fastsette krav), (2) implementere tiltak og (3) etterkontrollere/evaluere tiltak.

Revisjonen omfatter utvalgte sikkerhetstiltak for Betzy varsel, Betzy tilsyn og ePhorte, med underliggende infrastruktur (PC, database, applikasjonsserver og nettverk). Dette inkluderer tilgangskontroller, logging, sikkerhetsoppdatering og kontroll med enheter og programvare.

6.2.1. Dokumentasjon – policy/retningslinjer/rutiner

I henhold til personopplysningsloven § 13 andre ledd skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren.

Personopplysningsforskriftens kapittel 2 om informasjonssikkerhet gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler, der det blant annet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene. Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten skal i henhold til § 2-16 dokumenteres.

ISO 27002 kapittel 5 anbefaler blant annet at informasjonssikkerhetspolicyen understøttes av temaspesifikke policyer, som videre pålegger implementering av sikringstiltak for informasjonssikkerhet, og som er strukturert for å dekke behovene til bestemte målgrupper innenfor en virksomhet eller for å ta opp bestemte temaer.

Kapittel 12 om driftssikkerhet anbefaler at driftsprosedyrene dokumenteres og gjøres tilgjengelig for brukere som har behov for dem. Videre bør prosedyrene spesifisere instruksjoner for drift for blant annet installering og konfigurering av systemer (inkludert oppdatering), logging og overvåking.

Tiltakene Arbeidstilsynet har planlagt å gjennomføre, skal følge av retningslinjer i styringssystemet, klassifisering og risikoanalyser, og framkomme i en systemsikkerhetsplan for det enkelte system. Det er ikke utarbeidet systemsikkerhetsplan for systemene Betzy og ePhorte, jf. rapportens punkt 6.1.

Ifølge *Strategi for informasjonssikkerhet i Arbeidstilsynet* skal det være definert tekniske løsninger for tilgang, både på infrastruktur- og systemnivå. Slike valg skal være bevisste og langsiktige.

Det skal være dokumenterte rutiner for tilgangsstyring, hvor det skal gå fram hvem som kan autorisere tilganger, og hvem som skal kunne åpne for tilgang. Det skal også være etablert prosedyrer for fjerning av tilganger ved

[25] *Veiledning for risikoanalyse av informasjonssystemer* (versjon 1.0.1 av 15.10.2012) s. 9.
[26] ePhorte, risikoanalyse datert 20.3.2012.
[27] Betzy varsel, risikoanalyse datert 11.11.2015.
[28] Betzy tilsyn, risikoanalyse av datert 8.4.2015.

fratreden, ved opphør og endring av arbeidsoppgaver og ved tildeling av nye oppgaver. Alle tilganger som gis, skal være sporbare og dokumenterte.

Videre skal det være utarbeidet retningslinjer som beskriver hva som skal logges, hvordan og hvor lenge loggene skal oppbevares.

Ifølge *Retningslinje for sikring av nettverk og infrastruktur* skal det utarbeides og vedlikeholdes driftsprosedyrer for alt utstyr for informasjonsbehandling og kommunikasjon i infrastrukturen. Det skal være et bærende prinsipp at ingen brukere skal ha andrerettigheter og tilganger enn det som er nødvendig for å utføre arbeidet. Det skal være hensiktsmessig logging og overvåking for å gjøre det mulig å registrere tiltak som er relevante for sikkerheten. Revisjonen viser at Arbeidstilsynet har etablert prosesser for håndtering av flere av områdene som er omfattet av revisjonen. Tilsynet har i begrenset grad dokumentert eller stilt krav til hvordan tiltakene og prosessene skal gjennomføres. Rutiner og driftsprosedyrer synes ikke å være dokumentert på en systematisk og helhetlig måte. Videre finnes det ingen dokumentasjon som beskriver når og hvordan etterkontroll og evaluering av de enkelt sikkerhetstiltakene skal gjennomføres.

