Riksrevisjonen

# Revisjonsrapport for 2017 om styringssystem for informasjonssikkerhet i Statens kartverk


**Mottaker: Kommunal- og moderniseringsdepartementet**

**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.**

Forsideillustrasjon: Riksrevisjonen

# Innhold

# 1 Sammendrag

Målet med revisjonen har vært å kontrollere om Statens kartverk 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 informasjon som virksomhetene behandler, 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.

Statens kartverk samler inn, systematiserer, forvalter og videreformidler offentlig geografisk informasjon som er av vital betydning for hele det norske samfunnet. Dette gjelder blant annet eiendomsinformasjon i nasjonalt register for offentlig eiendomsinformasjon, tinglysing for fast eiendom og andeler i borettslag samt kartdata for både land og sjø. En del av informasjonen Kartverket behandler er nasjonale felleskomponenter (gjenbrukbare løsninger som dekker typiske behov på digitaliseringsfeltet, slik som innlogging, autentisering, registre, osv.). Flere fagsystemer behandler personopplysninger, blant annet systemene som benyttes i tinglysing og eiendomsforvaltning (grunnboken og matrikkelen). Kartverket er avhengig av god informasjonssikkerhet for å levere tjenester som samfunnet kan være sikre på er korrekte og bevarer integriteten.

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 for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem». Forskriftens § 15 stiller videre krav til at intern kontroll skal inkludere relevante krav som er fastsatt i og i medhold av 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 at dette er beste praksis for styring og gjennomføring av sikkerhetstiltak.

Revisjonen omfatter Kartverkets 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 Kartverket evaluerer og oppdaterer styringssystemet med bakgrunn i observerte sikkerhetshendelser og sikkerhetsrevisjoner.

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

Revisjonen viser at Kartverket har innført et styringssystem for informasjonssikkerhet som i stor grad dekker kravene i eForvaltningsforskriften § 15 og personopplysningsloven.

- Kartverket har et styringssystem for informasjonssikkerhet som definerer prosessene for arbeidet med informasjonssikkerhet, planlegging av sikkerhetstiltak, og hvordan arbeidet med informasjonssikkerhet skal evalueres og forbedres.
- Kartverket har i liten grad utarbeidet policy, retningslinjer eller rutiner for sikkerhetstiltak, og har i varierende grad gjennomført og fulgt opp tiltak i henhold til beste praksis.
- Kartverket har innført systemer for registrering, håndtering og oppfølging av avvik og informasjonssikkerhetshendelser.
- Kartverket har ikke en helhetlig oppfølging av om styringssystemet fungerer etter hensikten.

Utkast til rapport ble forelagt Kommunal- og moderniseringsdepartementet i brev av 6. april 2018. Departementet har i brev av 27. april 2018 gitt kommentarer til rapportutkastet.

Departementet framhever i svaret at det mener at Kartverket har etablert gode systemer og rutiner for IKT-sikkerhet, men at rapporten peker på klare forbedringstiltak når det gjelder dokumentasjon av etterlevelse og etterkontroll. Dette vil departementet følge nøye opp gjennom etatsstyringen. Av svarbrevet går det også fram at Kartverket erkjenner at de har en jobb å gjøre med å forbedre dokumentasjon av etterlevelse og etterkontroll.

# 2 Innledning

Statens Kartverk (Kartverket) er underlagt Kommunal- og moderniseringsdepartementet. Kartverket forvalter nasjonale felleskomponenter[1] og samler inn, systematiserer, forvalter og videreformidler offentlig geografisk informasjon. Kartverket er tinglysingsmyndighet for hele landet. Konkret innebærer det blant annet at Kartverket har ansvar for og leverer følgende:

- Nasjonalt geodetisk grunnlag: Kartverket har ansvar for bekreftelsesgrunnlaget som kart- og oppmålingsarbeidene i Norge bygger på.
- Posisjonstjenester: Tjenester som fastsetter nøyaktig, satellittbasert posisjon.
- Digitale kart: Kartverket produserer og forvalter nasjonale digitale kartserier (land- og sjøkart).
- Tinglysing: Tinglysing i fast eiendom og andeler i borettslag (grunnboken).
- Eiendomsinformasjon: Kartverket drifter de nasjonale registrene for offentlig eiendomsinformasjon (matrikkelen).
- Stedsnavn: Kartverket forvalter det nasjonale stedsnavnregisteret.
- Standarder: Nasjonale standarder for kart og geografisk informasjon.
- Elektronisk sjøkarttjeneste: Kartverket drifter den internasjonale elektroniske sjøkarttjenesten Primar.

Kartverket er organisert i fire divisjoner, geodesi-, land-, sjø- og eiendomsdivisjonen. Hovedkontoret ligger i Hønefoss. I tillegg er det blant annet ti fylkeskartkontor rundt om i landet, et kundesenter som er lokalisert i Ullensvang og et observatorium på Svalbard.

Flere av fagsystemene i Kartverket behandler informasjon som har vesentlig samfunnsmessig betydning. En del av fagsystemene behandler også personopplysninger, blant annet systemene som benyttes i tinglysing og eiendomsforvaltning (grunnboken og matrikkelen). Det er viktig at offentlige virksomheter beskytter informasjon som forvaltes 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[2] øker i takt med digitaliseringen av offentlig forvaltning. Kartverket har satt ut noe av driften av IKT-infrastruktur og systemer til Electronic Chart Centre AS, men drifter selv store deler av egen IKT-infrastruktur og systemer. Nasjonal sikkerhetsmyndighet (NSM) gjennomførte i 2015 tilsyn i Kartverket og avdekket manglende sikkerhetstiltak og en sårbar IKT-infrastruktur. De svakheter som ble påpekt i tilsynsrapporten er utbedret i løpet av vinteren 2018.[3]

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 medvirke 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 tiltakene settes i verk. Svakheter i sikkerhetstiltak kan indikere at styringssystemet ikke fungerer på alle områder, enten ved at svakhetene ikke er identifisert eller at det ikke er satt i verk korrigerende tiltak. Manglende sikkerhetstiltak kan føre til uheldige konsekvenser for enkeltpersoner, samfunnet og/eller skade omdømmet til offentlige virksomheter.

# 3 Revisjonens mål og problemstillinger

Målet med revisjonen er å kontrollere om Kartverket har et styringssystem for informasjonssikkerhet som er i samsvar med eForvaltningsforskriften § 15 og som ivaretar kravene i personopplysningsloven.

[1] https://www.regjeringen.no/no/tema/statlig-forvaltning/IKT-politikk/felleskomponenter/id2342598/
[2] Nasjonal strategi for informasjonssikkerhet har definert sensitiv informasjon til å være informasjon det av ulike hensyn er viktig å beskytte.
[3] Brev fra Kommunal- og moderniseringsdepartementet av 27. april 2018

Revisjonen er gjennomført med utgangspunkt i tre problemstillinger:

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

2. Problemstillingen omfatter Kartverkets arbeid med styring av informasjonssikkerhet, herunder sikkerhetsmål og sikkerhetsstrategier, samt klassifisering og risikovurdering for sikring av informasjon.

3. Har Kartverket sikret at det gjennomføres systematiske tiltak som skal bidra til å sikre tilfredsstillende informasjonssikkerhet i virksomheten?

4. Denne problemstillingen tar for seg et utvalg sikkerhetstiltak som skal bidra til tilfredsstillende informasjonssikkerhet i grunnboken og matrikkelen.

5. Følger Kartverket opp at sikkerhetsstrategi og tiltak gir tilfredsstillende informasjonssikkerhet?

6. Problemstillingen omfatter rutiner for hendelses- og avviksbehandling, og hvordan Kartverket følger opp at styringssystemet fungerer etter hensikten.

Avgrensning:

Applikasjoner og rutiner som er underlagt sikkerhetsloven, er ikke omfattet av vår revisjon.

# 4 Metoder

Problemstillingene er besvart gjennom dokumentanalyse, møter, observasjoner og analyse av uttrekk fra Kartverkets IKT-systemer. Kontroll og analyse av sikkerhetstiltak er gjennomført med grunnboken (hjemmelsregister) og matrikkelen (eiendomsregister) som utgangspunkt.

Det er avholdt oppsummeringsmøte i Kartverket 8. mars 2018 hvor formålet var å avklare faktagrunnlaget for de enkelte problemstillingene.

