Riksrevisjonen

Utsatt offentlighet jf. rrevl. § 18 (2)

Vår referanse: 2018/01015-100

Revisjonsrapport for 2018 om

Sikring mot dataangrep i Oljedirektoratet

Mottaker: Olje- og energidepartementet

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

Forsidefoto: Pixabay/typographyimages

Innhold

1. Sammendrag

Oljedirektoratet (OD) har en sentral rolle i forvaltningen av olje- og gassressursene på norsk kontinentalsokkel og utøver forvaltningsmyndighet i forbindelse med tildeling av areal og i forbindelse med leting etter og utvinning av petroleumsforekomster. Målet med revisjonen har vært å kontrollere om OD arbeider systematisk med å forhindre dataangrep og oppdage urettmessig tilgang til IKT-systemer.

Betydningen av gode styringssystemer for informasjonssikkerhet og beskyttelse av informasjon som virksomhetene behandler, øker i takt med digitaliseringen av offentlig forvaltning. I flere IKT-systemer behandler OD informasjon som ikke bør komme på avveie, og som eksterne aktører kan være interessert i. Dette er blant annet politisk, børssensitiv og forretningssensitiv informasjon. Det er derfor viktig at OD beskytter informasjonen det forvalter, og sørger for at nettverk og systemer til enhver tid er sikre og stabile. God informasjonssikkerhet er avhengig av at OD har implementert gode og relevante sikkerhetstiltak tilpasset virksomhetens risiko. Det er også viktig at OD har etablert et system for å styre og følge opp at sikkerhetstiltak fungerer etter hensikten, slik at virksomheten kontinuerlig kan forbedre sikkerhetsarbeidet og tilpasse det til endringer i risikobildet og teknologisk utvikling.

Riksrevisjonen har de siste årene gjennomført flere revisjoner av informasjonssikkerhet hvor det er avdekket vesentlige svakheter. Stortingets kontroll- og konstitusjonskomite deler Riksrevisjonens bekymring for svakheter ved informasjonssikkerheten i statlige virksomheter og understreker at mangelfull styring og oppfølging av informasjonssikkerhet er svært alvorlig.[1] Riksrevisjonen fant det sterkt kritikkverdig at OD for 2016 fortsatt ikke hadde et tilfredsstillende styringssystem for informasjonssikkerhet, og kontroll- og konstitusjonskomiteen forutsatte i innstilling 115 S (2017–2018) at departementet umiddelbart iverksatte tiltak for å avhjelpe manglene.

Riksrevisjonen har for 2018 gjennomført en revisjon for å vurdere arbeidet OD gjør for å sikre virksomheten og IKT-systemene mot dataangrep. Revisjonen omfatter styring av informasjonssikkerhet primært rettet mot planlegging av sikring mot dataangrep. Som ledd i revisjonen er det gjort analyser av styrende dokumenter, verdivurdering og risikovurdering for sikring av informasjon. Videre er det vurdert om det er etablert risikoreduserende organisatoriske og tekniske sikkerhetstiltak som er effektive, og eventuelt om tiltakene blir løpende oppdatert ved endringer i risikobildet. I tillegg er et utvalg sikkerhetstiltak testet for å kontrollere om ODs systemer vil motstå og oppdage forsøk på å omgå disse. Det er også kontrollert om OD evaluerer og oppdaterer styringssystemet og sikkerhetstiltak på bakgrunn av hendelser som er observert.

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

- *lov om behandlingsmåten i forvaltningssaker* (forvaltningsloven) § 15 a
- *forskrift om elektronisk kommunikasjon med og i forvaltningen* (eForvaltningsforskriften) § 15
- *reglement for økonomistyring i staten* og *bestemmelser om økonomistyring i staten*

Etter eForvaltningsforskriften § 15 andre ledd skal forvaltningsorgan «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». Revisjonen har også lagt til grunn anbefalinger fra Den internasjonale standardiseringsorganisasjonen (ISO), Nasjonal sikkerhetsmyndighet (NSM) og bransjestandarder. Dette er gjort ut fra en forutsetning om at anbefalingene er beste praksis for styring og gjennomføring av sikkerhetstiltak.

Revisjonen er gjennomført ved dokumentanalyser, intervjuer/møter, analytiske handlinger, observasjoner og test av kontroller.

OD er i likhet med flere andre offentlige virksomheter i Norge et utsatt mål for informasjonsoperasjoner fra andre lands myndigheter og profesjonelle aktører. Trusselbildet som eksisterer, gjør det viktig at OD har et godt system for å sikre informasjonen som behandles. Sikring mot dataangrep er ett aspekt av informasjonssikkerhet, og det blir stadig viktigere som følge av trusselbildet. Den overordnede styringen av informasjonssikkerhetsarbeidet, sikkerhetsmekanismer og sikkerhetstiltak skal være

[1] Innst. 115 S (2017–2018) *Innstilling til Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2016.*

tilpasset risikovurderinger, og informasjonssikkerheten i virksomheten bør følges opp og forbedres kontinuerlig.
Revisjonen for 2018 viser blant annet dette:

- ODs styrende dokumenter for informasjonssikkerhet gir rammer for et systematisk arbeid med å forhindre dataangrep og oppdage urettmessig tilgang til IKT-systemer.
- Det er vesentlige mangler i gjennomføringen av sentrale aktiviteter i styringssystemet. For eksempel er det gjennomført få risikovurderinger.
- ODs IKT-systemer har svakheter som kan utnyttes i forbindelse med dataangrep.
- Grunnlaget for ODs vurderinger i evalueringer og rapportering til departementet samsvarer ikke med forhold som er påvist i revisjonen.

Utkast til revisjonsrapport er lagt fram for Olje- og energidepartementet (OED) i brev av 22. mars 2019. Departementet har i brev av 11. april 2019 gitt kommentarer til rapportutkastet. Departementet har i utarbeidelsen av tilbakemeldingen fått innspill fra OD. Kommentarene er i hovedsak innarbeidet i endelig rapport.

2. Innledning

OD skal bidra til å skape størst mulig verdier for samfunnet fra olje- og gassvirksomheten gjennom en effektiv og forsvarlig ressursforvaltning. Direktoratet har en sentral rolle i forvaltningen av olje- og gassressursene på norsk kontinentalsokkel, og utøver forvaltningsmyndighet i forbindelse med tildeling av areal og i forbindelse med leting etter og utvinning av petroleumsforekomster. I tillegg har OD et nasjonalt ansvar for data fra petroleumsvirksomheten. I dette ligger blandt annet å holde oversikt over og formidle data og analyser. Direktoratet behandler i flere av sine IKT-systemer både intern og ekstern informasjon som ikke bør komme på avveie, og som eksterne aktører kan være interessert i. Dette er blant annet politisk, børssensitiv og forretningssensitiv informasjon, som søknader om produksjonslisenser på norsk sokkel og forskningsrapporter utarbeidet av oljeselskapene.

OD er organisert i en flat og fleksibel organisasjon som består av rundt 80 lag som er delegert myndighet for ulike områder. OD har dermed ingen seksjoner eller avdelinger. I OD er det rundt 220 medarbeidere som endrer lagtilhørighet løpende, og lag opprettes og legges ned ved behov. Lagtilhørighet avgjøres i et ukentlig ressursstyringsmøte. Ledelsen i OD roterer med jevne mellomrom. Oljedirektøren og fire direktører utgjør ODs strategiske ledergruppe, og tolv underdirektører utgjør ODs operative ledelse. Oljedirektøren og den strategiske ledelsen har overordnet resultatansvar og kan delegere myndighet til den operative ledelsen. Blant annet har underdirektøren for informasjonsforvaltning fått myndighet til å følge opp styringssystemet for informasjonssikkerhet, og underdirektøren for IT skal operativt følge opp IKT-driften.[2]

Det har vært en tydelig og jevn økning i antall målrettede dataangrep mot virksomheter i offentlig sektor de siste årene.[3] Politiets sikkerhetstjeneste (PST) vurderer at teknologiutviklere i petroleumssektoren vil være spesielt utsatt for etterretningsaktivitet.[4] PST opplyser om at det er et jevnt trykk av datanettverksoperasjoner mot statsforvaltningen fra aktører som representerer fremmede stater.[5] Tilsvarende opplyser Nasjonal sikkerhetsmyndighet (NSM) i sine risikovurderinger de siste årene at olje- og energisektoren er særlig utsatt for ulike angrep knyttet til IKT-infrastruktur, og NSM forventer at mengden og omfanget av denne typen angrep vil øke i årene som kommer.[6]

Riksrevisjonen rapporterte i Dokument 1 (2014–2015) om vesentlige svakheter ved informasjonssikkerheten i OD.[7] Revisjonen ble fulgt opp for regnskapsåret 2016[8], og Riksrevisjonen rapporterte i Dokument 1 (2017–2018) at det var sterkt kritikkverdig at OD fortsatt ikke hadde et

---

[2] Oljedirektoratet (2019) *Om OD* <http://www.npd.no/no/Om-OD/Organisasjon>, 27. februar 2019. Oljedirektoratet (2018) *Årsrapport 2017*. Riksrevisjonen (2018) *Referat fra moter med OD om [redacted] og [redacted] 13. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019. Riksrevisjonen (2019) *Referat fra moter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[3] Nasjonal sikkerhetsmyndighet (2017) *Risiko 2017*, s 8. <https://www.nsm.stat.no/aktuelt/risiko-2017/.>
[4] Politiets sikkerhetstjenester (2017) *Trusselvurdering 2017*.
[5] Politiets sikkerhetstjenester (2018) *Trusselvurdering 2018*, 30. januar 2018.
[6] Nasjonal sikkerhetsmyndighet (2015) *Risiko 2015*.
[7] Nasjonalt datalager for lete- og utvinningsrelatert informasjon fra norsk sokkel.
[8] Riksrevisjonen (2017) *Revisjonsrapport for 2016 om styringssystem for informasjonssikkerhet i Oljedirektoratet*, sendt OD 20. april 2017.

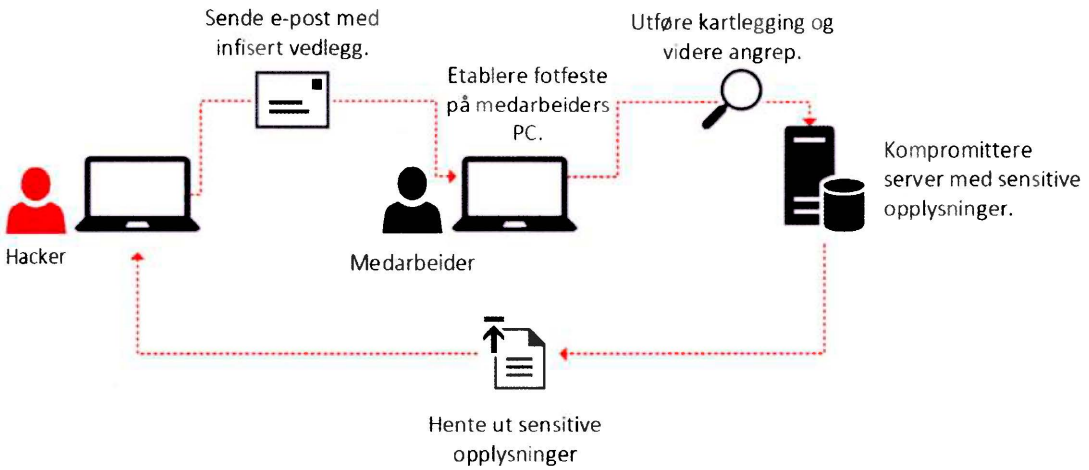
tilfredsstillende styringssystem for informasjonssikkerhet. Kontroll- og konstitusjonskomiteen forutsetter i innstilling 115 S (2017-2018) at departementet umiddelbart iverksetter tiltak for å avhjelpe manglene.

Riksrevisjonen har for 2018 gjennomført en revisjon av sikring mot dataangrep i OD, som omfatter styringssystemet for informasjonssikkerhet og sikkerhetstiltak på utvalgte områder.

Et styringssystem for informasjonssikkerhet skal hjelpe ledelsen og virksomheten for øvrig med å ha tilstrekkelig styring og kontroll med informasjonssikkerheten, gjennom systematisk internkontroll på området. Styringssystemet skal medvirke til at virksomheten velger riktige sikkerhetstiltak og sørger 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 eller manglende sikkerhetstiltak kan indikere at styringssystemet ikke fungerer på alle områder, enten ved at svakhetene ikke er identifisert, eller ved at det ikke er satt i verk korrigerende tiltak. Svakheter i sikringen av informasjon kan føre til at informasjon kommer på avveie og til uheldige konsekvenser for enkeltpersoner og/eller samfunnet. Videre kan det skade omdømmet til offentlige virksomheter.

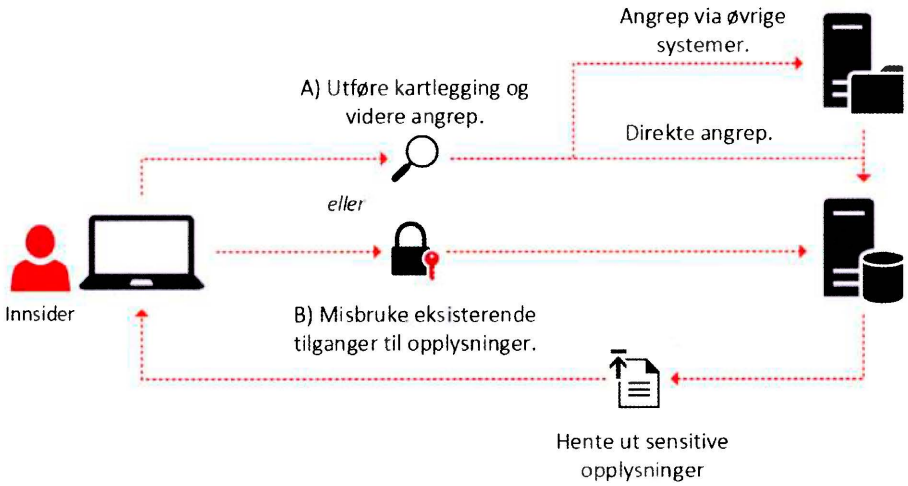
Dataangrep er en samlebetegnelse for målrettede og ikke-målrettede handlinger som rammer informasjonen som behandles i IKT-systemer. Det innebærer forsøk på å ødelegge, endre, eksponere eller stjele informasjon.[9] Angrep mot en virksomhets informasjonsverdier kan komme fra eksterne og fra aktører på innsiden av virksomheten (innsidere).