For områdene som er omfattet av revisjonen, er det utarbeidet enkelte beskrivelser av krav til og gjennomføring av følgende sikkerhetstiltak:

- tilgangsstyring i Betzy og ePhorte
- logging og oppfølging av logger i Betzy og ePhorte
- lokale administratorer og programvare på PC-er

Det er imidlertid ikke utarbeidet dokumenterte rutiner eller driftsprosedyrer slik det er beskrevet i strategien og retningslinje for sikring av nettverk og infrastruktur, og det mangler dokumentasjon for krav og gjennomføring av viktige sikkerhetstiltak. Dette gjelder:

- tilgangsstyring
    - administratorer på PC-er, databaser og nettverk
    - passord
- logging og oppfølging av logger for å identifisere sikkerhetshendelser
- oppdatering av operativsystem og programvare
- styring av programvare på PC-er og servere
- styring av enheter i nettverket

6.2.2. Implementering av sikkerhetstiltak

I henhold til personopplysningsloven § 13 første ledd, skal den behandlingsansvarlige og databehandleren gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Personopplysningsforskriften inneholder krav om sikkerhetstiltak i kapittel 2.

ISO 27001 punkt 8.1 om driftsplanlegging og kontroll anbefaler at virksomheten planlegger, implementerer og styrer prosesser som er nødvendig for å oppfylle informasjonssikkerhetskravene, og for å implementere tiltakene som er bestemt blant annet i forbindelse med risikohåndtering.

Tilgangskontroller
Personopplysningsforskriften § 2-8 første ledd stiller krav om at medarbeidere hos den behandlingsansvarlige bare skal bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk.

ISO 27002 punkt 9.2 anbefaler at virksomheten har etablert en formell prosess for registrering, endring og sletting av tilganger ved fratredelse eller endring i arbeidsforhold.

<u>Saksbehandlerrettigheter</u>
Arbeidstilsynet har etablert en formell prosess for registrering, endring og sletting av tilganger og rettigheter i Betzy og ePhorte. De bruker et felles elektronisk skjema for innmelding og endring av rettigheter. Arbeidstilsynet har utarbeidet oversikt over hvem som er godkjent som bestillere. IKT-servicedesk og Dokumentsenteret registrerer rettighetene i systemene på bakgrunn av mottatt bestilling. Det finnes dokumentasjon av prosessen i servicedesksystemet.

Det er i hovedsak regionene som har ansvar for å holde brukermassen oppdatert. Gjennomgang av ansatte som har sluttet, viser at kontiene er deaktivert i systemene. Det kan imidlertid ta noe tid fra en ansatt slutter, til brukerkontoen er deaktivert i ePhorte.

Administratorrettigheter
ISO 27002 punkt 9.1.1 anbefaler at tilgang til informasjon og systemer begrenses i henhold til tjenstlig behov, det vil si at medarbeidere ikke bør gis tilgang til mer enn det som er nødvendig for å utføre oppgavene sine. Videre er det anbefalt å vedlikeholde en autorisasjonsprosess og fortegnelse over alle tildelte rettigheter. Privilegerte tilgangsrettigheter bør tildeles en annen brukerkonto enn den som brukes til vanlige aktiviteter i virksomheten.

Revisjonen har omfattet administratorrettigheter på PC-er, database, server og nettverk. Arbeidstilsynet etterlever anbefalinger om å begrense og kontrollere administratorbrukere på PC-er, men ikke på servere, database og i nettverk:

- Nasjonal sikkerhetsmyndighet (NSM) anbefaler at sluttbrukere ikke tildeles utvidede rettigheter (lokal administrator), og framhever dette som et av de fire viktigste tiltakene mot dataangrep.[29] I Arbeidstilsynet skal sluttbrukere som hovedregel ikke være lokal administrator på PC-en. Analyse av uttrekk fra 60 PC-er viser at Arbeidstilsynet etterlever egne regler.

- Analyse av uttrekk av alle brukere i databasen for Betzy og ePhorte viser at det er brukere med tilgang som ikke skal ha det, og at det finnes vanlige brukerkonti med administratorrettigheter. Det er videre aktivert funksjoner i databasene som ikke er i henhold til beste praksis.