## 4.1. Problemstilling 1 og 3 – planlegging og evaluering av sikkerhetstiltak

For å besvare problemstillingene er det gjennomført dokumentanalyse og møter.

### 4.1.1. Dokumentanalyse

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

Analysen omfatter:

- dokumenter av styrende karakter
    - sikkerhetspolicy informasjonssikkerhet
    - grunnlagsdokument for sikkerhet
    - årsplan for virksomhetsstyring 2017
    - årsrapport for 2017 fra divisjonene
    - Kartverkets sikkerhetstilstand 2017
    - referat fra ledelsens gjennomgang av informasjonssikkerhet september 2017
    - IT-systemoversikt
    - program for revisjon, tilsyn og beredskapsøvelser i Kartverket 2017
    - oversikt over interne og eksterne sikkerhetshendelser 2017
    - beredskapsplan - IT-avdelingen
- interne rutinebeskrivelser
    - ledelsens gjennomgåelse
    - revisjoner i Kartverket

    - rutine – ROS-analyser av sikkerhet med tilhørende mal[4]
    - håndtering av avvik og forbedringstiltak
- rapporter etter sikkerhetshendelser
- ROS-analyser

Andre dokumenter er identifisert og beskrevet under det relevante området i rapportens punkt 6.1. og 6.3.

### 4.1.2. Møter

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

Referat fra dette møtet er verifisert av Kartverket i e-post av 12. desember 2017.

## 4.2. Problemstilling 2 – gjennomføring av sikkerhetstiltak

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

Det er kontrollert et utvalg tiltak med utgangspunkt i systemene matrikkelen og grunnboken, samt underliggende infrastruktur. Sikkerhetstiltakene er valgt på bakgrunn av hva anerkjente aktører innenfor informasjonssikkerhet anser å ha størst effekt for å redusere risiko på informasjonssikkerhetsområdet.[5] Det er lagt til grunn at Kartverket gjennom styringssystemet har vurdert og håndtert risiko ved å implementere grunnleggende sikkerhetstiltak på følgende områder:

- tilgangskontroller
    - saksbehandlerrettigheter i applikasjonene
    - administratorrettigheter på klienter (PC-er), databaser, servere og i nettverk
- logging og oppfølging av logger for applikasjon og underliggende infrastruktur
- oppdatering av operativsystem og programvare på klienter, databaser og servere
- kontroll med program- og maskinvare i nettverket
    - autorisert programvare på klienter og servere
    - autorisert maskinvare i nettverket

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

Revisjonen av de utvalgte sikkerhetstiltakene vil ikke gi et fullstendig bilde av sikkerhetstilstanden i Kartverket, men resultatene gir en indikasjon på om styringssystemet fungerer som forutsatt.

Revisjonen beskriver situasjonen på tidspunktene for gjennomførte revisjonsbesøk og datauttrekk foretatt i første halvdel av januar 2018.

### 4.2.1. Dokumentanalyse

Formålet med dokumentanalysen er å undersøke om Kartverket har dokumentert krav til gjennomføring av sikkerhetstiltak på områder omfattet av revisjonen. Det er foretatt en analyse av retningslinjer, rutiner og prosedyrer på områdene klienter, databaser, servere og nettverk.

Aktuell dokumentasjon for revisjon av sikkerhetstiltakene er nærmere beskrevet i punkt 6.2 under aktuelt område.

[4] ROS-analyse = risiko- og sårbarhetsanalyse
[5] 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)

### 4.2.2. Møter

Det ble avholdt møte med nøkkelpersoner for fagsystemene matrikkelen og grunnboken om tilgangsstyring og logging for disse to fagsystemene 10. og 11. januar 2018. Videre ble det avholdt møter med nøkkelpersoner for database, servere, nettverk og klienter. Følgende temaer ble tatt opp på de respektive områder:

- database: tilgangsstyring, oppdatering og logging
- servere: tilgangsstyring, oppdatering og logging
- nettverk: tilgangsstyring, logging og kontroll med enheter
- klienter: tilgangsstyring, oppdatering og kontroll med programvare

Formålet med møtene var å sikre korrekt forståelse av hvordan sikkerhetsarbeidet er organisert og gjennomføres.

### 4.2.3. Dataanalyse og observasjoner

Formålet med dataanalyser og observasjoner er å se hvordan ulike systemer og den underliggende IKT-infrastrukturen i Kartverket benyttes, samt undersøke om aktuelle sikkerhetstiltak er gjennomført og dokumentert i henhold til krav i regelverk og anbefalinger i anerkjente standarder.

Det er gjennomført analyser av følgende datauttrekk:

- Active Directory (AD) – katalogtjenesten som Kartverket benytter for å håndtere brukere, brukerrettigheter og ressurser
- informasjon fra servere knyttet til matrikkelen og grunnboken og et utvalg PC-er pålogget i nettverket. Informasjonen omfatter
    - installert programvare
    - oppdateringer av operativsystem og programvare
    - brukere med administratorrettigheter
- tilgangsrettigheter i og oppdateringer av databasen til matrikkelen og grunnboken

I etterkant av møtet ble det oversendt oppfølgingsspørsmål som er besvart av Kartverket i notat mottatt 8. februar 2018.

Aktuelle observasjoner, analyser og datauttrekk er omtalt under aktuelt område i punkt 6.2 Sikkerhetstiltak.

# 5 Revisjonskriterier

I dette kapitlet beskrives krav til informasjonssikkerhet i relevant lovverk og anbefalinger i anerkjente standarder som skal bidra til god informasjonssikkerhet.

*Forskrift om elektronisk kommunikasjon med og i forvaltningen,* (eForvaltningsforskriften)[6] er et virkemiddel for å styrke informasjonssikkerheten. Formålet er å legge til rette for sikker bruk av elektronisk kommunikasjon og sikre hensiktsmessige tekniske løsninger.

Forskriften stiller krav om styring og kontroll med informasjonssikkerhet i statlige forvaltningsorganer. Styringssystemet skal etter § 15 fjerde ledd bokstav g), når det er relevant, også adressere prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. *Lov om behandling av personopplysninger* (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* (personopplysningsforskriften) [7] 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.»

[6] Hjemlet i *lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker* (forvaltningsloven) § 15 a m.fl.
[7] 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).[8] 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.[9]

Av lovforarbeidene til personopplysningsloven[10] 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 hvert av de aktuelle områdene i kapittel 6 *Funn*, og i vedlegget som er unntatt offentlighet.

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 ny personvernlov 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.[11]

ISO 27001 punkt 5.2 gir anbefalinger om innhold i en overordnet policy, som skal gi føringer for styring av informasjonssikkerhet og ISO 27002 punkt 5.1.1 gir mer detaljerte anbefalinger om formål, ansvarsforhold og temaspesifikke policyer som videre pålegger virksomheten å sette i verk sikkerhetstiltak.

ISO 27001 punkt 6.1.2 har detaljerte anbefalinger for gjennomføring av risikovurderinger.

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.

I personopplysningsforskriftens § 2-4 er det krav om at det skal føres oversikt over hva slags personopplysninger som behandles. Med bakgrunn i risikovurderinger må virksomheten gjøre en vurdering av hvilke tiltak som er nødvendig for å ivareta lovens krav for behandling av personopplysninger etter personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.

[8] Jf. referansekatalogen til Difi.
[9] Datatilsynet.no, *Skjema for internkontroll*. <https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/etablering-internkontroll/Internkontroll-skjema-egenkontroll/> (Hentedato 15.12.2017)
[10] Ot.prp. nr. 92 (1998–99) Kapittel 16 *Kommentarer til enkeltparagrafer*, § 13.
[11] Ot. prp. nr. 92 (1998–99). Kapittel 16 kommentarer til enkeltparagrafer, § 13.

## 5.2. Problemstilling 2 – gjennomføring av sikkerhetstiltak

eForvaltningsforskriften § 15 fjerde ledd bokstav g) sier at i den grad det er relevant, skal sikkerhetsstrategien og internkontrollen ivareta, og om nødvendig stille krav til, blant annet prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. Tilsvarende stiller personopplysningsloven § 13 blant annet følgende krav til sikkerhetstiltak ved behandling av personopplysninger:

- Den behandlingsansvarlige[12] og databehandleren[13] 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. Følgende tiltak må vurderes opp mot sannsynligheten for og konsekvensen av sikkerhetsbrudd, jf. § 2-1 andre ledd (2):

- 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 for 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 første ledd skal det treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. 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.