Figurene nedenfor viser eksempler på hvordan et målrettet angrep fra henholdsvis en ekstern og en intern aktør kan ta form.



Figur 1 Eksempel på dataangrep fra eksterne aktører

[9] Basert på definisjon i ISO/IEC 27000:2017 punkt 2.3.



Figur 2 Eksempel på dataangrep fra intern aktør

3. Revisjonens mål og problemstillinger

Målet med revisjonen er å kontrollere om OD arbeider systematisk med å forhindre dataangrep og oppdage urettmessig tilgang til IKT-systemer.

Revisjonen er gjennomført med utgangspunkt i følgende problemstillinger:

1. Har OD et styringssystem for informasjonssikkerhet som omfatter planlegging av sikring mot dataangrep?

2. Har OD gjennomført systematiske tiltak for å forhindre dataangrep og oppdage urettmessig tilgang til IKT-systemer?

3. Har OD evaluert om styringen og kontrollen for å sikre mot dataangrep har fungert som forutsatt?

Avgrensning
OD opplyser å ha meget få dokumenter som er underlagt *lov om forebyggende sikkerhetstjeneste* (sikkerhetsloven).[10] Sikring av informasjon som er underlagt sikkerhetsloven, er derfor ikke omfattet av revisjonen.

4. Metoder

Problemstillingene er besvart gjennom dokumentanalyser, intervjuer/møter, analytiske handlinger, observasjoner og test av kontroller. I tillegg har revisjonen bedt om utfyllende informasjon fra OD, og OD har gitt skriftlige tilbakemeldinger på revisjonens forespørsler.

Revisjonen gjelder for budsjettåret 2018 og er gjennomført i perioden juni 2018 til mars 2019.

Det er avholdt oppsummeringsmøte med OD 5. mars 2019, hvor formålet var å presentere foreløpige resultater for de enkelte problemstillingene. Resultatet av revisjonen ble videre presentert for Olje- og energidepartementet den 14. mars 2019.

[10] Oljedirektoratet *Behandling av graderte dokumenter og taushetsbelagte opplysninger.*

4.1 Problemstilling 1 – styring av informasjonssikkerhet for å planlegge sikkerhetstiltak

For å besvare problemstilling 1 har revisjonen gjennomført dokumentanalyser og intervjuer/møter.

Dokumentanalyse

I kommunikasjonen med OD har revisjonen bedt om dokumenter som beskriver planleggingen av sikkerhetstiltak. Revisjonen har også hatt tilgang til dokumentasjon som er lagret i ODs styringsverktøy og på ODs intranett (OD-portalen). Revisjonen har gjennomgått den mottatte dokumentasjonen for å kontrollere om OD har utarbeidet og dokumentert krav til informasjonssikkerhetsarbeidet i virksomheten. Dette inkluderer kontroll av om OD har utarbeidet rutiner for og klassifisert informasjonsaktiva og risikovurderinger.

For problemstilling 1 omfatter analysen følgende dokumenter:

- *Strategi for informasjonssikkerhet*, oppdatert 23. august 2018
- overordnet årlig risikovurderinger for 2018 og 2019, som er rapportert til Olje- og energidepartementet
- *IKT-driftsinstruks for Oljedirektoratet*, sist godkjent/oppdatert 28. august 2018
- *Retningslinje – Risikovurdering for informasjonssikkerhet*, oppdatert 21. november 2018
- *Kriterier for å akseptere restrisiko*, 24. mai 2018
- *Momenter til verdivurdering av informasjonsressurser i OD*, notat av 17. januar 2018
- retningslinje og prosedyre for behandling av styrende dokumenter i OD, begge godkjent 2. juli 2018
- *Plan for risikovurderinger 2019*
- verdivurderinger av systemer og arbeidsoppgaver, informasjon lagret i styringsverktøyet
- risikovurderinger av systemer og arbeidsoppgaver, noen rapporter mottatt elektronisk, noen lagret i styringsverktøyet
- samsvarserklæring (SOA), informasjon lagret i styringsverktøyet

Dokumentene er benyttet i dokumentanalysen, og resultatene av analysen er presentert i rapportens kapittel 6.1.

Intervjuer/møter
For å få informasjon om hvordan OD arbeider med de ulike områdene som er omfattet av problemstilling 1, gjennomførte revisjonen intervjuer/møter med sikringskoordinatoren og IKT-sikkerhetsrådgiveren. I tillegg har den operative ledelsen deltatt på enkelte møter.

OD har verifisert referater fra intervjuer/møter 4. september, 27. november og 12. og 13. desember 2018.

4.2 Problemstilling 2 – gjennomføring av sikkerhetstiltak

For å besvare problemstilling 2 har revisjonen gjennomført dokumentanalyser, intervjuer/møter, analytiske handlinger, observasjon og test av kontroller.

Dokumentanalyse
I kommunikasjonen med OD har revisjonen bedt om dokumenter som beskriver hvordan sikkerhetstiltak og sikkerhetstesting gjennomføres. Revisjonen har også hatt tilgang til dokumentasjon som er lagret på ODs intranett (OD-portalen). Revisjonen har gjennomgått den mottatte dokumentasjonen for å forstå hvordan nettverk og systemer i OD er satt opp, og hvilke sikkerhetstiltak som er implementert. I gjennomgangen har revisjonen også kontrollert om OD har utarbeidet rutiner for nettverk, brannmur, servere, klienter, databaser, applikasjoner, logging og overvåking.

For problemstilling 2 omfatter analysen følgende dokumenter:

- *IKT-driftsinstruks for Oljedirektoratet*, sist godkjent/oppdatert 28. august 2018
- *IKT-retningslinjer for riktig bruk av PC, mobil, lagringsmedia og god informasjonssikkerhet*, oppdatert 12. oktober 2018
- avtale mellom OD og [redacted] om overvåking, oppstartstidspunkt 27. april 2016
- systemdokumentasjon for nettverk og brannmur, dokumenter opprettet 13. august 2018

- diverse rutiner og prosedyrer for tilgangsstyring
- oversikt over sikkerhetsteknologier i OD, mottatt 11. september 2018
- diverse rutiner og prosedyrer for informasjonssikkerhetshendelser
- ulike prosedyrer for drift, overvåking, logging, brannmur, nettverksutstyr, databaser, servere og klienter

Dokumentene er benyttet i dokumentanalysen, og resultatene av analysen er presentert i rapportens kapittel 6.2.

Intervjuer/møter
For å få informasjon om hvordan OD arbeider med de ulike områdene som er omfattet av problemstilling 2, har revisjonen hatt møter med ansatte i OD som arbeider med IKT-drift. OD har avtaler med flere eksterne konsulenter om bistand til IKT-drift. Etter vurdering fra OD har eksterne konsulenter deltatt på enkelte møter. I tillegg har den operative ledelsen deltatt på enkelte møter.

OD har verifisert referater fra 18 intervjuer/møter avholdt henholdsvis 4. september, 30. oktober og 12. og 13. desember 2018, og 15. og 16. januar 2019. I tillegg er det i møter om problemstilling 1 og 3 mottatt informasjon som også er relevant for problemstilling 2.

Analytiske handlinger, observasjoner og test av kontroller
Formålet med analytiske handlinger, observasjoner og test av kontroller er å se hvordan ulike systemer og den underliggende IKT-infrastrukturen i OD fungerer. Videre å undersøke om aktuelle sikkerhetstiltak er gjennomført og dokumentert i samsvar med krav i regelverk og anbefalinger i anerkjente standarder.

For å besvare problemstillingen har revisjonen utført analytiske handlinger ved å analysere uttrekk av data fra nettverk, brannmur, klienter og servere om antivirus, sikkerhetsoppdateringer, programmer, brukere, oppsett og innstillinger. Enkelte av kontrollene er gjennomført med systemene [redacted] og [redacted] som utgangspunkt. [redacted] OD opplyser at [redacted] er sentrale systemer som inneholder mye sensitiv informasjon.[11]

Observasjon er benyttet ved at OD har demonstrert sikkerhetsmekanismer ved gjennomgang av tilganger, passord, logging, overvåking og sikkerhetsinnstillinger. Videre har revisjonen testet kontroller for å vurdere om de tekniske sikkerhetsmekanismene for tilgangsstyring, antivirus og overvåking fungerer som forutsatt. Under sikkerhetstesting har revisjonen benyttet egenutviklede skript, verktøyer og kommandoer for å teste ODs kontroller. I forbindelse med test av kontroller har revisjonen forsøk å få uautorisert tilgang til ODs nettverk ved å benytte egen klient fra Riksrevisjonen og en virtuell klient[12] tildelt revisjonen. Revisjonen har gjennom test av kontroller vurdert sikkerhetstiltak i ODs IKT-systemer ved bruk av teknikker som benyttes av for eksempel en hacker. Til forskjell fra revisjonens test av kontroller vil et reelt hackerangrep normalt foregå over lengre tid og det vil bli benyttet flere verktøy og metoder. Dette kan gi andre resultater enn det revisjonen faktisk har vist.

Sikkerhetstesting er utført 16., 25. og 28. januar 2019. Vurdering av sikkerhetstiltak og sikkerhetstesting er gjennomført i perioden oktober 2018 til februar 2019. Resultatene fra vurderingen av sikkerhetstiltak og sikkerhetstesting er verifisert av OD i oversendelse 20. februar 2019.

Resultatene av analytiske handlinger, observasjoner og test av kontroller er presentert i rapportens kapittel 6.2. En detaljert framstilling av revisjonsfunnene oversendes OD i eget brev.

4.3 Problemstilling 3 – oppfølging og evaluering av styringssystem og sikkerhetstiltak

For å besvare problemstilling 3 har revisjonen gjennomført dokumentanalyser, intervjuer/møter og analytiske handlinger.

[11] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[12] En virtuell klient gjør at en bruker fra en hvilken som helst maskin kan logge seg på og få tilgang til programmer og data i virksomhetens nettverk.

Dokumentanalyse
I kommunikasjonen med OD har revisjonen bedt om dokumenter som beskriver hvordan styringssystemet og sikkerhetstiltak følges opp og evalueres. Revisjonen har også hatt tilgang til dokumentasjon som er lagret i ODs styringsverktøy og på ODs intranett (OD-portalen). Revisjonen har gjennomgått den mottatte dokumentasjonen for å kontrollere om OD har ivaretatt krav til oppfølging og evaluering av informasjonssikkerhetsarbeidet.

For problemstilling 3 omfatter analysen følgende dokumenter:

- *Strategi for informasjonssikkerhet*, oppdatert 23. august 2018
- årlige rapporter om sikkerhetstilstanden i 2017 og 2018, som er oversendt til Olje- og energidepartementet
- ROS analyse – informasjonssikkerhet Oljedirektoratet, utarbeidet av PwC, 4. april 2017, og tilhørende handlingsplan
- evaluering av måloppnåelse og Oljedirektoratets dataforvaltning, utarbeidet av A-2 Norge og Menon Economics, 13. september 2018
- dokumentasjon av systemeierens årlige egenkontroller av systemer
- rapporter fra [redacted]-systemet om rapportering av hendelser relatert til informasjonssikkerhet og avvik
- *Prosedyre for å rapportere informasjonssikkerhetshendelser/brudd*, 22. november 2018
- *Prosedyre for håndtering av informasjonssikkerhetshendelser IT-drift*, 7. september 2018
- *Prosedyre for registrering av tiltak etter revisjon*, 29. september 2018
- referater og saksframlegg fra ledermøter i OD
- ekstern gjennomgang av Active Directory av 17. februar 2017 og statusoversikt 28. august 2018

Dokumentene er benyttet i dokumentanalysen, og resultatene av analysen er presentert i rapportens kapittel 6.3.

Intervjuer/møter
For å få informasjon om hvordan OD arbeider med de ulike områdene som er omfattet av problemstilling 3, har revisjonen gjennomført intervjuer/møter med sikringskoordinatoren og IKT-sikkerhetsrådgiveren. I tillegg har den operative ledelsen deltatt på enkelte møter.

OD har verifisert referater fra intervjuer/møter 4. september, 27. november og 12. og 13. desember 2018.

Analytiske handlinger
For å besvare problemstillingen har revisjonen analysert uttrekk av data fra systemet [redacted] som viser informasjonssikkerhetshendelser. [redacted]

5. Revisjonskriterier

Revisjonskriterier er en samlebetegnelse for kriterier som utledes av Stortingets vedtak og forutsetninger, og de er beskrivelser av blant annet gjeldende bevilgningsvedtak, lover, forskrifter, retningslinjer, normer og standarder som er aktuelle for den enkelte etterlevelsesrevisjonen. Kriteriene har betydning for hvilke revisjonsbevis revisjonen innhenter, og de benyttes som grunnlag for revisjonens konklusjoner.