- Analyse av uttrekk viser at det er gitt administratorrettigheter på applikasjonsservere utover det som er nødvendig, og tildeling av rettigheter synes ikke å være systematisk.

- Arbeidstilsynet opplyser at administratorer skal ha færrest mulig rettigheter, men nok til å gjøre jobben sin. Analyse av uttrekk fra Active Directory (AD) viser at flere brukere, inklusiv systembrukere, er medlem i administratorgrupper i AD uten å ha behov for disse rettighetene.

Passord
Passord i AD styrer autentisering og passordkvalitet for brukere ved pålogging i Betzy, ePhorte, servere, nettverk og til dels databaser.

ISO 27002 punkt 9.4.3 anbefaler at virksomheten har et system som sikrer passordkvalitet og jevnlig bytte av passord. Brukere bør ha individuelle konti med eget passord for å ivareta ansvarlighet.

Microsoft anbefaler at det settes strenge krav til autentisering ved bruk av konti med privilegerte rettigheter, i utgangspunktet flerfaktorautentisering.[30]

Arbeidstilsynet skal i henhold til interne retningslinjer kreve passord med «streng policy» eller tofaktorautentisering for administratorer. Det er ikke definert hvilke krav som inngår i «streng policy».

Arbeidstilsynet opplyser at det er implementert tofaktorautentisering ved pålogging til Betzy samt ved pålogging på brannmur og proxy-server. For øvrig er det stilt like krav til administratorer og vanlige brukerkonti i nettverket. Passordkravene er satt opp slik at passord aldri utløper, og analyse av uttrekk fra AD viser at mange brukerkonti, både vanlige og administratorkonti, ikke hadde byttet passord på lang tid.

Arbeidstilsynet har i etterkant av revisjonen endret passordoppsettet i nettverket slik at alle brukere blir tvunget til passordskifte.

Logging
Personopplysningsforskriften § 2-8 tredje ledd stiller krav om at autorisert bruk av informasjonssystemet skal registreres. Videre stilles det krav i § 2-14 om at sikkerhetstiltak skal gjøre det mulig å oppdage forsøk på uautorisert bruk av systemer med personopplysninger.

[29] Nasjonal sikkerhetsmyndighet: *Fire effektive tiltak mot dataangrep* (Sjekkliste nr. 1).
[30] Microsoft: *Best Practices for Securing Active Directory* <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

ISO 27002 punkt 12.4.1 anbefaler at det produseres hendelseslogger som registrerer brukeraktiviteter (herunder påloggingsinformasjon og bruk av privilegier), avvik, feil og informasjonssikkerhetshendelser. Videre er det anbefalt at logger oppbevares og gjennomgås regelmessig, samt å beskytte logginformasjon mot misbruk og uautorisert tilgang.

Revisjonen viser at Arbeidstilsynet i varierende grad har aktivert logger. En del av loggene overføres til loggservere, men tilsynet følger dem i hovedsak opp i forbindelse med drift av systemene, og ikke sikkerhet. Arbeidstilsynet i ferd med å gjøre endringer i oppfølgingen av logger og skal innføre automatiske varsler for hendelser. Revisjonen viser at:

- Arbeidstilsynet har etablert logger slik personopplysningsforskriften krever for Betzy og i hovedsak for ePhorte. Gjennomgang av logger er ikke systematisert og gjennomføres ikke regelmessig for å oppdage eventuelle sikkerhetsbrudd, herunder uautorisert bruk av systemet.

- For underliggende infrastruktur er det enkelte mangler i loggoppsett. Foreløpig brukes ikke loggene til å identifisere sikkerhetshendelser, men Arbeidstilsynet er i ferd med å anskaffe et nytt verktøy som skal gi varsler ved unormal aktivitet i nettverket.

Oppdatering
NSM anbefaler at sikkerhetsoppdateringer for installert programvare tas i bruk så fort som mulig.[31] NSM framhever dette tiltaket som ett av de fire viktigste tiltakene mot dataangrep.[32] Center for Internet Security anbefaler at virksomheter tar i bruk verktøy som automatisk oppdaterer operativsystem og annen programvare, for alle systemer.[33] Sikkerhetsoppdateringer beskytter virksomheten mot sårbarheter som kontinuerlig oppdages i programvare.