Videre gir ISO 27002 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 anbefalinger fra relevante aktører og leverandører.

## 5.3. Problemstilling 3 – oppfølging og evaluering av sikkerhetstiltak

eForvaltningsforskriften § 15 fjerde ledd bokstav g) stiller krav til at internkontrollen om nødvendig også skal ta for seg prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. Personopplysningsloven § 14 stiller krav om å vedlikeholde informasjonssikkerheten

> *«Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.»*

[12] Jf. personopplysningsloven § 2 nr. 4 – behandlingsansvarlige: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
[13] Jf. personopplysningsloven § 2 nr. 5 – databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige

Nærmere krav til vedlikehold av tiltak går fram av personopplysningsforskriften. I § 2-3 går det fram at den daglige ledelsen har ansvar for at bestemmelsene i forskriftens kapittel 2 følges. Videre går det fram at bruk av informasjonssystemet jevnlig skal gjennomgås for å klarlegge om det er hensiktsmessig i forhold til virksomhetens behov, og om det gir tilfredsstillende informasjonssikkerhet som resultat.

I personopplysningsforskriften § 2-5 er det krav om at det jevnlig skal gjennomføres sikkerhetsrevisjon av bruk av informasjonssystemet.

Av forskriftenes § 2-6 går videre 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 27002 detaljerte anbefalinger for vedlikehold av informasjonssikkerheten.

# 6 Funn

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

Det er i tillegg utarbeidet et vedlegg som gir en mer detaljert framstilling av revisjonsfunn i rapportens punkt 6.2. Vedlegget er unntatt offentlighet fordi kunnskap om innholdet vil kunne lette gjennomføring av straffbare handlinger, jf. offentlighetsloven § 24, tredje ledd.

## 6.1. Problemstilling 1 – grunnlag for og planlegging av sikkerhetstiltak

### 6.1.1. Sikkerhetsmål og sikkerhetsstrategi

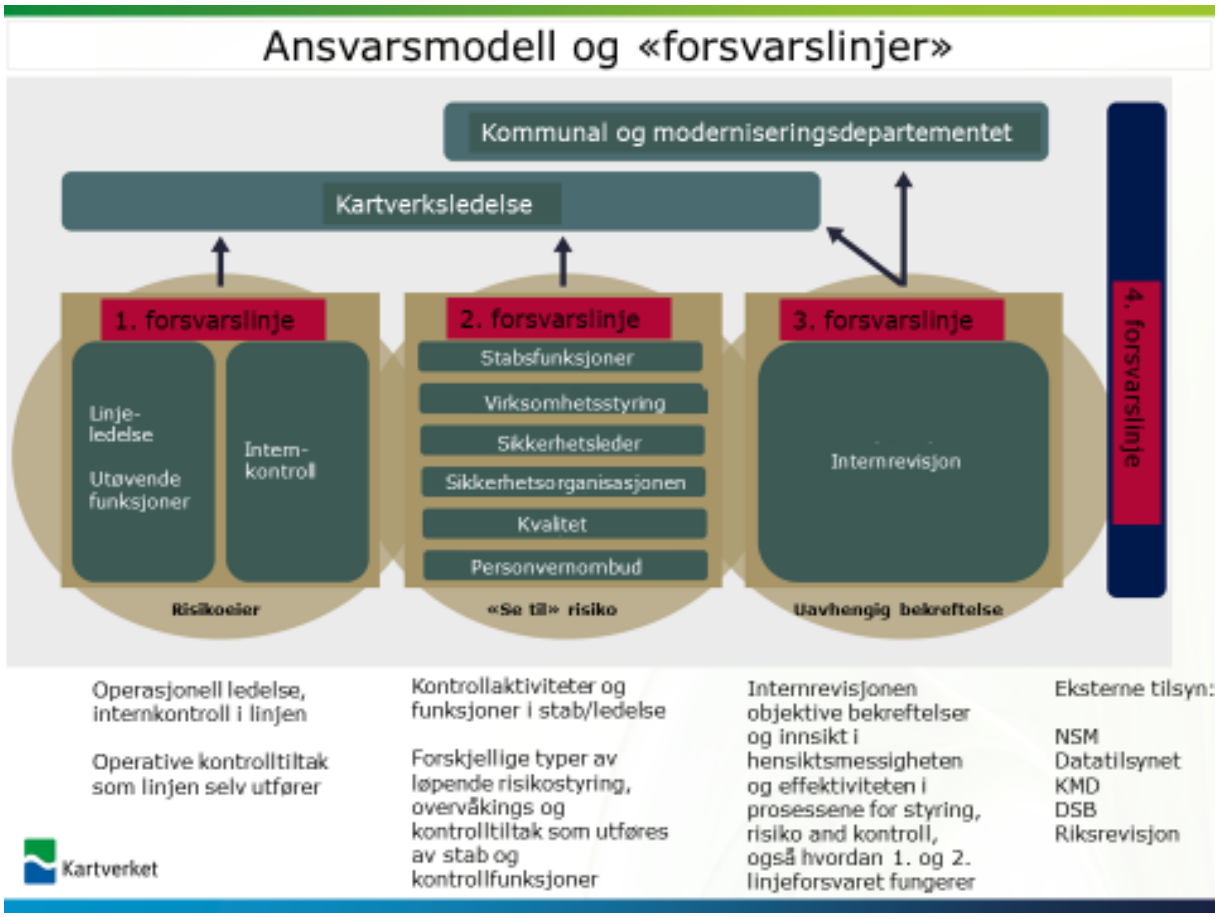
Ifølge eForvaltningsforskriften § 15 første ledd skal mål og strategi for informasjonssikkerhet i virksomheten være beskrevet (sikkerhetsmål og sikkerhetsstrategi) og danne grunnlaget for virksomhetens internkontroll (styring og kontroll) på informasjonssikkerhetsområdet.

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.

Det praktiske informasjonssikkerhetsarbeidet i Kartverket utøves i linjen. Risikostyring og kontrollaktiviteter gjennomføres av ledelsen. Kartverkets internrevisjon gjennomfører blant annet kontroller for å undersøke om og hvordan aktiviteter og prosesser i styring og kontrollarbeidet i forsvarslinje 1 og 2 fungerer. Se figuren nedenfor.

*Figur 1: Kartverkets ansvarsmodell for informasjonssikkerhet*




*Kilde: Kartverket*

**Sikkerhetsmål og strategier**

Revisjonen viser at Kartverket har utarbeidet en sikkerhetspolicy for informasjonssikkerhet[14] som gir et overordnet rammeverk og retningslinjer for sikkerhetsstyring internt i Kartverket og eksternt mot Kartverkets samarbeidspartnere. Formålet med policyen er å sikre hensiktsmessig og nødvendig informasjonssikkerhet gjennom kartlegging og synliggjøring av behov og tiltak. I policyen defineres Kartverkets hovedmål for informasjonssikkerhet som at Kartverkets informasjonsverdier skal sikres med hensyn til konfidensialitet, integritet og tilgjengelighet.

Policyen beskriver struktur, organisering, overordnede krav og prinsipper for sikkerhetsstyring, og er et grunnlag for underliggende dokumentasjon. Sikkerhetspolicyen er godkjent av kartverkssjefen, og sikkerhetsleder er ansvarlig for å utvikle og ajourholde den. Sikkerhetspolicyen skal revideres fortløpende ved endringer, men minst én gang hvert år, fortrinnsvis ved ledelsens gjennomgang, jf. punkt 1.3.[15] ISO 27001 og sikkerhetsloven med forskrifter skal ifølge sikkerhetspolicyen danne grunnlaget for internkontroll på sikkerhetsområdet. Kartverket skal etterleve sikkerhetsloven, personopplysningsloven, arkivloven og e-forvaltningsforskriften.

I «Grunnlagsdokument for sikkerhet»[16] (GDS) er styringssystemet for informasjonssikkerhet samt Kartverkets sikkerhetsorganisasjon beskrevet. Dokumentet er godkjent av kartverkssjefen. Sikkerhetsleder er ansvarlig for å utvikle og vedlikeholde dokumentet. Det skal oppdateres fortløpende, og revideres minst en gang hvert år.