Krav til og anbefalinger om hvordan en virksomhet kan sikre informasjonen i IKT-systemer gjennom et styringssystem og relevante sikkerhetstiltak, framkommer av ulike lover, forskrifter, internasjonale standarder og bransjestandarder.

Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) gjelder for alle forvaltningsorganer. Lovens § 15 a slår fast at et forvaltningsorgan kan benytte elektronisk kommunikasjon når det henvender seg til andre. *Forskrift om elektronisk kommunikasjon med og i forvaltningen* (eForvaltningsforskriften) er fastsatt med hjemmel i forvaltningsloven. Forskriften har som formål å

legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon og for samordning av sikre og hensiktsmessige tekniske løsninger.[13]

Internkontrollen skal baseres på anerkjente standarder, den bør være integrert i virksomhetens helhetlige styringssystem, og den bør ha et omfang og en innretning som er tilpasset risikoen, jf. forskriftens § 15 andre og tredje ledd. Dette samsvarer også med kravene til internkontroll omtalt i *reglement for økonomistyring i staten* § 14 og *bestemmelser om økonomistyring i staten* punkt 2.4. Det framgår at alle virksomheter skal etablere og dokumentere systemer, rutiner og tiltak for behandling og lagring av vesentlig informasjon som sikrer konfidensialitet, integritet og tilgjengelighet. Olje- og energidepartementet har over flere år, senest i tildelingsbrevet til OD for 2018, stilt krav om at direktoratet skal sikre god oppfølging av arbeidet med informasjonssikkerhet og implementere et styringssystem for informasjonssikkerhet.[14]

Nåværende Kommunal- og moderniseringsdepartement fikk fastsatt eForvaltningsforskriften i 2004, og ifølge § 15 andre ledd skal departementet peke ut et organ som skal gi anbefalinger på området. For informasjonssikkerhet er det Direktoratet for forvaltning og ikt (Difi) som er gitt i oppgave å komme med anbefalinger. I *Referansekatalogen for IT-standarder* anbefaler Difi at virksomhetene baserer seg på NS-ISO/IEC ISO 27001:2013 (heretter ISO 27001:2013) når de skal etablere internkontroll/styringssystem på informasjonssikkerhetsområdet.[15]

OD opplyser at informasjonssikkerhetsarbeidet i OD er basert på ISO 27001:2013.[16] NS-ISO/IEC 27001:2017 (heretter ISO 27001) er en ny versjon av ISO 27001:2013, men endringene fra forrige versjon er kun kosmetiske og innfører ingen nye krav/anbefalinger.[17] Ifølge ISO 27001 punkt 6.1.3 skal virksomheten definere og benytte en prosess for å håndtere informasjonssikkerhetsrisikoene. Det vil si å velge tiltak som skal implementeres. Når virksomhetene skal velge og implementere risikoreduserende tiltak, anbefaler Difi at det søkes støtte i anerkjente kilder.[18] Dette kan for eksempel være NS-ISO/IEC 27002:2017 (heretter ISO 27002), som gir anbefalinger om sikringstiltak til virksomheter som implementerer et styringssystem basert på ISO 27001, eller ulike rammeverk og veiledere fra NSM, Difi og Datatilsynet.

Revisjonen legger til grunn at OD ivaretar kravene til internkontroll i eForvaltningsforskriften, *reglementet for økonomistyring i staten* og *bestemmelser om økonomistyring i staten* ved å basere informasjonssikkerhetsarbeidet på ISO 27001 og ISO 27002. For å utdype anbefalingene i ISO-ene har revisjonen i tillegg benyttet veiledere fra NSM og aktuelle bransjestandarder.

5.1 Problemstilling 1 – styring av informasjonssikkerhet for å planlegge sikkerhetstiltak

Ifølge eForvaltningsforskriften § 15 første ledd skal mål og strategier for informasjonssikkerhet i virksomheten være beskrevet, og disse skal danne grunnlaget for virksomhetens internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Grunnleggende styringsprinsipper er også nedfelt i *reglement for økonomistyring i staten* § 4. Reglementets føringer er utledet i *bestemmelser om økonomistyring i staten* punkt 2.2. Ifølge dette regelverket har virksomhetens leder blant annet ansvaret for å etablere internkontroll som skal tilpasses virksomhetens egenart og virksomhetens risiko og vesentlighet.

Revisjonen legger til grunn at for å ivareta internkontroll knyttet til planlegging av sikkerhetstiltak har OD basert informasjonssikkerhetsarbeidet på følgende anbefalinger som utledes nærmere i rapportens kapittel 6:

- ISO 27001:
  - punkt 0.1 Generelt
  - punkt 5.1 Lederskap og forpliktelser
  - punkt 5.2 Policy

[13] eForvaltningsforskriften § 1, første ledd.
[14] Tildelingsbrev fra Olje- og energidepartementet til Oljedirektoratet for 2015, 2016, 2017 og 2018.
[15] Direktoratet for forvaltning og ikt *Internkontroll styringssystem ledelsessystem for informasjonssikkerhet*. <https://www.difi.no/fagomrader-og-tjenester/digitaliseringog-samordning/standarder/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet>.
[16] Oljedirektoratet (2014) *Strategi for informasjonssikkerhet*, oppdatert 23. august 2018.
[17] ISMS.online <https://www.isms.online/iso-27001/iso-27001-2013-iso-27001-2017-whats-the-difference/>.
[18] Direktoratet for forvaltning og ikt *Referansekatalogen*. <https://www.difi.no/fagomrader-og-tjenester/digitaliseringogsamordning/standarder/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet>.

- punkt 6.1.1 Generelt om tiltak for å håndtere risikoer og muligheter
- punkt 6.1.2 Risikovurdering av informasjonssikkerheten

- ISO 27002:
  - punkt 5.1.1 Policyer for informasjonssikkerhet
  - punkt 8.1.1 Oversikt over aktiva
  - punkt 8.1.2 Eierskap til aktiva
  - punkt 8.2.1 Klassifisering av informasjon
  - punkt 18.2.3 Gjennomgang av teknisk samsvar

5.2 Problemstilling 2 – gjennomføring av sikkerhetstiltak

eForvaltningsforskriften, *reglement for økonomistyring i staten* og *bestemmelser om økonomistyring i staten*, ISO 27001 og ISO 27002 gir ikke alltid tilstrekkelige detaljerte krav til og anbefalinger om hvordan tekniske sikkerhetstiltak bør innrettes ved bruk av ulike produkter eller tekniske løsninger. I slike tilfeller har revisjonen i tillegg tatt utgangspunkt i aktuelle bransjestandarder, leverandøranbefalinger og andre veiledere.

NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur) mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene skal være en del av et felles, nasjonalt rammeverk for sikring av IKT-systemer og et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet.

Dersom anbefalte sikkerhetstiltak ikke er implementert, vil det ifølge NSM i de aller fleste tilfeller medføre økt risiko, som må håndteres og vurderes opp mot virksomhetens risikotoleranse.[19] I grunnprinsippene viser NSM til at de fire tiltakene[20] i sjekkliste nr. 1 forhindrer 80–90 prosent av observerte internettangrep, og at NSM ikke har observert internettrelaterte dataangrep som samtidig klarer å omgå alle de ti tiltakene[21] i sjekkliste nr. 2.

Revisjonen legger til grunn at for å sikre informasjonen i ugraderte systemer har OD ved implementering av tekniske sikkerhetstiltak basert informasjonssikkerhetsarbeidet på følgende anbefalinger som utledes nærmere i rapportens kapittel 6:

- ISO 27002:
  - kapittel 5 Informasjonssikkerhetspolicy
  - punkt 9.1.1 Aksesskontrollpolicy
  - punkt 9.2.1 Registrering og sletting av brukere
  - punkt 9.2.2 Forvaltning av brukeraksess
  - punkt 9.2.3 Styring av privilegerte aksessrettigheter
  - punkt 9.4.3 Styringssystem for passord
  - punkt 10.1.1 Policy for bruk av kryptografiske kontroller
  - punkt 12.1.1 Dokumenterte driftsprosedyrer
  - punkt 12.2 Beskyttelse mot ødeleggende programvare
  - punkt 12.4 Logging og overvåking
  - punkt 13.1.1 Nettverkskontroller
  - punkt 13.1.3 Segregering i nettverk
  - punkt 14.1.1 Behovsanalyse og beskrivelse av krav til informasjonssikkerhet

- NSMs grunnprinsipper for IKT-sikkerhet:
  - punkt 2.3 Ivareta en sikker konfigurasjon (av maskin- og programvare)
  - punkt 2.4 Ha kontroll på IKT-infrastruktur
  - punkt 2.5 Ha kontroll på kontoer

[19] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for ikt-sikkerhet*, versjon 1.1.
[20] De fire tiltakene: oppgradere program- og maskinvare, installere sikkerhetsoppdateringer så fort som mulig, ikke tildele administratorrettigheter til sluttbrukere, blokkere kjøring av ikke-autoriserte programmer, jf. Nasjonal sikkerhetsmyndighet (2016) Sjekkliste nr 1 (S-01) *Fire effektive tiltak mot dataangrep*, 3. mars 2016.
[21] De 10 tiltakene: de fire tiltakene i sjekkliste nr 1 i tillegg til aktiver kodebeskyttelse mot ukjente sårbarheter, herde applikasjoner, bruk klientbrannmur, bruk sikker oppstart og diskkryptering, bruk antivirus/antiskadevare, ikke installer mer funksjonalitet enn nødvendig, jf. Nasjonal sikkerhetsmyndighet (2016) Sjekkliste nr 2 (S-02) *Ti viktige tiltak mot dataangrep*, 3. mars 2016.

- punkt 2.6 Kontroller bruk av administrative privilegier
- punkt 2.7 Kontroller dataflyt
- punkt 2.8 Beskytt data i ro og i transitt
- punkt 2.9 Beskytt e-post og nettleser
- punkt 3.2 Beskytt mot skadevare
- punkt 3.5 Overvåk og analyser IKT-systemet

- NSM: sjekkliste nr. 1 *Fire effektive tiltak mot dataangrep* og sjekkliste nr. 2 *Ti viktige tiltak mot dataangrep*

- Aktuelle bransjestandarder:
  - Password Policy, fra Microsoft, av 19. mars 2017
  - Recommendations and Guidelines on Configuring the Authentication Mode for SQL Server, fra Microsoft, oppdatert 2. april 2012
  - Best Practices for Securing Active Directory, Appendix D: Securing Built-In Administrator Accounts in Active Directory, fra Microsoft, av 31. mai 2017
  - Best Practices for Securing Active Directory, Attractive Accounts for Credential Theft, fra Microsoft, av 31. mai 2017

5.3 Problemstilling 3 – oppfølging og evaluering av styringssystem og sikkerhetstiltak

Alle virksomheter skal ifølge *reglement for økonomistyring i staten* § 14 etablere systemer og rutiner som har innebygd internkontroll, for å sikre mål og resultater og at eventuelle vesentlige avvik forebygges, avdekkes og korrigeres i nødvendig utstrekning. Ifølge Difis veiledningsmateriell om internkontroll i praksis bør virksomheter systematisk vurdere om sikkerhetstiltak fungerer, om regelverk etterleves, og om internkontrollarbeidet i virksomheten blir gjennomført som forutsatt.[22]

Virksomheter skal ifølge *reglement for økonomistyring i staten* § 16 sørge for at det gjennomføres evalueringer for å få informasjon om blant annet aktiviteter og resultater innenfor hele eller deler av virksomhetenes ansvarsområde. Ifølge bestemmelser om økonomistyring i staten punkt 2.6 skal frekvensen og omfanget av evalueringen bestemmes ut fra virksomhetens egenart, risiko og vesentlighet. Evalueringer kan utføres av interne eller eksterne fagmiljøer.

Gjennom blant annet målinger, evalueringer og revisjoner kan ledere på alle nivåer få bedre kunnskap om tilstanden på sitt ansvarsområde.[23] Hensikten med målinger er å teste om tiltak fungerer, og om pålegg blir etterlevd. [24] Målinger må gjennomføres både når tiltak etableres, og når de brukes.

Revisjonen legger til grunn at ODs informasjonssikkerhetsarbeid er basert på følgende anbefalinger, som utledes nærmere i rapportens kapittel 6:

- ISO 27001:
  - punkt 9.1 Overvåking, måling, analyse og evaluering
  - punkt 9.2 Intern revisjon
  - punkt 9.3 Ledelsens gjennomgang
  - kapittel 10 Forbedring

- ISO 27002:
  - punkt 16.1.1 Ansvar og prosedyrer
  - punkt 16.1.4 Behandling av informasjonssikkerhetshendelser
  - punkt 18.2.1 Uavhengig gjennomgang av informasjonssikkerhet
  - punkt 18.2.2 Samsvar med policyer og standarder for sikkerhet
  - punkt 18.2.3 Gjennomgang av teknisk samsvar

[22] Direktoratet for forvaltning og ikt *Internkontroll – informasjonssikkerhet: Måling, evaluering og revisjon.* <http://internkontroll.infosikkerhet.difi.no/systematiskeaktiviteter/maling-evaluering-og-revisjon>.
[23] Direktoratet for forvaltning og ikt *Internkontroll – informasjonssikkerhet: Måling, evaluering og revisjon.* <http://internkontroll.infosikkerhet.difi.no/systematiskeaktiviteter/malingevaluering-og-revisjon>.
[24] Direktoratet for forvaltning og ikt *Internkontroll – informasjonssikkerhet: Systematiske aktiviteter.* <http://internkontroll.infosikkerhet.difi.no/systematiske-aktiviteter/>.