Arbeidstilsynet har et system for håndtering av oppdateringer for operativsystem og tredjeparts programvare. Nye oppdateringer hentes ned, testes og rulles ut månedlig. Analyse av uttrekk fra PC-er, databaser og servere viser at PC-ene og servere synes å følge et jevnt oppdateringsløp, og at de er tilstrekkelig oppdatert. For databasene er én av to tilstrekkelig oppdatert. Utstyr som ikke er oppdatert med de siste sikkerhetsoppdateringene, er sårbare for kompromittering.

Programvare og enheter
ISO 27002 punkt 12.6.2 anbefaler å etablere og håndheve strenge regler for hvilken programvare sluttbrukere kan installere. NSM anbefaler at kun eksplisitt autorisert programvare kjøres på virksomhetens enheter, og at det kun installeres programvare med nødvendig funksjonalitet for å understøtte virksomhetens forretningsprosesser.[34] NSMs anbefalinger samsvarer med standard fra Center for Internet Security.[35] Bakgrunnen for anbefalingene er at dataangrep ofte innebærer installasjon av ondsinnet programvare og/eller utnyttelse av svakheter i ordinær programvare.

Revisjonen viser at Arbeidstilsynet har iverksatt tiltak for å begrense programvare og hindre kjøring av uautorisert programvare på PC-er.

Analyse av uttrekk fra applikasjonsserver for Betzy og ePhorte viser at det kun er nødvendig programvare som er installert.

ISO 27002 punkt 13.1.1 anbefaler at det implementeres prosedyrer for kontroll av nettverksutstyr og tiltak for å beskytte mot uautorisert tilgang.

CIS *Critical Security Controls 1 – Inventory of Authorized and Unauthorized Devices* anbefaler å etablere en oversikt over autorisert utstyr, at kun autorisert utstyr får tilgang til virksomhetens nettverk, og at uautorisert utstyr blir oppdaget og hindret tilgang.

Revisjonen viser at Arbeidstilsynet har etablert tiltak for å begrense muligheten for å koble til uautorisert utstyr i nettverk, både i trådløst og kablet nett. For besøkende og andre eksterne som bringer egen enhet, er det satt opp trådløst gjestenett som kun gir tilgang til internett.

[31] NSMs grunnprinsipper for IKT-sikkerhet, versjon 1.0, punkt 3.2.
[32] Nasjonal sikkerhetsmyndighet: *Fire effektive tiltak mot dataangrep* (Sjekkliste nr. 1).
[33] The Center for Internet Security (CIS): *Critical Security Controls (CSC) for effective cyber defense*, punkt 4.
[34] NSMs grunnprinsipper for IKT-sikkerhet, versjon 1.0, punkt 2.3.
[35] The Center for Internet Security (CIS): *Critical Security Controls (CSC) for effective cyber defense*, punkt 2.

6.2.3. Etterkontroll/evaluering av sikkerhetstiltak

Personopplysningsforskriften § 2-5 stiller krav til at det gjennomføres jevnlige sikkerhetsrevisjoner av sikkerhetstiltak. Bestemmelsen pålegger den behandlingsansvarlige jevnlig, eksempelvis årlig, å etterprøve sikkerhetsarbeidet for å verifisere at sikkerhetstiltakene som er vedtatt, faktisk er iverksatt og fungerer etter hensikten. Resultater fra slike sikkerhetsrevisjoner vil være grunnlaget for ledelsens gjennomgang av sikkerhetsmål og strategier og et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerheten.[36]

ISO 27002 punkt 18.2 anbefaler at ledere jevnlig gjennomgår at informasjonsbehandling og prosedyrer er i samsvar med gjeldende sikkerhetspolicyer, standarder og andre sikringskrav, innenfor sitt ansvarsområde. Videre er det anbefalt å regelmessig gjennomgå informasjonssystemene for å sikre at de er i samsvar med organisasjonens policyer og standarder for informasjonssikkerhet.