Kartverkssjefen har det overordnede ansvaret for sikkerhetsarbeidet. Kartverkets sikkerhetsorganisasjon (sikkerhetsforum) ledes av Kartverkets sikkerhetsleder. I tillegg er lokale sikkerhetsledere fra fem divisjoner,

[14] Sikkerhetspolicy informasjonssikkerhet, versjon 2, 02.05.2017.
[15] Organisasjonens øverste ledelse skal gjennomgå ledelsessystemet for informasjonssikkerhet med planlagte mellomrom for å sikre at det fortløpende er velegnet, tilstrekkelig og virkningsfullt.
[16] Grunnlagsdokument for sikkerhet, versjon 10.0, 31. desember 2016.

datasikkerhetsleder, leder for fysisk sikkerhet og leder for IT systemsikkerhet faste medlemmer. Sikkerhetsorganisasjonen skal bidra med krav, kontroll, rådgiving og koordinering innen sikkerhetsstyring, datasikkerhet, personellsikkerhet, fysisk sikkerhet og beredskap. Det praktiske sikkerhetsarbeidet skal utføres i linjen. Det betyr at ledere, prosesseiere, systemeiere, prosjekteiere, objekteiere og andre informasjonsverdieiere har et selvstendig ansvar for sikkerheten på sine virkeområder.

For å sette i verk sikkerhetspolicy for informasjonssikkerhet og GDS har Kartverket på noen områder utarbeidet prosedyrer, rutiner, veiledninger, m.m. som beskriver sikringstiltak. Dette er også omtalt under punkt 6.2.1, «Dokumentasjon – policy/retningslinjer/rutiner».

**Grunnlag for sikkerhetstiltak**
I punkt 2.2. i sikkerhetspolicyen står det at Kartverket skal ha oversikt over de informasjonsverdiene det råder over, og de truslene og sårbarhetene det er eksponert for. På bakgrunn av dette skal Kartverket utvikle sikkerhetstiltak som er tilpasset akseptabelt risikonivå. Da Kartverket i 2016 hadde etablert et styringssystem for informasjonssikkerhet i tråd med ISO 27001, ble det gjennomført en ekstern gjennomgang av styringssystemet. Et av forbedringspunktene som ble anbefalt i rapporten etter den eksterne gjennomgangen, var at Kartverket måtte tilpasse SoA-dokumentet[17] slik at det gir en fullstendig oversikt over alle sikkerhetstiltak i Kartverket. SoA-dokumentet mottatt fra Kartverket i januar 2018 viser alle sikringstiltakene i *Tillegg A – Referanser for sikringsmål og sikringstiltak til ISO 27001.* Tiltakene skal være etablert.

**Kommunikasjon av sikkerhetspolicy**
Revisjonen viser at sikkerhetspolicy for informasjonssikkerhet er kommunisert til de ansatte[18] og aktuelle samarbeidspartnere. Den ligger også tilgjengelig på Kartverkets intranett. I møte i sikkerhetsforum 10. oktober 2017 ble opplæring og synliggjøring av sikkerhet i Kartverket drøftet. Det ble konkludert med at det var behov for ytterligere opplæring internt, og det ble besluttet å opprette en arbeidsgruppe for å kartlegge behov og lage forslag til tiltak til for opplæring og synliggjøring.[19] Det er et prioritert tiltak for Kartverket i 2018 å styrke sikkerhetskulturen i hele virksomheten gjennom økt risikoforståelse og tydeliggjøring av ansvarslinjer.[20]

### 6.1.2. Identifisering og klassifisering av informasjonsaktiva/-verdier

I følge eForvaltningsforskriften § 15 fjerde ledd bokstav g) skal sikkerhetsstrategien og internkontrollen også stille nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Personopplysningsforskriften § 2-4 stiller krav om at det skal føres oversikt over hvilke personopplysninger som behandles. I § 2-16 i personopplysningsforskriften er det krav om at rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres.

ISO 27002 punkt 8.1 anbefaler at aktiva tilknyttet informasjon eller behandling av informasjon identifiseres og registreres, og at det pekes ut en eier som har ansvar for det enkelte aktivum. Videre anbefales det i punkt 8.2 at informasjon klassifiseres i henhold til juridiske krav, verdi, alvorlighetsgrad og sensitivitet. Dette bør gjøres for å sikre at informasjonen får et tilstrekkelig beskyttelsesnivå.

I punkt 24.1 i «Grunnlagsdokument for sikkerhet» går det fram at «Alle informasjonssystemer i Kartverket skal klassifiseres og inngå i egen liste som forvaltes av IT». Revisjonen viser at Kartverket ikke har utarbeidet overordnede rutiner eller prosedyrer for klassifisering av aktiva i virksomheten.[21] Kartverket klassifiserer informasjon med utgangspunkt i systemene som behandler informasjonen.

Kartverket vurderer blant annet følgende kriterier ved klassifisering:[22]

- om systemet behandler personopplysninger
- konsekvenser av produksjonsstopp
- om det er skjermingsverdige objekter i systemet
- hvilke lovkrav systemet er omfattet av

[17] Statement of Applicability – Tillegg A – Referanse for sikringsmål i ISO 27001
[18] Dokument «Informasjon til deg som leder», datert 2.desember 2016
[19] Referat fra møte i Sikkerhetsforum 10. oktober 2017.
[20] Dokument «Kartverkets sikkerhetstilstand 2017»
[21] Bekreftet av sikkerhetsleder per telefon 14. februar 2018.
[22] Bekreftet referat etter møte i Kartverket 25. oktober 2017.

Kartverket opplyser at det ikke er dokumentert hvilke vurderinger som ligger til grunn for klassifiseringen av de ugraderte informasjonssystemene. Ledelsen i hver divisjon identifiserer og klassifiserer divisjonens informasjonssystemer før den går videre til behandling i ledelsen på Kartverksnivå. Divisjonenes prioriteringer med hensyn til om systemet kategoriseres som kritisk vurderes ikke opp mot hverandre.[23] Det er opplyst at vurderinger og premisser for kritiske systemer vil bli en del av applikasjonsporteføljeforvaltningen som skal få en bedre systematikk i 2018.[24]

Kartverket legger vekt på linjeprinsippet i arbeidet med informasjonssikkerhet, og sikkerhet for øvrig. Hver divisjon har ansvar for å identifisere og klassifisere de informasjonssystemene divisjonen er systemeier for. Systemene er beskrevet i *IT systemoversikt Kartverket*. Systemoversikten omfatter alle de store og viktige systemene, og viser blant annet hvem som er systemeiereier, hvilke oppgaver det løser, og om det behandler personopplysninger. Behandlingshjemmel (lov) det aktuelle systemet har for behandling av aktuell informasjon, fremgår også i dokumentet. Oversikten over hvilke personopplysninger som behandles i de ulike systemene er imidlertid ikke fullstendig, da det for noen systemer ikke går tydelig fram hvilke personopplysninger som behandles. I e-post av 9. mars 2018 har revisjonen mottatt en foreløpig mal, «Oversikt over behandling av personopplysninger», som er under utarbeidelse i forbindelse med Kartverkets arbeid med å sette i verk kravene i ny personopplysningslov som trer i kraft i løpet av 2018. Malen vil kunne gi Kartverket en dokumentert oversikt over hvilke personopplysninger som behandles i deres IKT-systemer.

### 6.1.3. Risikostyring

Ifølge eForvaltningsforskriften § 15 tredje ledd skal omfang og innretning på internkontrollen være tilpasset risiko. ISO 27001 punkt 6.1.2 anbefaler virksomheten å etablere en prosess for risikovurderinger på informasjonssikkerhetsområdet. Prosessen bør inneholde kriterier for risikoaksept, identifisering-, analyse- og evaluering av risiko. Gjentatte risikovurderinger bør gi konsistente, gyldige og sammenlignbare resultater.

I ISO 27001 punkt 5.1 om lederskap og forpliktelse anbefales det i punkt b at ledelsen skal sikre at kravene i ledelsessystemet for informasjonssikkerhet integreres i organisasjonens øvrige styringsprosesser. Revisjonen legger til grunn at risikostyring på informasjonssikkerhetsområdet skal inngå i Kartverkets ordinære prosess for virksomhetsstyring, og at risikoanalyser skal gjennomføres på et nivå som viser risiko for informasjonssikkerhet i Kartverket som helhet.