6. Funn

Nedenfor presenteres utledningen av revisjonskriterier og funn for hver av de tre problemstillingene revisjonen dekker. Det er i tillegg utarbeidet et eget dokument som gir en mer detaljert framstilling av revisjonsfunnene i rapportens kapittel 6.2. Dokumentet er unntatt offentlighet fordi kunnskap om innholdet vil kunne gjøre det lettere å gjennomføre straffbare handlinger, jf. offentlighetsloven § 24 tredje ledd.

6.1 Problemstilling 1 – styring av informasjonssikkerhet for å planlegge sikkerhetstiltak

Problemstilling 1 omfatter ODs styring av informasjonssikkerhet for å planlegge sikkerhetstiltak. I dette inngår sikkerhetsmål og -strategier, som skal danne grunnlag for virksomhetens internkontroll, og aktivitetene verdivurdering og risikovurdering, som skal sikre at virksomheten planlegger og iverksetter sikkerhetstiltak for å beskytte informasjon på en god måte.

Områdene som er revidert for å besvare problemstilling 1, presenteres nedenfor, og disse er valgt på bakgrunn av ODs egne krav til styring av informasjonssikkerhet og beste praksis.

6.1.1 Overordnet rammeverk for styring av informasjonssikkerhet

Et styringssystem for informasjonssikkerhet skal bidra til å bevare konfidensialiteten, integriteten og tilgjengeligheten til informasjon ved å benytte en risikostyringsprosess, forhindre eller redusere uønskede virkninger og oppnå kontinuerlig forbedring jf. ISO 27001 punktene 0.1 og 6.1.1. Videre fremgår det av ISO 27001 punkt 5.2 og ISO 27002 punkt 5.1.1 at virksomhetens ledelse bør utarbeide en policy som definerer formål med og ansvar for styring av informasjonssikkerhet, og prinsipper for vesentlige aktiviteter.

Dokumentanalyse viser at OD har utarbeidet flere styrende dokumenter for informasjonssikkerhet. *Strategi for informasjonssikkerhet* er hoveddokumentet i ODs styringssystem. [25] Strategien definerer rammer for arbeidet med informasjonssikkerhet, herunder mål, viktige prinsipper, ansvar og roller, avviksrapportering og -håndtering, og oppfølging og evaluering.

OD har i strategien definert at målet for informasjonssikkerhetsarbeidet er å hindre at sensitiv informasjon bevisst eller ubevisst gjøres tilgjengelig for uvedkommende. Videre framgår det at informasjonssikkerheten i OD skal omfatte tiltak som bidrar til å verne om verdier og informasjon og til å gjøre OD i stand til å løse prioriterte oppgaver. Dette skal skje ved at tiltakene sikrer

- at kun medarbeidere med autorisert tilgang kan benytte informasjonssystemene (konfidensialitet)
- at informasjonen til enhver tid er et resultat av rettmessige registreringer og kontrollerte aktiviteter (integritet)
- at medarbeidere har korrekt tilgang til tjenester og informasjon til rett tid og på riktig sted, og at eksterne brukere har korrekt tilgang til aktuelle systemer (tilgjengelighet)

OD opplyser at direktoratet så langt som mulig vil følge anbefalingene i ISO-en.[26] For å vise hvilke aktiviteter, roller, dokumenter og prosesser som vil ivareta de ulike punktene i ISO 27002, har OD utarbeidet oversikten Statement of Applicability (SOA).

OD har i de senere årene ansatt flere personer for å arbeide med styringssystemet for informasjonssikkerhet, blant annet en sikringskoordinator og en IKT-sikkerhetsrådgiver. OD opplyser at den strategiske og den operative ledelsen er involvert i arbeidet og jevnlig deltar i møter.[27] Ansvar og roller for informasjonssikkerhet er i strategien definert på følgende måte:

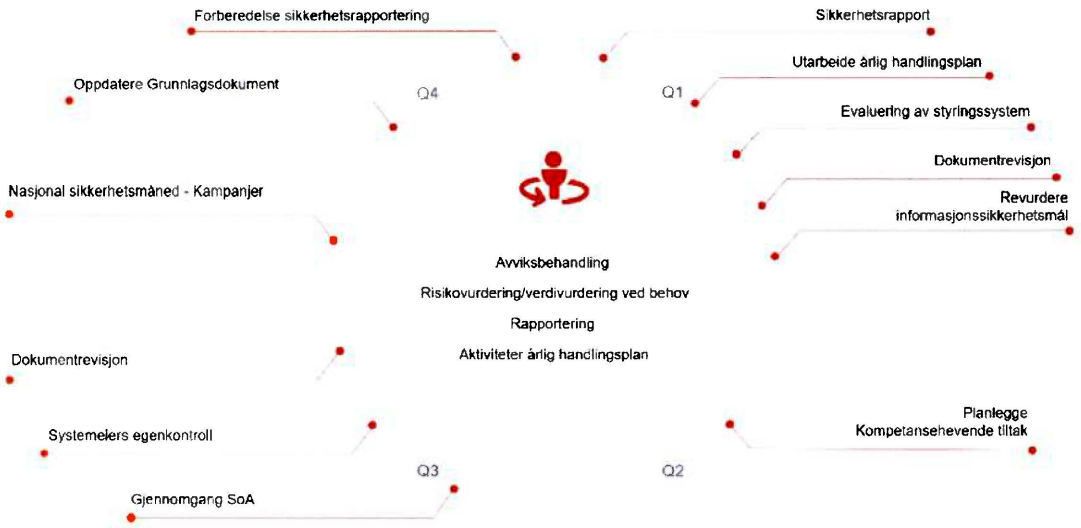
- Oljedirektøren godkjenner strategi for informasjonssikkerhet i OD.
- En av ODs operative ledere har ansvar for at ODs styringssystem er basert på anerkjent standard.
- Alle lederne i OD skal arbeide for kontinuerlig forbedring av informasjonssikkerheten innenfor sine resultatområder og for at det enkelte IKT-system har en eier med nødvendig kompetanse.

[25] Oljedirektoratet (2014) *Strategi for informasjonssikkerhet*, oppdatert 23. august 2018.
[26] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[27] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.

- IKT-systemeier er ansvarlig for at informasjonssystemet har tilfredsstillende funksjonalitet, sikkerhet og kvalitet.
- Sikringskoordinator er ansvarlig for å oppdatere og videreutvikle ODs strategi og regelverk for informasjonssikkerhet, og for holdningsskapende aktiviteter i OD.
- Den enkelte medarbeider i OD skal følge lover, regelverk og interne retningslinjer som regulerer informasjonssikkerheten i OD.

Hvem som har myndighet ved utarbeidelse og vedlikehold av interne dokumenter, og hvordan disse skal gjøres tilgjengelige, er beskrevet i *Retningslinje for behandling av styrende dokumenter i OD*. [28] OD opplyser at de styrende dokumentene to ganger i året oversendes dokumenteieren for gjennomgang og eventuelt revidering.[29] Dokumentanalyse viser at OD følger egen rutine for å utarbeide og oppdatere styrende dokumenter.

OD har definert et årshjul som viser aktiviteter i styringssystemet for informasjonssikkerhet og når det er planlagt at disse skal gjennomføres, jf. Figur 3. Årshjulet viser at OD i løpet av et år skal gjennomføre sentrale aktiviteter, blant annet verdi- og risikovurdering, hendelseshåndtering, oppfølging, evalueringer og dokumentrevisjoner. Aktivitetene er definert i egne retningslinjer, prosedyrer og rutiner for informasjonssikkerhet som omtales senere i rapporten.



Figur 3 Årshjul. Kilde: [redacted]

Styringssystemet for informasjonssikkerhet blir driftet i styringsverktøyet [redacted], som ble tatt i bruk i desember 2017.[30] På revisjonstidspunktet var det bare tre personer ([redacted]) som hadde tilgang til styringsverktøyet.[31] Styringsverktøyet skal etter planen være ferdig konfigurert, testet og tilgjengelig for alle systemeierne i 2019/2020.

Oppsummert viser revisjonen at OD følger anbefalinger på området ved at OD har etablert et rammeverk for styring av informasjonssikkerhet. Samlet definerer rammeverket mål, ansvar, roller, sentrale aktiviteter og prinsipper i informasjonssikkerhetsarbeidet.

6.1.2 Identifisering av informasjonsaktiva[32]

[28] Oljedirektoratet (2018) *Retningslinje for behandling av styrende dokumenter i OD*, 2. juli 2018.
[29] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019. Oljedirektoratet (2018) *Prosedyre for behandling av styrende dokumenter i OD*, 2. juli 2018.
[30] Oljedirektoratet (2014) *Strategi for informasjonssikkerhet*, oppdatert 23. august 2018.
[31] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[32] Med informasjonsaktiva menes datasystemer med tilhørende data, og infrastruktur til behandling, transport og lagring av data.

Av ISO 27002 punkt 8.1.1 framgår det at virksomheten bør identifisere informasjon og andre aktiva knyttet til informasjon og systemer for informasjonsbehandling, og at den bør utarbeide og vedlikeholde en oversikt over disse aktivaene. Aktiva som vedlikeholdes i oversikten, bør underlegges eierskap, jf. ISO 27002 punkt 8.1.2.

For å sikre at informasjonen er godt nok beskyttet, må virksomheten ha oversikt over hvilken informasjon som forvaltes, og hvor informasjon oppbevares og behandles. OD har gjennomført en intern kartlegging for å få oversikt over systemer og arbeidsoppgaver. OD opplyser at det kontinuerlig oppdateres oversikter over aktiva etter hvert som systemer fases ut eller implementeres.[33] Dokumentanalysen viser at sentrale systemer ser ut til å være identifisert, og at systemene i oversikten er tildelt en eier. OD opplyser imidlertid at det pågår en prosess for å gjennomgå alle roller, for å tydeliggjøre blant annet hva rollen som systemeier innebærer.[34]

Oppsummert viser revisjonen at OD har utarbeidet oversikt over aktiva slik som anbefalt, og at identifiserte systemer er tildelt systemeier.

6.1.3 Verdivurdering av informasjonsaktiva

Virksomheten skal etablere og dokumentere internkontroll slik at den kan forvalte virksomhetens verdier på en forsvarlig måte, jf. *bestemmelser om økonomistyring i staten* punkt 2.4. ISO 27002 punkt 8.2.1 anbefaler at virksomheten etablerer en metode for verdivurdering for å sikre felles forståelse av krav til beskyttelse. Det framgår videre at verdivurderingen bør oppdateres ved endringer i aktivaene.

For å sikre innholdet i systemet skal OD verdivurdere alle IKT-systemer, jf. *IKT-driftsinstruks for Oljedirektoratet*. Ved store endringer skal det utarbeides ny verdivurdering.[35] Ifølge ODs *Retningslinje - Risikovurdering for informasjonssikkerhet* skal utgangspunktet for verdivurderingen være innholdet i systemet eller arbeidsoppgaven.[36] OD opplyser at systemer og arbeidsoppgaver blir verdivurdert med utgangspunkt i Difis veiledningsmateriell *Internkontroll i praksis - informasjonssikkerhet - typiske arbeidsoppgaver og tilhørende informasjonstyper*.[37] OD opplyser videre å ha tilpasset modellen fra Difi, for å dekke egne behov.

Figur 4 viser kategorier og nivåskalaen som OD benytter ved verdivurdering av systemer og arbeidsoppgaver. Hver av kategoriene *sensitivitetsgrad innhold*, *sensitivitetsgrad output*, *konfidensialitet*, *integritet* og *tilgjengelighet* gis en verdi i henhold til skalaen som er definert per kategori. I verdivurderingen summeres verdien av de fem kategoriene til en totalverdi, som merkes rødt dersom den er i intervallet 13–16, gult dersom den er i intervallet 9–12, og grønt dersom den er i intervallet 5–8.[38]

SENSITIVITETSGRAD INNHOLD	SENSITIVITETSGRAD OUTPUT	KONFIDENSIALITET	INTEGRITET	TILGJENGELIGHET
1. Offentlig info	1. NEI	1. LAV	1. LAV	1. LAV
2. Intern ikke sensitiv	2. JA	2. MIDDELS	2. MIDDELS	2. MIDDELS
3. Intern sensitiv		3. HØY	3. HØY	3. HØY
4. Personsopplysninger				
5. Børs og forretningssensitiv				

Figur 4 Verdivurdering – kategorier og skala per kategori. Kilde: [redacted]

Figur 5 viser et eksempel av verdivurderingen av [redacted] Verdivurderingen av [redacted] framgår av styringsverktøyet, og kategoriene sensitivitetsgrad innhold, sensitivitetsgrad output, konfidensialitet, integritet og tilgjengelighet er vurdert til henholdsvis 5, 2, 3, 3 og 3. Dette gir en totalverdi for verdivurderingen på 16, og det medfører rød status.

---

[33] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019. Oljedirektoratet (2019) *Svar fra OD etter oppsummeringsmøte 5. mars 2019*, 11. mars 2019.
[34] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[35] Oljedirektoratet (2018) *IKT-driftsinstruks*, oppdatert 28. august 2018, punkt 3.2.
[36] Oljedirektoratet (2018) *Retningslinje - Risikovurdering for informasjonssikkerhet*, oppdatert 21. november 2018, side 3.
[37] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[38] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019 og [redacted].
[39] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.

Navn	Innhold	Sensitivt output	Konfidensialitet	Integritet	Tilgjengelighet	Verdivurdering	Status
[redacted]	5	2	3	3	3	16	

Figur 5 Verdivurdering av [redacted]. Kilde: [redacted]

Gjennomførte verdivurderinger

OD opplyser at sikringskoordinatoren og IKT-sikkerhetsrådgiveren i samtale med systemeieren har utarbeidet verdivurderinger etter metoden, og at alle aktuelle systemer er verdivurdert. [40] Dokumentanalyse viser at OD på revisjonstidspunktet har verdivurdert 76 systemer og 24 arbeidsoppgaver. OD opplyser videre at verdivurderingene vil bli gjennomgått på nytt i 2019 for å sikre at eventuelle avhengigheter mellom arbeidsoppgaver, systemer og underliggende infrastruktur blir hensyntatt.