For Arbeidstilsynets infrastruktur er det i liten grad beskrevet hvilke tiltak som skal implementeres, og hvordan. Det er heller ikke stilt krav om evaluering eller etterkontroll av implementerte tiltak, jf. også rapportens punkt 6.2.1. og 6.3. Sikringstiltak synes ikke å bli fulgt opp jevnlig og på en systematisk måte, og manglende etterlevelse omtalt i 6.2.2 er avvik som ville ha vært fanget opp av etterkontroller.

Revisjonen har omfattet etterkontroll av tilgangsstyring, logging, oppdatering samt programvare og enheter og viser at Arbeidstilsynet gjennomfører etterkontroller på enkelte områder. Det er imidlertid viktige områder det ikke er gjennomført etterkontroller eller evalueringer av. Dette omfatter følgende:

- Det er etablert etterkontroll av brukere og tildelte rettigheter i Betzy og ePhorte, men ikke for administratorrettigheter i databaser, servere og nettverk.

- En etterkontroll/evaluering av arbeidet med logger vil for eksempel innebære en kontroll av om det er iverksatt tilstrekkelig logging ut fra virksomhetens krav til aktuelt informasjonssystem, og om loggene er fulgt opp i henhold til interne regler. En etterkontroll er først aktuell når det er stilt krav om logging og loggene brukes aktivt i virksomheten.

  Arbeidstilsynet har ikke etablert etterkontroll av logging og oppfølging av logger hverken i applikasjon eller i underliggende infrastruktur.

- Arbeidstilsynet bruker systemet for administrasjon av oppdatering til å følge opp om oppdateringer er vellykket. Tilsynet er i ferd med å utvikle et nytt uttrekk av informasjon fra systemet siden kontrollen ikke anses å være god nok.

- Vanlige brukere er ikke lokal administrator på egen PC, og Arbeidstilsynet har på denne måten begrenset brukernes mulighet til å installere programvare. I tillegg følger Arbeidstilsynet med på hvilke programvare som er installert ved å benytte et system som henter inn informasjon om installert programvare fra alle PC-ene.. Systemet inneholder også en liste over uønsket programvare.

- Arbeidstilsynet skanner nettverket hver dag for å kontrollere om det er ukjente enheter i nettverket.

6.3. Problemstilling 3 – oppfølging og evaluering av styringssystemet

6.3.1. Hendelseshåndtering

Ifølge eForvaltningsforskriften § 15 fjerde ledd bokstav g) skal sikkerhetsstrategien og internkontrollen også stille nødvendig krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon etter personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.

Etter personopplysningsforskriften § 2-6 skal bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, behandles som avvik. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse.

36 Datatilsynet (2000) *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer*.

ISO 27002 punkt 16.1 anbefaler å etablere prosesser for å sikre rapportering, behandling, reaksjon på og læring av informasjonssikkerhetshendelser. ISO 27002 punkt 16.1.6 anbefaler at erfaringer fra informasjonssikkerhetshendelser bør brukes for å redusere sannsynlighet for, eller konsekvens av, framtidige hendelser.

Informasjonssikkerhetsstrategien stiller krav om at det skal foreligge et dokumentert avvikssystem for informasjonssikkerhet.

Revisjonen viser at Arbeidstilsynet ikke har etablert en prosess for håndtering av informasjonssikkerhetshendelser. Det er ikke definert hva som er en informasjonssikkerhetshendelse. Videre er det ikke utarbeidet rutiner eller prosedyrer som beskriver hvordan hendelseshåndteringen for informasjonssikkerhetshendelser skal sikre at avvik blir oppdaget og korrigert, og at gjentakelse hindres.

Arbeidstilsynet opplyser at IKT-hendelser skal meldes via servicedesken. Det er imidlertid opplyst at det ikke er utarbeidet rutiner for å håndtere informasjonssikkerhetshendelser som blir meldt inn til eller oppdaget av IKT-seksjonen.