I punkt 6.1.3 i ISO 27001 går det fram at virksomheten bør definere og benytte en prosess for risikohåndtering av resultatet av risikovurderingene.

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

I GDS slås det fast at risikovurderinger skal være bærebjelken i det forebyggende sikkerhetsarbeid i Kartverket. Dokumenterte risikovurderinger skal være en del av virksomhetens styringsgrunnlag.

Kartverket skal gjennomføre risikovurderinger for de aktivitetene, systemene/fagsystemene, tjenestene, og/eller områdene som det etter lov og forskrift er stilt krav til, og som er viktige/kritiske for Kartverket og samfunnet. I henhold til rutinen skal risikovurderinger følges opp årlig.[25]

Revisjonen viser at Kartverket har utarbeidet *Rutine – ROS-analyse av sikkerhet (26. april 2017),* som beskriver formål, prosedyrer og hvilke kompetansegrupper som er aktuelle deltakere i gjennomføringen av risiko- og sårbarhetsanalyser (ROS-analyse).

[23] Bekreftet referat etter møte i Kartverket 25. oktober 2017.
[24] E-post av 4. desember 2017 som svar på spørsmål i vår e-post av 20. november.2017.
[25] *ROS-analyser av sikkerhet*, 26. april 2017, Pkt. 2.1.

Tiltak som følge av funn som avdekkes i en dokumentert ROS-analyse skal følges opp via avviks- og forbedringsverktøyet TQM i linjen. IT-prioriteringsrådet kan ha en sentral rolle i denne oppfølgingen.[26]

I Kartverkets sikkerhetspolicy er det beskrevet at det er ledelsens ansvar å beslutte og kommunisere aktuelt risikoakseptnivå og risikotoleranse. Kartverket har ikke utarbeidet risikoakseptkriterier generelt[27] fordi disse tilpasses den enkelte analyse. I prosedyre for ROS-analyse[28], med tilhørende mal[29], er det laget et utgangspunkt som eventuelt kan tilpasses. Punkt 6 i denne malen inneholder veiledning til hva som er akseptabel risiko for tilgjengelighet, konfidensialitet og integritet. Ledelsen i den aktuelle divisjonen fastsetter akseptabelt risikonivå med bakgrunn i anbefalinger i ROS-analysen.

Kartverket gjennomfører ikke ROS-analyse på overordnet nivå, men det utarbeides en årlig rapport om sikkerhetstilstanden i Kartverket.[30] Dette er en vurdering og oppsummering av sikkerhetstilstanden, og regnes som en overordnet risikovurdering i forbindelse med ledelsens årlige gjennomgang. Rapporten inngår som vedlegg til Kartverkets årlige rapport til Kommunal- og moderniseringsdepartementet.

I dokumentet *IT systemoversikt* har Kartverket listet opp sine kritiske systemer. Risikoanalysene skal oppdateres årlig for de kritiske systemene. Revisjonen viser at risikoanalysen bare er oppdatert for et utvalg av systemene i 2017. Kartverket opplyser at det er i en overgangsfase, men at alle
ROS-analysene skal være oppdatert i løpet av 2. tertial 2018, og at alle tiltak skal registreres og følges opp i TQM.[31]

For å oppnå enhetlige analyser og vurderinger av risiko er det to dedikerte personer som deltar i arbeidet med de fleste risikoanalysene som gjennomføres.[32] Som et ekstra ledd for å sikre samme nivå på ROS-analysene blir enkelte av analysene gjennomgått av sikkerhetsleder.[33]

IT-prioriteringsrådet skal vurdere gjennomførte ROS-analyser, og kontrollere at disse er gjennomført i henhold til vedtatte rutiner, både kvalitets- og tidsmessig.[34]

En gjennomgang av et utvalg gjennomførte ROS-analyser[35] viser at det i disse er definert faktor for akseptabel risiko. Identifiserte risikoer blir beskrevet med mulige konsekvenser og eksisterende risikoreduserende tiltak. I tillegg er det skissert eventuelle ytterligere tiltak som må settes i verk for å redusere risiko til akseptabelt nivå.

Tiltak som planlegges gjennomført, registreres og følges opp i avviks- og forbedringsverktøyet TQM. Utskrift fra TQM for grunnboken og matrikkelen for sist gjennomførte ROS-analyse på disse systemene viser at det er beskrevet gjennomførte og planlagte tiltak. Kartverket har opplyst at flere ROS-analyser ble gjennomført før Kartverket tok i bruk TQM, og tiltak fra disse ROS-analysene er derfor ikke registrert i systemet.

I dokumentet *Kartverkets sikkerhetstilstand 2017* er et prioritert tiltak at det i 2018 skal gjennomføres flere og bedre ROS-analyser for risikoutsatte prosesser, prosjekter, anskaffelser og informasjonssystemer. Målet er at dette skal føre til et bedre overordnet risikobilde som grunnlag for risikobaserte beslutninger.

## 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 grunnboken og matrikkelen med underliggende infrastruktur (klienter (PC-er), database, applikasjonsserver og nettverk. Dette inkluderer tilgangskontroller, logging, sikkerhetsoppdatering, og kontroll med enheter og programvare.

[26] Dokument «ROS-analyser av sikkerhet», 26. april 2017, pkt. 2.6.
[27] Notat av 3.10.17 fra sikkerhetsleder - Dokumentasjon for revisjon av informasjonssikkerhet
[28] Dokumentet ROS-analyser av sikkerhet av 26. april 2017
[29] Mal risiko- og sårbarhetsanalyse
[30] Kartverkets sikkerhetstilstand 2017, datert 26. januar 2018
[31] E-post fra Kartverket av 4. desember.2017 som svar på spørsmål i vår e-post av 20. november.2017.
[32] Bekreftet referat etter møte i Kartverket 25. oktober 2017.
[33] Bekreftet referat etter møte i Kartverket 25. oktober 2017.
[34] Bekreftet referat etter møte i Kartverket 25. oktober 2017.
[35] ROS-analyse - Fagsystem elektronisk tinglysning 18.09.2017, ROS-analyse - Matrikkelsystemet - 26.09.2017, ROS-analyse Arken 22.12.2017, ROS-analyse Satref 1.1.2014, ROS-analyse sentral felles kartdatabase 27.5.2016

### 6.2.1. Dokumentasjon - policy/retningslinjer/rutiner

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.

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 for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet 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.

I Kartverket skal det praktiske sikkerhetsarbeidet utføres i linjen, jf. punkt 6.1. Det går fram av GDS at operasjonelle prosedyrer skal være dokumentert som en del av IT-tjenestens kvalitetssystem. Videre skal det være utarbeidet detaljerte sjekklister for det enkelte system som kan sikre kontinuerlig drift og være til hjelp ved feilsøking og feilretting for å imøtekomme utskifting av personell eller perioder med tynnere bemanning. Kartverkets SoA-dokument inneholder oversikt over alle sikkerhetstiltakene som er skissert i *Tillegg A – Referanser for sikringsmål og sikringstiltak til ISO 27001*. I SoA-dokumentet er alle tiltak vurdert til å være etablert. I følge dokumentet er driftsprosedyrer dokumentert, vedlikeholdt og gjort tilgjengelig som en del av driftsdokumentasjonen på IT.

Revisjonen viser imidlertid at Kartverket i varierende grad har utarbeidet rutiner, prosedyrer eller lignende som benyttes i driften av etatens systemer. Rutiner og driftsprosedyrer synes ikke å være dokumentert på en systematisk og helhetlig måte. Videre finnes det ikke dokumentasjon som beskriver når og hvordan etterkontroll og evaluering av de enkelte sikkerhetstiltakene skal gjennomføres.

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

- tilgangsstyring i grunnboken og matrikkelen
- logging og oppfølging av logger i forbindelse med drift av grunnboken
- lokale administratorer (delvis)
- oppdatering av databaser (praktisk driftsprosedyre)
- tilgangsstyring av administratortilganger på servere

For øvrige tiltak som er omfattet av revisjonen er det ikke utarbeidet beskrivelse av krav til og gjennomføring. Dette gjelder:

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

Kommunal- og moderniseringsdepartementet opplyser[36] at Kartverket har etablert to ulike sett vaktpermer for å sikre kontinuerlig drift og avhjelpe ved feilsøking og feilretting. Vaktpermene ble ikke forelagt ved revisjonsbesøket, men er oversendt i mai 2018. Vaktpermene synes ikke å inneholde instruksjoner for blant annet installering og konfigurering av systemer (inkludert oppdatering), og heller ikke for logging og overvåking slik ISO 27002 anbefaler. Departementet opplyser videre at noen prosedyrer er godt kjent av de medarbeiderne det gjelder og anses som etablert praksis, men er ikke dokumentert.