Siden systemeierne ikke har tilgang til styringsverktøyet, har [redacted] og [redacted] lagt inn resultatene fra verdivurderingen i verktøyet. OD opplyser at all dokumentasjon om verdivurderinger av aktiva ligger i styringsverktøyet.[41]

I styringsverktøyet er det mulig å legge inn kommentarer til den enkelte verdivurdering. Dokumentanalyse viser imidlertid at 99 av de 100 gjennomførte verdivurderingene ikke har kommentarer som viser hvorfor de ulike kategoriene er vurdert til gitt verdi. For kategoriene konfidensialitet, integritet og tilgjengelighet har OD spesifisert når verdiene høy, middels og lav skal benyttes. Av styringsverktøyet går det for eksempel fram at konfidensialitet skal vurderes til høy dersom informasjonen er sensitiv (personsensitiv, børs- og forretningssensitiv). Den skal vurderes som middels dersom deler av informasjonen er tilgjengelig eller tilgjengelig internt for de personene som trenger den. Videre skal den vurderes som lav dersom informasjonen er tilgjengelig for alle. Dokumentanalyse viser imidlertid at dette er generelle spesifikasjoner som ikke dokumenterer de spesifikke vurderingene knyttet til det enkelte systemet eller den enkelte arbeidsoppgaven som er verdivurdert. Når vurderingen av valgt verdi for de ulike kategoriene ikke er dokumentert, kan det være vanskelig å forstå bakgrunnen for vurderingene. Dette kan gjøre det utfordrende å vurdere om det er behov for å oppdatere verdivurderingen, og det kan gjøre det utfordrende for andre, for eksempel nytt personell eller ledelsen, å forstå bakgrunnen for verdivurderingen.

Dokumentanalyse viser videre at ODs modell for verdivurdering vekter konfidensialitet høyere enn integritet og tilgjengelighet. Bakgrunnen er at konfidensialitet vurderes i de tre kategoriene sensitivitetsgrad innhold, sensitivitetsgrad output og konfidensialitet, mens integritet og tilgjengelighet kun vurderes i én kategori hver. Systemer eller arbeidsoppgaver som gis høy verdi på konfidensialitet, vil dermed få en høy verdi i tre kategorier, noe som medfører en høy totalverdi. Ifølge OD er det imidlertid også viktig at data og opplysninger er tilgjengelige til enhver tid og ikke er utsatt for manipulasjon. OD vurderer at inngripen i tilgjengelighet og integritet har et minst like stort skadepotensial som brudd på konfidensialitet.[42] Til tross for dette viser dokumentanalyse at flere systemer[43] med høy verdi på integritet og tilgjengelighet kun oppnår totalvurderingen moderat viktighet (gult). Dette som følge av at systemene ikke er vurdert til å inneholde informasjon som må beskyttes (konfidensialitet), slik at de får lav verdi i kategoriene sensitivitetsgrad innhold, sensitivitetsgrad output og konfidensialitet.

I forbindelse med revisjonen opplyser OD at beregningsmodellen for verdivurdering vil bli evaluert i den årlige gjennomgangen av styringssystemet, metode og rammeverk for 2019.[44]

Oppsummert viser revisjonen at OD følger anbefalinger på området ved at verdivurderinger av 76 systemer og 24 arbeidsoppgaver er gjennomført. Revisjonen viser imidlertid at det er svakheter i metoden som benyttes, ved at begrunnelsen for tildelt verdi ikke er dokumentert. Videre er det en svakhet at konfidensialitet blir høyere vektet enn integritet og tilgjengelighet, og dette selv om OD har vurdert at de to sistnevnte er minst like vesentlig som konfidensialitet.

---

[40] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[41] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[42] Oljedirektoratet (2018) *Momenter til verdivurdering av informasjonsressurser i OD*, notat av 17. januar 2018.
[43] Systemene [redacted], [redacted] og [redacted].
[44] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.

OED har merket seg revisjonens merknader knyttet til verdivurderinger, og vil inkludere disse i det videre oppfølgingsarbeidet med OD. Departementet vil videre følge opp at OD gjennomfører en evaluering av modellen i løpet av 2019.[45]

6.1.4 Risikovurdering av systemer og arbeidsoppgaver

ISO 27001 punkt 6.1.2 anbefaler at virksomheten etablerer en prosess for risikovurderinger på informasjonssikkerhetsområdet, og at risikovurderinger utføres med planlagte intervaller eller ved betydelige endringer.

OD har i *Retningslinje – Risikovurdering for informasjonssikkerhet* beskrevet en metode for hvordan ansatte med behandlingsansvar i OD skal oppdatere eller utføre nye risikovurderinger på operativt nivå.[46] Metodikken for risikovurdering er implementert i styringsverktøyet og bygger på Difis veiledningsmateriell *Internkontroll i praksis – informasjonssikkerhet*, som blant annet er basert på ISO 27001. OD har i tillegg utarbeidet *Kriterier for å akseptere restrisiko*, som skal brukes av ledelsen for å vurdere om restrisiko kan aksepteres med de tiltakene som er iverksatt.[47]

OD opplyser at verdivurderingen av systemer og arbeidsoppgaver avgjør om det skal utarbeides risikovurdering.[48] Høy verdivurdering (rød) medfører at det skal utarbeides risikovurdering. Moderat verdivurdering (gul) tilsier at behovet for risikovurdering skal vurderes. I slike tilfeller vil OD blant annet ta hensyn til hvordan de ulike kategoriene (innhold, output, konfidensialitet, integritet og tilgjengelighet) er vurdert. Ved lav verdivurdering (grønn) vurderer OD at det ikke er behov for risikovurdering. Som en følge av ODs metode for verdivurdering vil systemer og arbeidsoppgaver som er kritiske med hensyn til integritet og tilgjengelighet, og som vurderes til lav på konfidensialitet, maksimalt få totalverdi 9 (gul). Metoden setter dermed ikke krav til at risikovurdering skal utarbeides for systemer og arbeidsoppgaver som er kritisk med hensyn til integritet og konfidensialitet.

Sikringskoordinatoren og IKT-sikkerhetsrådgiveren i OD er prosessledere i arbeidet med risikovurdering. Øvrige deltakere i arbeidet velges med utgangspunkt i deres kunnskap om og erfaring med det som skal risikovurderes. OD opplyser å ha utarbeidet en risikofaktorliste som brukes som utgangspunkt i arbeidet med risikovurdering.[49] For hver risikofaktor vurderes sannsynlighet og konsekvens på en skala fra 1 til 3. Resultatet av sannsynlighets- og konsekvensvurderingen avgjør fargekoden for det enkelte risikomomentet. Skalaen for risikovurdering er bestemt av OD, og inndelingen er slik at risikomomentet merkes med rød dersom resultatet av vurderingen er i intervallet 6–9, med gul dersom det er i intervallet 3–5, og med grønn dersom det er i intervallet 1–2.[50]

Gjennomførte risikovurderinger

OD har verdivurdert [redacted] systemer og [redacted] arbeidsoppgaver, og av styringsverktøyet går det fram at [redacted], [redacted] og [redacted] av disse er vurdert til henholdsvis rødt, gult og grønt.

Dokumentanalyse viser at OD på revisjonstidspunktet kun har risikovurdert [redacted] systemer (7%) som har blitt verdivurdert til rødt, og at ingen arbeidsoppgaver er risikovurdert. OD opplyser at risikovurdering av ytterligere ett system er gjennomført, men at denne mangler godkjenning fra ledelsen da nye planer kan medføre endringer i systemet.[51] OD har i 2015 og 2017 i tillegg gjennomført sikkerhetstester av henholdsvis to systemer og ett system. Sikkerhetstester gir god oversikt over risikobildet for det enkelte systemet, men disse kan ifølge ISO 27002 punkt 18.2.3 ikke erstatte risikovurdering.

Dokumentanalyser og intervjuer viser videre at det ikke foreligger risikovurderinger av blant annet [redacted] og [redacted], eller [redacted] og [redacted], selv om disse har høy verdivurdering og er merket rødt.[52] Ifølge *Plan for risikovurdering 2019* skal OD i løpet av 2019 risikovurdere 21 systemer,

---

[45] Olje- og energidepartementet, brev av 11. april 2019 til Riksrevisjonen.
[46] Oljedirektoratet (2018) *Retningslinje - Risikovurdering for informasjonssikkerhet*, oppdatert 21. november 2018.
[47] Oljedirektoratet (2018) *Kriterier for å akseptere restrisiko*, 24. mai 2018.
[48] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[49] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[50] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
Oljedirektoratet (2018) *Retningslinje - Risikovurdering for informasjonssikkerhet*, oppdatert 21. november 2018.
[51] Oljedirektoratet (2019) *Plan for risikovurderinger 2019*.
[52] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.

prosjekter og oppgaver.[53] OD opplyser at risikovurdering av [redacted] og [redacted] er påbegynt per 18. februar 2019.[54]

Oppsummert viser revisjonen at OD følger anbefalinger på området om å utarbeide en prosess for risikovurderinger på informasjonssikkerhetsområdet, men risikovurderinger er i liten grad gjennomført.

OED opplyser i sine merknader til rapportutkast at OD har gjennomført risikovurderinger parallelt med revisjonen og at OD følger oppsatt plan for gjennomføring av risikovurderinger. Ved utgangen av 2019 forventer OD å ha risikovurdert alle de kritiske systemene. Departementet vil fremover følge opp at OD følger oppsatt plan for å utføre risikovurderinger.[55]

6.1.5 Overordnet risikovurdering

I ISO 27001 punkt 5.1 anbefales det at ledelsen sikrer at kravene i ledelsessystemet for informasjonssikkerhet integreres i virksomhetens øvrige styringsprosesser.

OD skal hvert år oversende overordnet risiko- og vesentlighetsvurdering til Olje- og energidepartementet.[56] Risikovurderingen skal relateres til mål- og resultatkravene og er dermed en integrert del av styringen. Departementet har for 2018 satt krav til at OD skal arbeide særskilt med informasjonssikkerhet, blant annet sikre god oppfølging og implementering av direktoratets styringssystem.[57]

Overordnet risikovurdering inneholder en vurdering av områder og hendelser som kan ha negativ innvirkning på ODs måloppnåelse.[58] Vurderingene i overordnet risikovurdering for 2018 og 2019 er gjort med utgangspunkt i arbeidet med å implementere styringssystem for informasjonssikkerhet. Risikovurderingen for 2019 er i tillegg basert på en ekstern evaluering[59], som har konkludert med at ODs arbeid på området er i samsvar med eForvaltningsforskriften § 15.

OD har i overordnede risikovurderinger for 2018 og 2019 vurdert risikoen knyttet til arbeidet med informasjonssikkerhet til lav. [60] Av de overordnede risikovurderingene går det videre fram at PST anser risikoen for etterretningsvirksomhet rettet mot norske interesser som høy. Grunnet robuste tiltak som [redacted] vurderer imidlertid OD risikoen som moderat til lav i 2018. For 2019 vurderer OD risikoen som moderat grunnet robuste tiltak.[62]

Oppsummert viser revisjonen at ODs vurdering av informasjonssikkerheten i overordnet risikovurdering ikke er basert på dokumenterte risikovurderinger av systemer og arbeidsoppgaver.

Departementet understreker at hensikten med overordnet risikovurdering er å identifisere hendelser eller forhold som kan ha innvirkning på måloppnåelsen til OD. Overordnede risikovurderinger følges opp årlig i styringsdialogen, og departementet vil gjennom styringsdialogen i 2019 ha et særskilt fokus på rapportering av risiko knyttet til ODs delmål som omfatter informasjonssikkerhet. [63]

6.2 Problemstilling 2 – gjennomføring av sikkerhetstiltak

Problemstilling 2 omfatter et utvalg sikkerhetstiltak som skal beskytte informasjon mot dataangrep og oppdage urettmessig tilgang eller forsøk på slik tilgang til IKT-systemene. Dersom det er svakheter i sikkerhetstiltakene, kan uvedkommende forsøke å utnytte disse for å få urettmessig tilgang til

[53] Oljedirektoratet (2019) *Plan for risikovurderinger 2019*.
[54] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[55] Olje- og energidepartementet, brev av 11. april 2019 til Riksrevisjonen.
[56] Olje- og energidepartementet (2014) *Instruks økonomi- og virksomhetsstyring i Oljedirektoratet*, 2. januar 2014.
[57] Olje- og energidepartementet (2018) *Tildelingsbrev 2018*.
[58] Oljedirektoratet (2017) *Overordnet risikovurdering for 2018*. Oljedirektoratet (2018) *Overordnet risikovurdering for 2019*.
[59] A-2 Norge AS og Menon Economics (2018) *Evaluering av måloppnåelse og Oljedirektoratets dataforvaltning*, sluttrapport av 13. september 2018.
[60] Oljedirektoratet (2017) *Overordnet risikovurdering for 2018*. Oljedirektoratet (2018) *Overordnet risikovurdering for 2019*. Oljedirektoratet (2019) Overordnede risikovurderinger, e-post til Riksrevisjonen 17. januar 2019.
[61] Med perimeterskring menes sikkerhetstiltak iverksatt for å beskytte virksomhetens nettverk mot Internett.
[62] Oljedirektoratet (2017) *Overordnet risikovurdering for 2018*.
[63] Olje- og energidepartementet, brev av 11. april 2019 til Riksrevisjonen.

systemer og informasjon. Det er derfor viktig at virksomhetene etablerer kontroller for å oppdage forsøk på dataangrep.