Arbeidstilsynet bruker QualityManager+ for å håndtere HMS-hendelser. I dette systemet er det også opprettet en egen kategori for informasjonssikkerhetshendelser. Analyse av hendelser i QM+ fra 1. januar 2016 til 31. mai 2017 viser at det ikke er registrert informasjonssikkerhetshendelser i perioden.

6.3.2. Interne sikkerhetsrevisjoner

Etter eForvaltningsforskriften § 15 andre ledd skal forvaltningsorganet ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet, som er basert på anerkjente standarder for styringssystem for informasjonssikkerhet.

ISO 27001 punkt 9.2 anbefaler at det gjennomføres interne revisjoner med planlagte intervaller for å gi informasjon om styringssystemet er i samsvar med interne krav, og at dette implementeres og vedlikeholdes på en hensiktsmessig måte.

Revisjonen viser at Arbeidstilsynet ikke har stilt konkrete krav om evaluering av sikkerhetstiltak og sikkerhetsrevisjoner i sine styrende dokumenter for informasjonssikkerhet.

Arbeidstilsynet har imidlertid utarbeidet *Sjekkliste for informasjonssikkerhet*. Sjekklisten er et hjelpemiddel som skal bidra til å sikre at viktige krav til informasjonssikkerhet blir etterlevd i systemene. Mal for sjekklisten er utarbeidet i august 2016, og tilsynet har opplyst at prosessen med å benytte skjemaet for revisjon / «self assessment» har startet.

Arbeidstilsynet opplyser at det tidligere er gjennomført en penetrasjonstest, hvor det ikke ble oppdaget vesentlige svakheter. Videre at det pågår en gjennomgang av fysisk sikkerhet ved regionskontorene.

Revisjonen viser imidlertid at Arbeidstilsynet ikke har kontrollert og evaluert om organiseringen av informasjonssikkerhetsarbeidet og de etablerte sikkerhetstiltakene fungerer som forutsatt.

Se for øvrig rapportens punkt 6.1.3. om risikostyring og punkt 6.2.3 om etterkontroll/evaluering av sikkerhetstiltak.

6.3.3. Ledelsens gjennomgang og kontinuerlig forbedring

Etter eForvaltningsforskriften § 15 andre ledd skal forvaltningsorganet ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som er basert på anerkjente standarder for styringssystem for informasjonssikkerhet.

ISO 27001 punkt 9.1 anbefaler at virksomheten evaluerer prestasjonen til og virkningen av styringssystemet for informasjonssikkerhet. I henhold til punkt 9.3 er det anbefalt at ledelsen gjennomgår styringssystemet for informasjonssikkerhet jevnlig for å sikre at det er velegnet, tilstrekkelig og virkningsfullt. Videre anbefales det i kapittel 10 at virksomheten reagerer på eventuelle avvik og innfører korrigerende tiltak. Virksomheten bør kontinuerlig forbedre egnetheten, tjenligheten og virkningen til styringssystemet for informasjonssikkerhet.

Revisjonen viser at Arbeidstilsynet ikke har gitt føringer for ledelsens gjennomgang eller kontinuerlig forbedring av styringssystemet for informasjonssikkerhet.[37]

Arbeidstilsynet opplyser at det i 2014 ble det laget en enhetlig rapport over ikke-akseptable risikoer i hvert av systemene ved Arbeidstilsynet som ledelsen gjennomgikk. Etter dette har ikke ledelsen gjennomgang vært gjennomført.

Arbeidstilsynet opplyser at direktøren har initiert en gjennomgang av hele sikkerhetsorganisasjonen. Gjennomgangen inkluderer informasjonssikkerhet, fysisk sikkerhet, personellsikkerhet samt helse-, miljø- og sikkerhet knyttet til arbeidsmiljø Det er videre opplyst at det har vært for lite samlet oppmerksomhet på disse tre områdene. I forbindelse med gjennomgangen er det startet et arbeid med ny overordnet sikkerhetspolicy, som består av dagens informasjonssikkerhetspolicy og strategidokument, og som skal knytte informasjonssikkerhet, personellsikkerhet og fysisk sikkerhet tettere sammen. Den nye personopplysningsloven som trer i kraft i 2018, vil også ha betydning for styringssystemet. Ny sikkerhetspolicy er vedtatt og etatens nye overordnede styringssystem planlegges ferdigstilt innen oktober 2018.