### 6.2.2. Gjennomføring av sikkerhetstiltak

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

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.

I SoA-dokumentet går det fram at alle tiltakene skal være etablert. Revisjon av utvalgte tekniske tiltak viser at enkelte av de utvalgte tiltakene ikke er etablert, eller er at de er svakere enn anbefalt/beste praksis.

**Tilgangskontroller**
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 arbeidsforholdet.

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.

Saksbehandlerrettigheter
Kartverket har etablert en formell prosess for registrering, endring og sletting av tilganger og rettigheter i grunnboken og matrikkelen, men dokumenterer i varierende grad prosessen. Det er definert hvem som kan bestille og registrere rettigheter både for interne og eksterne brukere i systemene.

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 få tilgang til mer enn det som er nødvendig for utførelsen av oppgavene. Videre bør det vedlikeholdes en autorisasjonsprosess og fortegnelse over alle tildelte rettigheter. Privilegerte tilgangsrettigheter bør tildeles en annen brukerkonto enn den som brukes for vanlige aktiviteter i virksomheten.

Revisjonen har omfattet administratorrettigheter på klient, database, server og nettverk. Kartverket etterlever i varierende grad anbefalinger om å etablere en formell autorisasjonsprosess og å begrense og kontrollere administratorbrukere.

Passord
Passord i AD styrer autentisering av brukere ved pålogging i grunnbok, matrikkel, databaser, servere og nettverk.

ISO 27002 punkt 9.4.3 anbefaler at virksomheten har et system som sikrer passordkvalitet og jevnlig bytte av passord.

Microsoft anbefaler at det settes strenge krav til autentisering ved bruk av kontoer med privilegerte rettigheter, i utgangspunktet flefaktor-autentisering.[37]

Samme passordkrav gjelder for kontoer med utvidede rettigheter som til øvrige brukerkontoer i Kartverkets nettverk. Det er ikke satt sterke krav til autentisering av brukere med utvidede rettigheter i samsvar med

[36] Brev av 27. april 2018 fra Kommunal- og moderniseringsdepartementet til Riksrevisjonen, vedlagt notat fra Statens kartverk av 19. april 2018 om tilbakemelding på rapportutkast med vedlegg
[37] 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)

anbefalinger. Svakheter i autentisering av brukere kan gjøre det enklere for angripere å overta brukerkontoer med utvidede rettigheter.

**Logging**
ISO 27002 punkt 12.4.1 anbefaler at det produseres hendelseslogger som registrerer brukeraktiviteter (inkludert påloggingsinformasjon og bruk av privilegier), avvik, feil og informasjonssikkerhetshendelser. Videre anbefales det at logger oppbevares og gjennomgås regelmessig, og at logginformasjon beskyttes mot misbruk og uautorisert tilgang.

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.

Revisjonen viser at Kartverket i varierende grad har aktivert logger. Loggene overføres til loggservere og kopieres over på tape for sikker oppbevaring. Kartverket følger i hovedsak opp logger i forbindelse med drift av systemene, og ikke sikkerhet. Revisjonen viser videre at Kartverket har:

- aktivert logging i applikasjonene. Loggene viser aktiviteter og historikk for saksbehandling.
- for underliggende infrastruktur er det flere mangler i oppsett av sikkerhetslogger.

**Oppdatering**
NSM anbefaler at sikkerhetsoppdateringer for installert programvare blir tatt i bruk så fort som mulig.[38] NSM framhever dette tiltaket som et av de fire viktigste tiltakene mot dataangrep.[39] Center for Internet Security anbefaler at virksomheter tar i bruk verktøy som automatisk oppdaterer operativsystem og annen programvare for alle systemer.[40] Sikkerhetsoppdateringer beskytter virksomheten mot sårbarheter som kontinuerlig oppdages i programvare.

Kartverket bruker et system for håndtering av oppdateringer for operativsystem og programvare fra Microsoft. Oppdateringer rulles ut etter en testperiode på en gruppe testbrukere. Revisjonen viser at oppdateringer synes å ha blitt rullet ut på Kartverkets servere. Det er enkelte avvik i oppdateringen av klienter. Kartverket har ikke utarbeidet rutiner for oppdatering av databaser, og databasene er ikke tilstrekkelig oppdatert. Utstyr som ikke er oppdatert med siste sikkerhetsoppdateringer er sårbare for kompromittering.

**Program- og maskinvare**
ISO 27002 punkt 12.6.2 anbefaler at det etableres og håndheves strenge regler for hvilken programvare sluttbrukere kan installere. NSM anbefaler at bare eksplisitt autorisert programvare kjøres på virksomhetens enheter, og at det bare installeres programvare med nødvendig funksjonalitet for å støtte virksomhetens forretningsprosesser.[41] NSMs anbefalinger samsvarer med standard fra Center for Internet Security.[42] Bakgrunnen for anbefalingene er at dataangrep ofte innebærer installasjon av ondsinnet programvare og/eller utnyttelse av svakheter i ordinær programvare.

Revisjonen viser at Kartverket i liten grad har styring av programvare på klienter, men arbeider med en løsning for sikrere plattform.

Det synes å være lite programvare installert på applikasjonsserverene for grunnboken og matrikkelen. På klientene synes det imidlertid å være installert mer programvare enn det som er nødvendig.

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

[38] NSMs grunnprinsipper for ikt-sikkerhet, versjon 1.0, punkt 3.2
[39] Nasjonal sikkerhetsmyndighet: Fire effektive tiltak mot dataangrep (Sjekkliste nr. 1)
[40] The Center for Internet Security (CIS): Critical Security Controls (CSC) for effective cyber defense, punkt 4
[41] NSMs grunnprinsipper for ikt-sikkerhet, versjon 1.0, punkt 2.3
[42] The Center for Internet Security (CIS): Critical Security Controls (CSC) for effective cyber defense, punkt 2

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

Kartverket har i varierende grad etablert tiltak for å begrense muligheten for å koble til uautorisert utstyr i nettverket. Kartverket arbeider med en løsning for å utbedre svakheter.

### 6.2.3. Etterkontroll/evaluering av sikkerhetstiltak

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 bør informasjonssystemer regelmessig gjennomgås for å sikre samsvar med organisasjonens policyer og standarder for informasjonssikkerhet.

Personopplysningsforskriften § 2-5 stiller krav om at det gjennomføres jevnlige sikkerhetsrevisjoner av sikkerhetstiltak. Bestemmelsen pålegger den behandlingsansvarlige jevnlig, eksempelvis årlig, å etterprøve sikkerhetsarbeidet for å verifisere at de sikkerhetstiltakene som er besluttet etablert, faktisk er satt i verk og fungerer etter hensikten. Resultater fra denne typen sikkerhetsrevisjoner vil være grunnlaget for ledelsens gjennomgang av sikkerhetsmål og strategier og et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerheten.[43]

I GDS kapittel 9 om samsvar og risikobasert sikkerhet står det følgende:

> *«Kartverket har omfattende eksterne og interne krav til virksomheten, og det er behov for metodikk og systematisk gjennomgang for å sikre samsvar og etterlevelse. Dette gjelder både juridiske og kontraktsmessige krav, og Kartverkets egne bestemmelser innen sikkerhet. Tilnærmingen til dette følger i hovedsak linjeprinsippet ved at de som står for anskaffelser, utvikling, prosesser osv. har ansvar for å identifisere gjeldende lovgiving/forpliktelser og å utvikle tilstrekkelige tiltak og oppfølging for å sikre samsvar.»*

For Kartverkets systemer og infrastruktur er det i liten grad beskrevet hvilke tiltak som skal settes i verk og hvordan. Utover overordnet føring om etterkontroll i GDS er det ikke stilt krav om evaluering eller etterkontroll av iverksatte tiltak. Sikkerhetstiltak synes ikke å bli fulgt opp på en jevnlig og systematisk måte, og ledelsen etterspør heller ikke dette. Jf. punkt 6.2.1. og 6.3. Manglende etterlevelse omtalt i 6.2.2 er avvik som ville ha blitt fanget opp av etterkontroller.