De sikkerhetstiltakene som er revidert, presenteres nedenfor, og de er valgt på bakgrunn av NSMs anbefaling om hvilke tiltak en virksomhet bør vurdere for å sikre sine systemer og informasjon. Dette omfatter tiltak for å hindre at en angriper får tilgang til nettverket uten å bli oppdaget. I tillegg må virksomheten iverksette tiltak for å forhindre at en angriper eller en innsider som har tilgang i nettverket, får uautorisert tilgang til ytterligere systemer. Etter revisjonen har OD opplyst at flere av de påviste forholdene er eller vil bli korrigert. Det har imidlertid ikke vært en del av revisjonen å følge opp disse korrigeringene.

Detaljert beskrivelse av funn påvist i revisjonen av sikkerhetstiltakene er blitt oversendt OD med kopi til Olje- og energidepartementet. Departementet opplyser at det er innhentet status fra OD om gjennomføringen av sikkerhetstiltak. OD har i parallell med og i etterkant av revisjonen iverksatt en rekke tiltak og forbedringer. Målet med tiltakene er blant annet å sikre at sikkerhetstiltakene tydeligere baserer seg på de gjennomførte risikovurderingene og departementet vil følge opp dette. [64]

Videre tilføyer departementet at OD og departementet har prioritert økte ressurser til arbeidet med å erstatte dagens systemer med moderne og mer effektive systemer. De nye systemene skal følge pålegg som er stilt i Digitaliseringsrundskrivet, og andre relevante krav til offentlige IKT-systemer og forhold som gjelder informasjonssikkerhet. [65]

6.2.1 Krav, policy, prosedyrer og rutiner for teknisk infrastruktur

For at informasjonssikkerhet skal være en integrert del av informasjonssystemer gjennom hele livsløpet, bør krav til informasjonssikkerhet innlemmes i kravene til nye informasjonssystemer eller ved forbedring av eksisterende informasjonssystemer, jf. ISO 27002 punkt 14.1.1. Krav til informasjonssikkerhet som gjenspeiler verdi og risiko bør identifiseres og dokumenteres.

Ifølge ODs SOA skal applikasjonsbeskrivelser, krav til leverandører og prosjektveiviseren ivareta anbefalingene i ISO 27002 punkt 14.1.1 om behovsanalyse og beskrivelse av krav til informasjonssikkerhet.[66] OD har utarbeidet en mal for applikasjonsbeskrivelser[67] og opplyser at det vil bli utarbeidet applikasjonsbeskrivelser for alle nye systemer.[68] OD opplyser videre at det ikke er utarbeidet applikasjonsbeskrivelser for eksisterende systemer, men at direktoratet planlegger å gjøre dette. Applikasjonsbeskrivelser skal være grunnlaget for risikovurderinger av systemet og blant annet dokumentere grunnlaget for brannmurregler og servicebrukere.

I ISO 27002 kapittel 5 anbefales det å utarbeide temaspesifikke policyer som understøtter informasjonssikkerhetspolicyen og videre pålegger virksomheten å implementere sikkerhetstiltak som blant annet aksesskontroll, beskyttelse mot ødeleggende programvare, håndtering av tekniske sårbarheter og kommunikasjonssikkerhet. Dokumentanalyse av *IKT-driftsinstruks for Oljedirektoratet* viser at instruksen blant annet omfatter policy for tiltak for sikring mot dataangrep. Instruksen omhandler sikkerhetsmessige forhold ved driften av ODs systemer.[69] Den baserer seg på og oppdateres etter NSMs grunnprinsipper for IKT-sikkerhet, som tar utgangspunkt i ISO 27001 og 27002.[70]

Det anbefales videre at virksomheten dokumenterer og tilgjengeliggjør driftsprosedyrer som spesifiserer instruksjoner for drift, blant annet installering og konfigurasjon av systemer (inkludert oppdatering), logging og overvåking, jf. ISO 27002 punkt 12.1.1. Formålet med gode prosedyrer og dokumentasjon er å sikre at driftsoppgaver utføres på samme måte, uavhengig av hvem som utfører det.

---

[64] Olje- og energidepartementet, brev av 11. april 2019 til Riksrevisjonen.
[65] Olje- og energidepartementet, brev av 11. april 2019 til Riksrevisjonen.
[66] Oljedirektoratet *Statement of Applicability (SOA)*, informasjon lagret i styringsverktøyet.
[67] Oljedirektoratet *Mal Applikasjonsutvikling - Applikasjonsbeskrivelse*, mottatt fra OD 31. august 2018.
[68] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019. Riksrevisjonen (2018) *Referat fra møte med OD om nettverk og brannmur 30. oktober 2018*, verifisert av OD 23. november 2018.
[69] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, oppdatert 28. august 2018.
[70] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.

Det er utarbeidet IKT-retningslinjer for interne og eksterne brukere av ODs IKT-utstyr og nettverk. Ifølge ODs SOA skal IKT-retningslinjer og IKT-driftsinstruks med tilhørende driftsprosedyrer ivareta kravene om dokumentasjon i ISO 27002 punkt 12.1.1.[71] OD har utarbeidet IKT-retningslinjer, og dokumentanalysen viser at dokumentet inneholder policy og regler for bruk av klient, mobiltelefoner, lagringsmedia og informasjonssikkerhet.[72]

Som vedlegg til IKT-driftsinstruksen har OD utarbeidet flere driftsprosedyrer som i hovedsak gjelder for IKT-personell. Observasjoner viser at [redacted] OD har følgende driftsprosedyrer som omfatter sikkerhetstiltakene, og som inngår i revisjonen:

[redacted]

Oppsummert viser revisjonen at OD gjennom IKT-driftsinstruksen har dokumentert temaspesifikke policyer som viser hvilke tiltak direktoratet skal implementere blant annet for å forhindre dataangrep og oppdage urettmessig tilgang til IKT-systemer. OD etterlever imidlertid i mindre grad anbefalinger om dokumentasjon av krav, prosedyrer og rutiner. På dette området avdekket revisjonen følgende mangler:

- Malen som skal benyttes for å dokumentere krav til informasjonssikkerhet, er ikke benyttet på ODs systemer, og OD har dermed ikke dokumentert krav.
- [redacted] ODs driftsprosedyrer beskriver i liten grad instruksjoner for drift på en slik måte at andre kan overta driftsoppgaver dersom dette skulle bli nødvendig. [redacted]

6.2.2 Sikker konfigurasjon av maskin og programvare

Herding er en prosess for å fjerne svakheter i et system for eksempel ved å oppdatere systemet, fjerne programmer som ikke er i bruk og endre standard passord. Herding er en viktig del av den totale informasjonssikkerheten, og manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i IKT-infrastrukturen, jf. NSMs grunnprinsipper for IKT-sikkerhet punkt 2.3.

Revisjonen har vurdert følgende temaer når det gjelder sikker konfigurasjon av maskin- og programvare:

- **Sikring av klienter (fysiske og virtuelle)**

[redacted]

[71] Oljedirektoratet *Statement of Applicability (SOA)*, informasjon lagret i styringsverktøyet.
[72] Oljedirektoratet (2018) *IKT --retningslinjer for riktig bruk av PC, mobil, lagringsmedia og god informasjonssikkerhet*, oppdatert 12. oktober 2018.
[73] [redacted]

[redacted]

- **Autorisert programvare på klienter**
  NSM anbefaler at kun autorisert programvare blir kjørt på virksomhetens enheter.

[redacted]

- **Krav til passord**
  Det er anbefalt i ISO 27002 punkt 9.4.3 at virksomheten har et system som sikrer passordkvalitet og jevnlig bytte av passord. I NSMs grunnprinsipper for IKT-sikkerhet punkt 2.5 står det at kontoer bør ha sterke passord. Revisjonen er basert på Microsofts anbefaling om passordinnstillinger.[81]

[redacted]

[74] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[75] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[76] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[77] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[78] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, datert 28. august 2018.
[79] Oljedirektoratet (2018) *Prosedyre for sikring av klient*, av 20. september 2018.
[80] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[81] Security policy settings reference - password policy <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy>.
[82] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, datert 28. august 2018.

[redacted]

Oppsummert viser revisjonen at OD delvis oppfyller anbefalingene, og dette gjelder følgende forhold:

- OD har iverksatt tiltak for å begrense programvare og hindre installasjon av uautorisert programvare på klienter.
- OD benytter standardisert mal for å installere og opprette klienter. På revisjonstidspunktet hadde imidlertid ikke OD [redacted]

[redacted] Passordpolicyen i AD følger nå beste praksis, men [redacted]

6.2.3 Kontroll på IKT-infrastruktur

For å unngå at en angriper får tilgang til hele virksomhetens infrastruktur, anbefaler NSM at virksomheter deler inn nettverk i sikkerhetssoner ved å segregere og/eller segmentere IKT-infrastrukturen. Med segregering menes fysisk adskillelse, og med segmentering menes logisk adskillelse.

Virksomheter bør også sikre nettverket for det tilfellet at klienter overtas av en angriper fra innsiden (en innsider). En innsider kan være en utro tjener, en leverandør med tilgang til infrastrukturen eller en ekstern som får tilgang til den fysiske infrastrukturen. [86]

I ODs IKT-driftsinstruks[87] går det fram at direktoratet vil følge NSMs råd for sikring av nettverk.

Revisjonen har vurdert følgende temaer knyttet til ODs kontroll med IKT-infrastrukturen:

- **NAC-løsning[88]**
  Nettverkskontroller og nettverk bør styres og kontrolleres for at informasjonen i systemer og applikasjoner skal være beskyttet, jf. ISO 27002 punkt 13.1.1. Videre anbefales det at systemer i nettverket autentiseres,[89] og at systemtilkobling til nettverket begrenses. NSM anbefaler i grunnprinsipper for IKT-sikkerhet punkt 2.4. at virksomhetene kontrollerer og beskytter IKT-infrastruktur mot interne og eksterne trusler.

  [redacted]

[83] Evry (2014) *Active Directory Health Check*, datert 17. februar 2017. Oljedirektoratet (2018) *Status AD - helsesjekk*, datert 28. august 2018.
[84] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[85] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[86] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet*, punkt 2.4.
[87] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, oppdatert 28. august 2018.
[88] NAC er en løsning som skal forhindre uautoriserte enheter i å koble seg til et nettverk.
[89] Med autentisering menes her at systemets identitet bekreftes.
[90] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[91] Riksrevisjonen (2018) *Referat fra møte med OD om enheter i nettverket og NAC 30. oktober 2018*, verifisert av OD 27. november 2018.

- **Segmentering av nettverk**
  Grupper av informasjonstjenester, brukere og informasjonssystemer bør være tilkoblet ulike nettverksoner, jf. ISO 27002 punkt 13.1.3. NSM anbefaler i grunnprinsipper for IKT-sikkerhet punkt 2.4 at virksomheter kontrollerer og beskytter IKT-infrastrukturen mot interne og eksterne trusler og segmenterer den i nettverk og soner som gjenspeiler virksomhetens risikoprofil og sikkerhetssoner.

[redacted]

Oppsummert viser revisjonen at OD ikke har etablert tiltak i samsvar med anbefalinger. Dette gjelder følgende:

[redacted]

6.2.4 Kontroll på brukerkontoer og administrative rettigheter

En angriper har ofte som hensikt å få tilgang til en legitim konto for å bruke denne til å øke rettigheter eller ta over andre kontoer med utvidede rettigheter. Kontoer som er blitt satt inaktive, men hvor rettigheter ikke er fjernet, kan også bli forsøkt utnyttet av angripere.[93]

En vanlig angrepsteknikk for å få kontroll på en bruker med utvidede rettigheter er å få en bruker til å åpne et e-postvedlegg, laste ned en fil fra en ondsinnet nettside eller gå inn på en nettside som inneholder skadevare. En annet teknikk er å skaffe seg flere privilegier ved å gjette eller knekke passordet til en administratorbruker.[94]

For å angi virksomhetens krav til aksesskontroll bør virksomheten etablere, dokumentere og vedlikeholde en policy for aksesskontroll, jf. ISO 27002 punkt 9.1.1. Policyen bør blant annet inneholde prinsipper for autorisasjon som for eksempel tjenstlig behov, segregering av roller, krav til formell autorisasjon, fjerning av rettigheter og periodisk gjennomgang.

ISO punkt 9.2 beskriver anbefalinger for styring av tilganger og rettigheter. Det er anbefalt at virksomheten etablerer en formell prosess for registrering, endring og sletting av tilganger når noen slutter i en stilling eller får endret arbeidsforhold, og en formell prosess for periodiske gjennomganger. Det er også anbefalt å benytte unike brukerkontoer. Videre bør virksomheten vedlikeholde en autorisasjonsprosess og en fortegnelse over alle tildelte rettigheter. Privilegerte tilgangsrettigheter bør begrenses og kontrolleres og tildeles en annen brukerkonto enn den som brukes til vanlige aktiviteter i virksomheten. Tilsvarende framgår det av NSMs grunnprinsipper for IKT-sikkerhet punkt 2.5 at virksomheten bør ha kontroll på kontoer, og at alle kontoer bør være personlige.