Se for øvrig rapportens punkt 6.1.1.

7 Konklusjoner

Arbeidstilsynet skal bidra til et åpent, trygt og fleksibelt arbeidsliv. En av Arbeidstilsynets hovedoppgaver er å føre tilsyn med at virksomheter følger kravene i arbeidsmiljøloven. I gjennomføringen av oppgavene forvalter Arbeidstilsynet sensitive personopplysninger om arbeidstakere, blant annet knyttet til personskade og sykdom som oppstår i arbeidssammenheng. Behandlingen av sensitive personopplysninger skjer gjennom etatens fagsystem Betzy varsel og arkivsystemet ePhorte. I Betzy tilsyn dokumenteres tilsynets ordinære tilsynsvirksomhet.

Målet med revisjonen har vært å kontrollere om Arbeidstilsynet har et styringssystem for informasjonssikkerhet i henhold til kravene i eForvaltningsforskriften og som ivaretar krav i personopplysningsloven.

Et styringssystem for informasjonssikkerhet skal hjelpe ledelsen og virksomheten for øvrig til å ha tilstrekkelig styring og kontroll med informasjonssikkerheten, gjennom systematisk internkontroll på området. Det skal bidra til at virksomheten velger riktige sikkerhetstiltak, og sørge for at de valgte løsningene blir evaluert og om nødvendig forbedret.

Arbeidstilsynet har innført et styringssystem for informasjonssikkerhet som delvis dekker kravene i eForvaltningsforskriften § 15 og personopplysningsloven. Det er utarbeidet mål og prinsipper som definerer prosessene for arbeidet med informasjonssikkerhet og planlegging av sikkerhetstiltak. Dette inkluderer føringer for klassifisering av informasjonssystemer, risikoanalyser og avvikshåndtering. Det er imidlertid ikke stilt krav om interne revisjoner eller gjennomganger av om sikkerhetsstrategien og sikkerhetstiltakene fungerer etter hensikten. Videre er det ikke stilt krav om evaluering og kontinuerlig forbedring av styringssystemet.

Informasjonssystemene er blitt klassifisert. Risikoarbeidet på informasjonssikkerhetsområdet har imidlertid ikke vært en del av den ordinære virksomhetsstyringen ved Arbeidstilsynet, og den helhetlige risikoen på området er ikke blitt vurdert siden 2014. Videre er ikke risikovurderingene på systemnivå fullstendige for alle systemene som er omfattet av revisjonen. Tiltak for å håndtere risiko går ikke alltid fram av risikoanalysene, og det er ikke dokumentert om identifiserte tiltak er gjennomført eller evaluert. Tilsynet har ikke utarbeidet en samlet oversikt over sikkerhetstiltak for hvert system, slik det er gitt føringer om i styringssystemet.

Arbeidstilsynet har ikke utarbeidet retningslinjer eller rutiner for viktige sikkerhetstiltak som tilgangsstyring, logging, oppdateringer og kontroll med programvare og enheter. Dette kan være årsaken til at flere av tiltakene som er omfattet av revisjonen, ikke er implementert i henhold til beste praksis og anbefalinger i anerkjente standarder.

Det foreligger ikke et helhetlig system for registrering, håndtering og oppfølging av informasjonssikkerhetshendelser.

[37] Se rapportens punkt 6.1.1.

Arbeidstilsynet har ikke kontrollert og evaluert om arbeidet med informasjonssikkerhet og sikkerhetstiltak fungerer som forutsatt, og ledelsens gjennomgang er ikke gjennomført de seneste årene.

Det er igangsatt en gjennomgang av sikkerhetsarbeidet hos Arbeidstilsynet. Gjennomgangen inkluderer styringssystemet for informasjonssikkerhet, fysisk sikkerhet og personellsikkerhet. Den nye personopplysningsloven som trer i kraft i 2018, vil ha betydning for dette arbeidet.