Revisjonen har omfattet etterkontroll av tilgangsstyring, logging, oppdatering samt program- og maskinvare, og viser at Kartverket i liten grad har gjennomført etterkontroller av sikkerhetstiltak eller evaluert om de fungerer etter hensikten. Dette omfatter følgende:

- Det er etablert etterkontroll av brukere og tildelte rettigheter i grunnboken og matrikkelen. For administratorrettigheter og passord på klient, database, server og nettverk er det imidlertid ikke gjennomført etterkontroller.

- En etterkontroll/evaluering av arbeidet med logger vil for eksempel innebære en kontroll av om det er satt i verk tilstrekkelig logging i forhold til virksomhetens krav til det aktuelle informasjonssystemet, og hvorvidt loggene er fulgt opp i henhold til interne regler. En etterkontroll er først aktuelt når det er stilt krav om logging og at loggene benyttes aktivt i virksomheten. Kartverket har ikke etablert etterkontroll av logging og oppfølging av logger.

- Kartverket benytter systemet for håndtering av oppdateringer for å sjekke status for operativsystem og programvare på klienter og servere. Men det gjennomføres ikke jevnlige eller systematiske etterkontroller for å sikre at klienter og servere er oppdatert. Det er heller ingen oppfølging av oppdatering av databaser.

- Det er ikke etablert etterkontroller for å verifisere at det bare er godkjent programvare og autoriserte enheter i nettverket.

43 «Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer» Datatilsynet 2000.

## 6.3. Problemstilling 3 – oppfølging og evaluering av sikkerhetstiltak

### 6.3.1. Avviks- og hendelseshåndtering

Ifølge eForvaltningsforskriften § 15 fjerde ledd bokstav g) skal sikkerhetsstrategien og internkontrollen også stille nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

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.

ISO 27002 punkt 16.1 anbefaler at det etableres ansvarslinjer for oppfølging av informasjonssikkerhetshendelser, og at det utarbeides og kommuniseres prosedyrer for å overvåke, oppdage, analysere og rapportere om informasjonssikkerhetshendelser og -brudd. Videre anbefaler standarden at det etableres prosedyrer for å reagere på og håndtere informasjonssikkerhetshendelser. I punkt 16.1.6 anbefales det at erfaringer fra informasjonssikkerhetshendelser brukes for å redusere sannsynlighet for, eller konsekvens av, framtidige hendelser.

GDS definerer roller og ansvar for sikkerhetsarkitektur, sikker drift og utvikling, samt oppdagelse og håndtering av dataangrep.

Kartverket opplyser at sikkerhetstruende hendelser er definert som forsøk på inntrengning, innbrudd på systemene eller tyveri av data.[44]

Av punkt 27 i GDS går det fram at hendelseshåndtering skal følge NSMs anbefalinger. Rutinen *Håndtering av avvik og forbedringstiltak* skal sikre at avvik/hendelser følges opp på en systematisk og enhetlig måte. Den beskriver blant annet avvik, bevishåndtering, behandling av hendelser, og verktøy for registrering, oppfølging og forbedring.

Videre inneholder beredskapsplanen for IT-divisjonen også retningslinjer for hvordan uønskede hendelser innen informasjonssikkerhet skal håndteres.

Avdekkede sikkerhetshendelser skal behandles og rapporteres i linjen, og registreres i avviks- og forbedringsverktøyet *TQM forbedring* i henhold til egne rutiner. Ved alvorlige sikkerhetshendelser skal sikkerhetsleder[45] informeres/involveres. Når det avdekkes kritiske sårbarheter ved Kartverkets digitale infrastruktur skal også datasikkerhetsleder[46] involveres.[47]

Ansvaret for å holde oversikt og følge opp rapporterte sikkerhetshendelser følger av linjeansvaret i Kartverket. I tillegg har sikkerhetsleder et overordnet ansvar for at hendelser blir fulgt opp. Oppfølging av hendelser skjer ved hjelp av TQM. Det gjennomføres analyse av registrerte hendelser blant annet med tanke på å redusere sannsynlighet og konsekvens for tilsvarende hendelser.[48]

For å kontrollere om sikkerhetshendelser blir registrert i TQM og fulgt opp, er to interne[49] og to eksterne hendelser[50] gjennomgått. Det foreligger en beskrivelse og analyse, kommentar-/konsekvensbeskrivelse, samt oversikt over hvilke tiltak som er gjennomført. Videre går det fram hvem som har registrert hendelsen, hvem som er ansvarlig for å følge opp, og dato for lukking av hendelsen.

Årsrapportene fra divisjonene viser at det stor variasjon mellom divisjonene i antall hendelser og avvik som rapporteres i TQM, fra 21 til 435. I dokumentet *Kartverkets sikkerhetstilstand 2017* er det antydet at dette kan skyldes ulik bruk av verktøyet, ved at noen enheter underrapporterer hendelser, selv om de er kjent som sikkerhetstruende.

[44] Bekreftet referat etter møte i Kartverket 25. oktober 2017.
[45] Sikkerhetsleder er Kartverkssjefen sikkerhetsfaglige rådgiver, etablerer styringssystem for sikkerhet og forvalter dette.
[46] Datasikkerhetsleder er Kartverkssjefens IT-sikkerhetsfaglige rådgiver og skal etablere den delen av styringssystemet for sikkerhet som gjelder IT-sikkerheten og forvalte dette.
[47] Grunnlagsdokument for sikkerhet, punkt 28
[48] Veiledning for bruk av TQM avviks- og forbedringsverktøy
[49] Hendelse-ID: 3765 og 4080
[50] Hendelse-ID 3418 og 3825

### 6.3.2. Interne sikkerhetsrevisjoner

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.

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

I kapittel 14 i GDS er det krav om at Kartverket årlig skal gjennomføre uavhengige internrevisjoner på utvalgte styringssystemer og prosesser med vekt på sikkerhet for å vurdere etterlevelse og hensiktsmessighet. Kartverket har laget en rutine[51] som beskriver hvordan interne revisjoner skal planlegges, settes i verk og følges opp. Dette omfatter både revisjoner som har til formål å måle at Kartverkets kvalitetssystem fungerer, og revisjoner av virksomhetens styringssystem for informasjonssikkerhet. Resultatet fra alle typer revisjoner skal benyttes til forbedring og skal være et sentralt ledelsesverktøy for å nå Kartverkets kvalitetsmål.

Revisjonen viser at det er utarbeidet en plan for revisjoner, tilsyn og beredskapsøvelser i 2017.[52] Av denne planen går det fram at det er planlagt interne revisjoner av sikkerhetsstyring som grunnlag for å forbedre styringssystemet for informasjonssikkerhet. Dokumentet oppdateres løpende, og versjonen datert 7. september 2017 viser at det er gjennomført og pågår revisjoner som grunnlag for forbedring av sikkerhetsstyringen.

I tillegg til interne revisjoner leier Kartverket inn eksterne aktører til å gjennomføre revisjoner og tester. Dette har bakgrunn i at det er ønskelig med uavhengig testing, og i tillegg kan det være nødvendig med spesialkompetanse som Kartverket ikke har. Som eksempler på revisjoner/tester utført av eksterne nevner Kartverket sikkerhetstesting av Kartverkets eksponerte infrastruktur og ekstern bistand i forbindelse med en beredskapsøvelse for hendelseshåndtering på IT.[53]

Etter gjennomførte revisjoner går sikkerhetsleder gjennom rapportene og følger opp at avdekkede avvik blir fulgt opp i linjen.[54] Sikkerhetsleder er også leder for Kartverkets internrevisjon, men deltar ikke aktivt i gjennomføring av sikkerhetsrevisjoner.

### 6.3.3. Evaluering og forbedring av styringssystemet for informasjonssikkerhet

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.

ISO 27001 punkt 9.1 anbefaler at virksomheten skal evaluere prestasjonen til og virkningen av styringssystemet for informasjonssikkerhet. Standardens punkt 9.3 anbefaler at ledelsen skal gjennomgå styringssystemet for informasjonssikkerhet jevnlig for å sikre at det fortløpende er velegnet, tilstrekkelig og virkningsfullt.