ODs policy for brukerhåndtering og tilgangskontroll er nedfelt i ODs IKT-driftsinstruks.[95]

Prosedyre for å tildele rettigheter og tilgang i it-systemer beskriver ODs formelle rutine for å opprette brukerkonti i AD og tildele rettigheter gjennom AD-grupper for ansatte, alminnelige brukere, driftspersonell og konsulenter. For upersonlige brukerkonti som standard administratorkonto og konti som brukes av systemer har OD etablert et eget system for håndtering av passord. ODs rutiner er videre beskrevet i dokumentet *Rutine - Styring av tilgang til informasjonssystemer i OD*. Rutinen beskriver blant annet hvordan OD skal autorisere brukere [redacted]

[92] Oljedirektoratet (2018) *Nettverk System dokumentasjon*, v. 1.1 12. september 2018.
[93] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet*, punkt 2.5.
[94] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet*, punkt 2.6.
[95] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, oppdatert 28. august 2018.

Revisjonen har vurdert følgende temaer knyttet til ODs kontroll på brukerkontoer og administrative rettigheter:

[redacted] Tilganger [redacted]

[redacted]

[redacted] Tilganger [redacted]

[redacted]

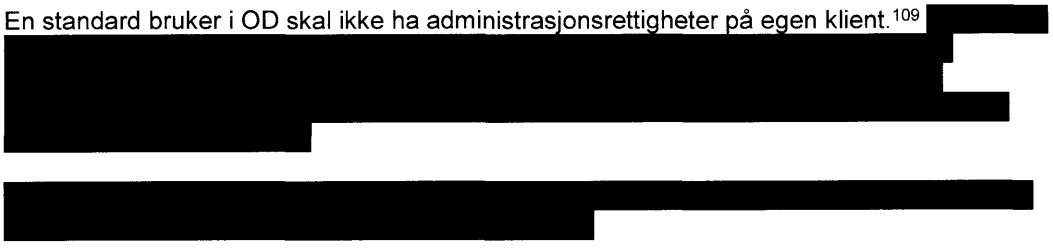
[96] Riksrevisjonen (2019) *Referat fra møter med Oljedirektoratet om* [redacted] *og* [redacted] *13. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[97] Riksrevisjonen (2019) *Referat fra møter med Oljedirektoratet om* [redacted] *og* [redacted] *13. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[98] Uttrekk fra Active Directory av 10. januar 2019.
[99] Riksrevisjonen (2019) *Referat fra møter med Oljedirektoratet om* [redacted] *og* [redacted] *13. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[100] [redacted]
[101] Oljedirektoratet (2019) *Utklipp fra ODs arkivplan*, sist godkjent 15. januar 2019.
[102] Riksrevisjonen (2019) *Referat fra møter med Oljedirektoratet om* [redacted] *og* [redacted] *13. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[103] Riksrevisjonen (2019) *Referat fra møter med OD om* [redacted] *og* [redacted] *13. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.

- **Tilganger databaser**
  Microsoft anbefaler at det kun benyttes Windows-autentisering for å autentisere brukere som logger på en databaseserver, så sant det er mulig.[104]

- **Tilgang til brannmur**

- **Lokale administratorrettigheter klient**
  NSM anbefaler at sluttbrukere ikke gis utvidede rettigheter (lokal administrator) på klient og trekker fram dette som ett av de fire viktigste tiltakene mot dataangrep.[108] Bakgrunnen for anbefalingen er at utvidede rettigheter gjør det lettere for en angriper å ta kontroll over en klient. Det er også en risiko for at en sluttbruker kan installere programvare med kjente sårbarheter.

  En standard bruker i OD skal ikke ha administrasjonsrettigheter på egen klient.[109]



[104]

[105] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, oppdatert 28. august 2018.
[106] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[107] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[108] NSM: Sjekkliste nr 1 *Fire effektive tiltak mot dataangrep og Sjekkliste nr 2 Ti viktige tiltak mot dataangrep.*
[109] Oljedirektoratet (2018) *Ikt-driftsinstruks for Oljedirektoratet*, oppdatert 28. august 2018.
[110] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[111] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.

[redacted]

- **Administratorkonti nettverk – Active Directory**
  Microsoft anbefaler at den innebygde administratorkontoen i Active Directory (AD) kun benyttes i forbindelse med gjenoppbygging etter en katastrofe og konfigureres slik at den ikke er mulig å logge på via nettverket, men kun lokalt på domenekontrollerne.[113] Dette for å unngå at den misbrukes.

[redacted]

- **Tilgang til systemer og filområder**
  Test av kontroller og observasjon viser [redacted]

[112] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[113] *Best Practices for Securing Active Directory, Appendix D: Securing Built-In Administrator Accounts in Active Directory* <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory>
[114] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[115] *Best Practices for Securing Active Directory, Attractive Accounts for Credential Theft* <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/attractive-accounts-for-credential-theft>
[116] Riksrevisjonen (2018) *Referat fra møter med OD om Active directory 13. desember 2018*, verifisert av OD 11. februar 2019.
[117] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[118] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[119] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[120] Evry (2017) *Active Directory Health Check*, datert 17. februar 2017 og Oljedirektoratet (2018) *Status AD - helsesjekk*, datert 28. august 2018.
[121] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.

[redacted]

Manglende oppfølging av brukerkonti kan medføre uautorisert tilgang til systemer og data. Manglende bruk av personlige administratorkonti kan gjøre at det ikke er mulig å spore hvem som har foretatt endringer.

Oppsummert viser revisjonen at OD har definert policy og rutiner for brukerhåndtering og tilgangskontroll, men at ikke alle anbefalinger følges:

- Det er etablert en formell prosess slik det er anbefalt med hensyn til oppretting, endring og fjerning/deaktivering av brukere i AD, og med hensyn til vedlikehold av tilgangsrettigheter og jevnlige kontroller.
- Det er etablert en formell prosess for tilganger til [redacted] og [redacted] slik det er anbefalt, men [redacted]
- OD har prosesser for å holde oversikt over brukere i databasene som understøtter [redacted] og [redacted], men [redacted]
- OD etterlever anbefaling om at brukere ikke gis lokale administratorrettigheter på klient.
- Det er etablert en formell prosess for å autorisere medlemmer i administratorgrupper i AD slik det er anbefalt, men [redacted]

6.2.5 Kontroll av dataflyt

Angripere utnytter systemer som kan nås fra Internett eller fra arbeidsstasjoner og bærbare og mobile enheter som er koblet til virksomhetens nettverk. For å ha kontroll på data som flyter gjennom virksomhetens perimetre[123] og mellom sikkerhetssoner, bør virksomheten kontrollere informasjonsflyten. Sikring av ytre perimetre, og mellom sikkerhetssoner bør bygges etter prinsippet «sikkerhet i dybden» og baseres på brannmurer, soneinndeling, nettverksbaserte deteksjons- (IDS) og beskyttelsessystemer (IPS).[124]

Brannmurer er maskinvare og/eller programvare som beskytter nettverk og systemer mot uønsket kommunikasjon. Brannmurer analyserer og kontrollerer kommunikasjonen ut fra forhåndsdefinerte regler. I reglene bestemmes det om trafikk skal tillates eller stoppes.

Ifølge ISO 27002 punkt 13.1.3 kan tilgang mellom nettverksdomener tillates, men slik tilgang bør kontrolleres ved hjelp av en gateway (for eksempel en brannmur eller en filtrerende ruter). Kriteriene for segregering av nettverk i domener og tilgangen som tillates gjennom gatewayene, bør være basert på en vurdering av sikkerhetskravene for hvert domene. NSM anbefaler i grunnprinsipper for IKT-sikkerhet punkt 2.7 at virksomheten bør benytte brannmurer med logging for å filtrere og kontrollere trafikken mellom ulike sikkerhetssoner og mot Internett. Filtreringen bør kun tillate forhåndsgodkjent nettverkstrafikk. Brannmurreglene bør ha en begrunnelse for åpning og bør revideres jevnlig.

I ODs IKT-retningslinjer[125] står det at direktoratet vil følge NSMs råd for sikring av nettverk, og at det skal være definert brannmurregler for all innkommende og utgående trafikk.

Revisjonen har vurdert følgende temaer knyttet til ODs kontroll av dataflyt:

---

[122] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[123] Med perimeter menes virksomhetens kontaktpunkt mot Internett.
[124] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet*, punkt 2.7.
[125] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, oppdatert 28. august 2018.

- **Brannmur**

[redacted]

6.2.6 Beskyttelse mot skadevare

Skadelig kode er en integrert og farlig del av cybertrusler, og den kan utformes for å påvirke systemer, enheter og data.[129] E-post og nettsider som er infisert med skadevare (virus, trojanere, og lignende), er vanlige inngangsportaler for angrep, og innholdet kan skreddersys for å lure en bruker. Virksomheter bør sikre e-post slik at ingen uvedkommende får tilgang til eller kan manipulere innholdet, at avsender verifiseres, og at e-post ikke kan benyttes til å levere skadevare. I tillegg bør nettleser konfigureres slik at skadelig kode i størst mulig grad blir hindret i å kjøre.[130] Virksomheter bør installere sikkerhetsoppdateringer så fort som mulig for å unngå å benytte produktversjoner med sikkerhetshull. Nyere produktversjoner har færre sikkerhetshull enn eldre versjoner, og de har ofte flere og bedre sikkerhetsfunksjoner.[131]

ISO 27002 punkt 12.2 anbefaler at virksomheter installerer og regelmessig oppdaterer programvare som kan oppdage ødeleggende programvare og reparere dersom det har oppstått skader. Dette for å kunne skanne datamaskiner og medier som et forebyggende eller rutinemessig sikkerhetstiltak.

[redacted]

Revisjonen har vurdert følgende temaer knyttet til ODs beskyttelse mot skadevare:

- **E-post med vedlegg og lenker**

[redacted]

- **Skript[133] og kommandoer**

[redacted]

- **Sikkerhetsoppdatering klienter og databaser**

[redacted]

---

[126] Oljedirektoratet (2018) *Firewall System dokumentasjon*, v.1.1 datert 24. august 2018.
[127] Riksrevisjonen (2019) *Referat fra møter med OD om brannmurer 13. desember 2018 og 16. januar 2019*, verifisert av OD 11. februar 2019.
[128] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[129] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet*, punkt 3.2.
[130] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet*, punkt 2.9.
[131] NSM: Sjekkliste nr. 2 (S-02) Ti viktige tiltak mot dataangrep.
[132] Riksrevisjonen (2019) *Referat fra møter med OD om antivirus og spam 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[133] Skript er et lite program som kjører en serie kommandoer eller instruksjoner.
[134] Oljedirektoratet (2018) *IKT-driftsinstruks for Oljedirektoratet*, oppdatert 28. august 2018.

[redacted]

Oppsummert viser revisjonen at OD i hovedsak etterlever anbefalinger ved at

- OD har etablert en løsning for beskyttelse av e-post som følger god praksis
- potensielle skadelige vedlegg og lenker blir oppdaget og stoppet [redacted]
- OD har etablert rutiner for automatisert utrulling av nye oppdateringer for klienter, og verktøy og rutiner for oppfølging

6.2.7 Kryptering

Av ISO 27002 punkt 10.1.1 framgår det at virksomheten bør utarbeide og implementere en policy for bruk av kryptografiske kontroller for å beskytte informasjon. NSM anbefaler i grunnprinsipper for IKT-sikkerhet punkt 2.8 å beskytte data og videre å benytte anbefalt kryptering i de tjenestene som tilbyr slik funksjonalitet.

Revisjonen har vurdert følgende temaer knyttet til ODs kryptering:

- **Ukrypterte tjenester** [redacted]
- **Svak kryptering** [redacted]

Oppsummert viser revisjonen at OD ikke etterlever anbefalinger ved at det benyttes [redacted]

6.2.8 Logging og overvåking

Hendelseslogger som registrerer brukeraktiviteter, avvik, feil og informasjonssikkerhetshendelser, bør produseres, oppbevares og gjennomgås regelmessig, jf. ISO 27002 punkt 12.4. Det er vesentlig å oppdage uregelmessigheter og hendelser tidlig for å kunne oppdage og håndtere dataangrep. Mangelfull logging, sammenstilling og analyse av loggdata gjør at angripere kan skjule tilstedeværelse, handlinger og aktiviteter i virksomhetens nettverk og på maskiner som utnyttes.[140]

[redacted]

[135] Oljedirektoratet (2018) *Prosedyre for sikring av klient,* av 20. september 2018.
[136] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[137] Riksrevisjonen (2019) *Referat fra møter med OD om sikring av klienter 12. desember 2018 og 15. januar 2019*, verifisert av OD 11. februar 2019.
[138] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[139] Informasjon om passordhasher.
[140] Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet*, punkt 3.5.
[141] Riksrevisjonen (2018) *Referat fra møte med OD om logging og overvåking 30. oktober 2018*, verifisert av OD 23 november 2018.

[redacted]

Revisjonen har gjennom ulike metoder vurdert ODs evne til oppdage følgende aktiviteter gjennom logging og overvåking:

- **Nettverksskanning**
  [redacted]
- **Innhøsting av passordhasher**[146]
  [redacted]
- **Kjøring av skript og kommandoer**
  [redacted]
- **Søk på filområder og påloggingsforsøk**
  [redacted]

Oppsummert viser revisjonen at OD ikke etterlever anbefalinger, ettersom ODs overvåking [redacted]

6.3 Problemstilling 3 – oppfølging og evaluering av styringssystem og sikkerhetstiltak

Problemstilling 3 omfatter aktiviteter for å følge opp og evaluere styringssystemet for informasjonssikkerhet og sikkerhetstiltak. Virksomheten bør systematisk vurdere om sikkerhetstiltakene fungerer, om regelverket etterleves, og om internkontrollarbeidet gjennomføres som forutsatt.