ISO 27001 kapittel 10 anbefaler at virksomheten skal reagere på eventuelle avvik og innføre korrigerende tiltak. Videre anbefales det at virksomheten kontinuerlig skal forbedre egnetheten, tjenligheten og virkningen til styringssystemet for informasjonssikkerhet.

Revisjonen viser at Kartverkets sikkerhetspolicy gir føringer for at sikkerhet skal være styrt og integrert i ordinær virksomhetsledelse. Dette omfatter blant annet virksomhetsplanlegging, ledelsens gjennomgåelse, revisjoner og systematisk forbedring. Det er også presisert i GDS at ledelsen har ansvar for å veilede og støtte ledere og ansatte og fremme kontinuerlig forbedring innen sikkerhet. Dokumentet *Ledelsens gjennomgåelse* viser hvordan ledelsens gjennomgang skal gjennomføres i tråd med etablerte styringsstandarder (ISO 9001[55] og ISO 27001).

[51] Revisjoner i Kartverket, versjon 7.0
[52] Dokument «Program for revisjon, tilsyn og beredskapsøvelser i Kartverket 2017», versjon 1.1.
[53] Bekreftet referat etter møte i Kartverket 25. oktober.2017
[54] Bekreftet referat etter møte i Kartverket 25. oktober 2017
[55] ISO 9001 Ledelsessystemer for kvalitet.

Ledelsens gjennomgang gjennomføres årlig i Kartverket. Grunnlaget for hva som tas opp i ledelsens gjennomgang starter i de enkelte divisjonene hvor alle avdelingslederne formidler aktuelle saker til divisjonsledelsen, som utarbeider rapport fra den aktuelle divisjonen. Divisjonsdirektørene presenterer rapporten fra sin divisjon i møtet. I tillegg lager sikkerhetslederen en samlet oversikt for hele Kartverket over status på sikkerhetstilstanden.[56]

Referatet fra et ledermøte i Kartverket 26. og 28. september 2017 viser at ledelsen har hatt en gjennomgang av kvalitet og sikkerhet i virksomheten, med bakgrunn i blant annet aktuelle problemstillinger de ulike divisjonene har presentert fra sin divisjon. Videre at det har vært en diskusjon av prinsipielle spørsmål omkring gjennomføring av ledelsens gjennomgåelse i ledermøtet. Fokus har vært på hva Kartverket ønsker med informasjonssikkerhetsarbeidet, og om dette er oppnådd, samt eventuelle tiltak. Kartverket opplyser at de viktigste diskusjonene om informasjonssikkerhet foregår i den enkelte divisjon[57], og ikke i ledelsens gjennomgang.

Utover ledelsens årlige gjennomgang viser tilsendte dokumenter at det også rapporteres på sikkerhet og kvalitet i tertial- og årsrapporter fra divisjonene. Enkeltsaker og ad-hoc-saker løftes opp på øverste ledelsesnivå hvis nødvendig.

Sikkerhetsleder gjennomfører hver måned møte med ledelsen for å orientere om status i sikkerhetsarbeidet. Møtene dokumenteres ikke.

Kartverket har ingen rutine for oppdatering av styringssystemet, men opplyser at dette skjer fortløpende ved behov.[58] Det er imidlertid utarbeidet en egen rutine[59] som skal sikre at oppdatering av styrende dokumenter og fagprosedyrer gjøres på en enhetlig måte.

# 7 Konklusjoner

Statens kartverk samler inn, systematiserer, forvalter og videreformidler geografisk informasjon som er av vital betydning for hele det norske samfunnet. Dette gjelder blant annet eiendomsinformasjon i nasjonalt register for offentlig eiendomsinformasjon, tinglysning i fast eiendom og andeler i borettslag samt kartdata for både land og sjø. Det er viktig at dataene som kartverket forvalter, er tilgjengelige og bevarer konfidensialitet og integritet.

Behov for et styringssystem for informasjonssikkerhet og beskyttelse av sensitiv informasjon øker i takt med digitaliseringen av offentlig forvaltning. Et styringssystem for informasjonssikkerhet skal hjelpe ledelsen, og virksomheten for øvrig til å ha tilstrekkelig styring og kontroll, gjennom systematisk internkontroll på området. Det skal medvirke til at virksomheten velger riktige sikkerhetstiltak, og sørge for at de valgte løsningene blir evaluert og forbedret om nødvendig. Manglende sikkerhetstiltak eller svakheter i etablerte sikkerhetstiltak kan indikere at styringssystemet ikke fungerer på alle områder. Dette kan føre til uheldige konsekvenser for enkeltpersoner, samfunnet, og skade omdømmet til virksomheten.

Målet med revisjonen er å kontrollere om Kartverket har et styringssystem for informasjonssikkerhet som er i henhold til kravene i eForvaltningsforskriften §15 og som ivaretar kravene i personopplysningsloven[60].

Kartverket har innført et styringssystem for informasjonssikkerhet som i stor grad dekker kravene i eForvaltningsforskriften § 15 og ivaretar kravene i personopplysningsloven. Det er utarbeidet mål og prinsipper som definerer prosessene for arbeidet med informasjonssikkerhet og planlegging av sikkerhetstiltak. Dette inkluderer rutiner for risikostyring og avvikshåndtering, men ikke for klassifiseringsarbeid. Det er gitt føringer i styrende dokumenter om at det årlig skal gjennomføres uavhengige internrevisjoner av styringssystemet for å vurdere etterlevelse og hensiktsmessighet, og resultatene av revisjoner skal benyttes til forbedring. Dokumentene som beskriver styringssystemet i Kartverket er godkjent av ledelsen.

Klassifisering av informasjon og systemer skal danne et grunnlag for videre arbeid med risikovurderinger og planlegging av sikkerhetstiltak. Kartverket har klassifisert informasjonssystemene de vurderer som kritiske, men vurderingene som ligger til grunn for klassifiseringen, er ikke dokumentert.

[56] Bekreftet referat etter møte i Kartverket 25. oktober 2017.
[57] Bekreftet referat etter møte i Kartverket 25. oktober 2017.
[58] Notat fra Kartverket av 12. desember 2017.
[59] Dokumentansvarlig og godkjenner – ansvar, versjon 7.0.
[60] Lov om behandling av personopplysninger (personopplysningsloven) 14. april 2000 nr. 31.

Risikoanalyser skal være det bærende element i Kartverkets sikkerhetsarbeid. Oppdatering av risikoanalyser for kritiske systemer er ikke gjennomført slik det går fram av styringssystemet. Kartverket har utarbeidet en oversikt over hvilke sikkerhetstiltak som skal være etablert

For de sikkerhetstiltakene som er omfattet av revisjonen, har Kartverket i varierende grad dokumenterte rutiner, prosedyrer eller lignende som benyttes i driften av etatens systemer. Videre er det ikke dokumentert når og hvordan etterkontroll og evaluering av de enkelte sikkerhetstiltakene skal gjennomføres.

Styringen av arbeidet med informasjonssikkerhet bidrar ikke godt nok verken til planlegging, gjennomføring eller evaluering av sikkerhetstiltak. En del av de tekniske tiltakene som skal være innført, viser seg å ikke være etablert, eller er svakere enn beste praksis. Dette gjelder spesielt database og nettverk. Videre er det i liten grad gjennomført etterkontroller av sikkerhetstiltak eller evalueringer av om disse fungerer etter hensikten. Manglende dokumentasjon og etterkontroll kan være årsaken til at flere av tiltakene som er omfattet av revisjonen ikke er implementert i henhold til beste praksis.

Kartverket har rutiner og systemer for registrering, håndtering og oppfølging av sikkerhetshendelser som synes å fungere. Det er videre stilt krav og innført rutiner for evaluering og forbedring av styringssystemet. Dette skal skje med bakgrunn i sikkerhetshendelser, interne og eksterne revisjoner samt gjennomførte risikovurderinger. Kartverket har identifisert og satt i verk tiltak etter sikkerhetshendelser og etter interne revisjoner. Hovedansvaret for oppfølging og evaluering av sikkerhetstiltakene følger Kartverkers linjeprinsipp, og status skal oppsummeres i ledelsens årlige gjennomgang. Styringssystemet som helhet er imidlertid ikke tilstrekkelig vurdert. De etablerte rutinene synes ikke å ha fanget opp manglende sammenheng mellom planlegging og etablering av sikkerhetstiltak, samt svakheter ved de etablerte tiltakene.