[142] Riksrevisjonen (2018) *Referat fra møte med OD om antivirus og proxy 30. oktober 2018*, verifisert av OD 23 november 2018.
[143] Riksrevisjonen (2018) *Referat fra møte med OD om logging og overvåking 30. oktober 2018*, verifisert av OD 23 november 2018.
[144] Riksrevisjonen (2019) *Referat fra møte med OD om logging og overvåking 16. januar 2019*, verifisert av OD 11. februar 2019.
[145] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.
[146] Passordhash er passord som ikke er i klartekst, og hvor metoden passordhashing er benyttet for å skjule passordet.
[147] Riksrevisjonen (2019) *Oppsummering og spørsmål teknisk av 11. februar 2019*, verifisert av OD 20. februar 2019.

Formålet er at virksomheten gjennom målinger, undersøkelser, evalueringer og revisjoner skal få bedre kunnskap om sikkerhetstilstanden og sørge for kontinuerlig forbedring. Områdene som er revidert for å besvare problemstilling 3, presenteres nedenfor, og de er valgt på bakgrunn av beste praksis og ODs egne krav til oppfølging og evaluering.

6.3.1 Avviks- og hendelseshåndtering på informasjonssikkerhetsområdet

ISO 27002 punkt 16.1.1 anbefaler at virksomheten utarbeider og kommuniserer prosedyrer for å overvåke, oppdage, analysere, reagere på, håndtere og rapportere informasjonssikkerhetshendelser og -brudd. Videre anbefaler standarden at virksomheten oppretter hensiktsmessig kontakt med myndigheter som håndterer forhold knyttet til informasjonssikkerhetsbrudd. Informasjonssikkerhetshendelser bør vurderes ved bruk av en skala for å avgjøre om hendelsen skal klassifiseres som et informasjonssikkerhetsbrudd, jf. ISO punkt 16.1.4. Det å klassifisere og prioritere brudd kan bidra til å identifisere virkningen og omfanget av et informasjonssikkerhetsbrudd.

[redacted]

Ifølge *Strategi for informasjonssikkerhet* skal den enkelte medarbeider i OD rapportere dersom han eller hun mistenker eller oppdager sikkerhetsbrudd. *Prosedyre for å rapportere informasjonssikkerhetshendelser/brudd* og *Prosedyre for håndtering av informasjonssikkerhetshendelser IT-drift* definerer hvilke hendelser som skal rapporteres, og hvordan disse skal rapporteres.[149]

OD har to digitale systemer[150] hvor ansatte kan rapportere hendelser som gjelder informasjonssikkerhet. OD opplyser at innrapporterte hendelser følges opp av sikringskoordinatoren, og den operative ledelsen som vurderer hendelsen, utpeker gjennomføringsansvarlig og godkjenner tiltak.[151] Ansatte kan også rapportere informasjonssikkerhetshendelser direkte til sin nærmeste leder og/eller til sikringskoordinatoren, som i slike tilfeller skal registrere hendelsen i systemene. I tillegg har OD en postkasse for anonyme henvendelser som følges opp av sikringskoordinatoren.[152]

Dokumentanalyse av innrapporterte hendelser viser at det i det ene systemet for 2017 ikke er registrert noen saker som omfatter informasjonssikkerhet, og at det i 2018 ble registrert én sak.[153] I det andre systemet er det registrert flere saker som gjelder informasjonssikkerhet.[154] For dette systemet opplyser OD at kategorien «Informasjonssikkerhetshendelser» først ble innført i august 2018, og at innrapporterte hendelser før dette ble kategorisert som «*hendelser*».[155] Analyser av uttrekk fra systemet viser at det for 2017 og fram til august 2018 ble rapportert to hendelser knyttet til informasjonssikkerhet, og at det etter august er registrert 12 hendelser for 2018. Disse hendelsene er i stor grad rapportert av de som har sentrale roller i informasjonssikkerhetsarbeidet i OD. I tillegg viser analysene at det for 2017 og 2018 totalt er registrert 184 saker. I disse har det i hovedsak vært behov for å følge opp klienten med hensyn til skadevare. Analysene viser videre at de fleste sakene omtalt ovenfor er løst, og at saker som ikke er løst, er påbegynt og av nyere dato.[156]

Systemeieren skal omtale informasjonssikkerhetshendelser i en årlig egenkontroll. OD opplyser at hensikten er å fange opp og håndtere hendelser som allerede er rapportert i systemene.[157] Dokumentanalysen viser imidlertid at spørsmålet om informasjonssikkerhetshendelser i

---

[148] Nasjonal sikkerhetsmyndighet (2014) *Varslingssystem for digital infrastruktur* <https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/>.
[149] Oljedirektoratet (2018) *Prosedyre for å rapportere informasjonssikkerhetshendelser/brudd*, 22. november 2018. Oljedirektoratet (2018) *Prosedyre for håndtering av informasjonssikkerhetshendelser IT-drift*, oppdatert 7. september 2018.
[150] Servicedesk ([redacted]) og [redacted]- avvikssystemet.
[151] Oljedirektoratet (2018) *Prosedyre for å rapportere informasjonssikkerhetshendelser/brudd*, 22. november.2018. Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[152] Oljedirektoratet (2018) *Prosedyre for å rapportere informasjonssikkerhetshendelser/brudd*, 22. november 2018. Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[153] Oljedirektoratet (2019) *Hendelsesrapport - Informasjonssikkerhet* [redacted] mottatt fra OD 7. februar 2019.
[154] Oljedirektoratet (2019) *Oversikt over hendelser* [redacted], mottatt fra OD 7. februar 2019.
[155] Oljedirektoratet (2019) *Svar på spørsmål fra Riksrevisjonen*, 31. januar 2019.
[156] *Hendelsesrapport - Informasjonssikkerhet* [redacted], mottatt fra OD 7. februar 2019 og Oversikt over hendelser [redacted], mottatt fra OD 7. februar 2019.
[157] Oljedirektoratet (2019) *Tilbakemelding til Riksrevisjonen etter oppsummeringsmøte*, 11. mars 2019.

egenkontrollen er stilt på en slik måte at systemeierne svarer forskjellig på like tilfeller, selv om ingen av systemeierne har rapportert om hendelser.[158]

Hendelser skal omtales i rapport om sikkerhetstilstanden som OD oversender til departementet. OD opplyser at det er en overordnet vurdering av hendelsesrapportene som blir presentert for oljedirektøren og den strategiske ledelsen i forbindelse med gjennomgang av utkast til rapport om sikkerhetstilstanden i OD.[159] Dokumentanalyse viser at OD ikke benytter en skala for å identifisere virkningen og omfanget av innrapporterte informasjonssikkerhetshendelser. I rapportene om sikkerhetstilstanden for 2017 og 2018, som er oversendt departementet, opplyser OD at det ikke har vært alvorlige hendelser i forbindelse med informasjonssikkerhet.[160]

Oppsummert viser revisjonen at OD delvis følger anbefalingene ved at det er etablert en metode for å rapportere informasjonssikkerhetshendelser, og revisjonen registrerer at antallet innrapporterte hendelser har økt fra 2017 til 2018. Hendelser er imidlertid i hovedsak innrapportert av personell med sentrale roller i informasjonssikkerhetsarbeidet, og det er uklart om metoden for innrapportering av hendelser er godt nok kommunisert til ansatte i OD. Videre omfatter ikke metoden en dokumentert vurdering av hvor alvorlig hendelsen er. Det er derfor vanskelig å se hvilke vurderinger som er gjort av alvorlighetsgraden av hendelsene i rapporteringen til departementet.

6.3.2 Uavhengige gjennomganger av informasjonssikkerheten

ISO 27001 punkt 9.2 anbefaler at det gjennomføres revisjoner for å få informasjon om styringssystemet er i samsvar med krav. Videre anbefaler punkt 9.2 at styringssystemet implementeres og vedlikeholdes på en hensiktsmessig måte. Av ISO 27002 punkt 18.2.1 går det fram at en uavhengig gjennomgang bør omfatte sikkerhetsmål, sikkerhetstiltak, strategier, prosesser og prosedyrer for informasjonssikkerhet, og at ledelsen bør vurdere korrigerende tiltak dersom det blir identifisert avvik.

Riksrevisjonen rapporterte for 2013 at OD ikke hadde implementert et styringssystem for informasjonssikkerhet. En ny revisjon ble gjennomført for 2016, og Riksrevisjonen rapporterte om vesentlige svakheter ved informasjonssikkerheten i OD. Følgende mangler ble påvist:

- Klassifisering av informasjon med hensyn til hvor sensitiv den er, er ikke ferdigstilt.
- Årlig risikoprosess er definert, men ikke etablert i praksis.
- Sikkerhetstiltak er ikke utledet fra styringssystemet og er i varierende grad dokumentert og evaluert.
- Det finnes ikke et enhetlig system for å rapportere og håndtere informasjonssikkerhetshendelser.
- Styringssystemet er ikke evaluert og forbedret.

Det framgår av ODs SOA at det skal gjennomføres en uavhengig gjennomgang av informasjonssikkerheten hvert tredje år. OD har hatt uavhengige gjennomganger av informasjonssikkerheten i både 2017 og 2018.[161] OD opplyser at det også var planlagt en sikkerhetsgjennomgang høsten 2018, men at denne foreløpig er utsatt til våren 2019 på grunn av Riksrevisjonens etterlevelsesrevisjon av sikring mot dataangrep.[162]

I 2017 ble styringssystemets egnethet vurdert av en ekstern aktør. Det framgår av rapporten at vurderingene bygger på informasjon fra intervjuer med ODs ansatte og aktuell dokumentasjon, men at det ikke er utført kontrollhandlinger. Gjennomgangen i 2018 er utført på oppdrag fra Olje- og energidepartementet og gjaldt flere forhold, blant annet status for arbeidet med informasjonssikkerhet. Rapporten viser at analyser og evaluering er basert på dokumentstudier og intervjuer. I tillegg mottok OD i 2017 en ekstern vurdering av AD, med anbefalinger om blant annet [redacted][163]

[158] Oljedirektoratet (2018) [redacted] - *systemeiers årlige egenkontroll 2018*. Oljedirektoratet (2018) [redacted] - *systemeiers årlige egenkontroll 2018*. Oljedirektoratet (2018) [redacted] - *systemeiers årlige egenkontroll 2018*.
[159] Oljedirektoratet (2019) *Svar på spørsmål fra Riksrevisjonen*, 31. januar 2019.
[160] Oljedirektoratet (2018) *Utdrag rapport om sikkerhetstilstanden 2017*, oversendt til Olje- og energidepartementet 12. januar 2018. Oljedirektoratet (2019) *Utdrag rapport om sikkerhetstilstanden 2018*, oversendt til Olje- og energidepartementet 15. januar 2019.
[161] PricewaterhouseCoopers AS (2017) *ROS analyse - informasjonssikkerhet Oljedirektoratet*, 4. april 2017. A-2 Norge AS og Menon Economics (2018) *Evaluering av måloppnåelse og Oljedirektoratets dataforvaltning*, 13. september 2018.
[162] Riksrevisjonen (2018) *Referat fra kartleggingsmøte med OD 4. september 2018*, verifisert av OD 3. oktober 2018.
[163] Evry (2017) *Active Directory Health Check*, datert 17. februar 2017.

Den uavhengige gjennomgangen i 2017 peker på 22 forhold knyttet til informasjonssikkerhet, blant annet disse:

- Vedlikeholdet av dokumentasjon i styringssystemet fremstår som tilstrekkelig, men det mangler fortsatt dokumentasjon for at styringssystemet skal være komplett og ivareta informasjonssikkerhet.
- Analyser og kontinuerlig forbedring av informasjonssikkerhet er ikke tilstrekkelig dokumentert og ikke implementert.
- Gjennomføring av risiko- og sikkerhetsvurderinger av systemer er ikke godt nok utført, og OD har ingen formell metode for å benytte identifiserte risikoer i forbedringsarbeid.
- Sikkerhetstesting av systemer er ikke tilstrekkelig gjennomført eller dokumentert.

Den uavhengige gjennomgangen i 2018 har vurdert hvordan OD har fulgt opp forhold påpekt i Riksrevisjonens revisjon for 2016 og i den uavhengige gjennomgangen i 2017. Det framkommer blant annet at «arbeidet med styringssystemet er såpass videreutviklet og aktiviteter for styringen i en slik grad implementert at styringssystemet for informasjonssikkerhet vurderes å være i samsvar med eForvaltningsforskriften § 15». Den uavhengige gjennomgangen i 2018 anbefaler følgende fire tiltak knyttet til informasjonssikkerhet:

- kontinuerlig videreutvikle styringssystemet og fullføre planhjulet med nødvendige tiltak
- fullføre risikoanalysen av kritiske IKT-systemer
- gjennomføre ny sikkerhetsgjennomgang
- fokusere på informasjonssikkerhet i digitaliseringsprogrammet, både knyttet til utvidet selvbetjening, løsningsdesign, systemutvikling, test og drift.

Utover å anbefale disse tiltakene kommenterer den uavhengige gjennomgangen i 2018 at enkelte av de tidligere påpekte forholdene må følges opp på et senere tidspunkt. Dette gjelder blant annet kontinuerlig forbedring, som både Riksrevisjonen i 2016 og den uavhengige gjennomgangen i 2017 påpekte, og som den uavhengige gjennomgangen i 2018 foreslår at OD vurderer når alle aktivitetene i årshjulet er gjennomført.

OD har utarbeidet *Prosedyre for registrering av tiltak etter revisjon*, og denne har til hensikt å beskrive hvordan OD skal håndtere tiltak etter uavhengige gjennomganger.[164] OD opplyser at de vurderer foreslåtte tiltak fortløpende, og at de registrerer aktuelle tiltak i styringsverktøyet.[165] OD opplyser videre at det arbeides med å følge opp anbefalte tiltak fra de uavhengige gjennomgangene i 2017 og 2018.

Oppsummert viser revisjonen at OD følger anbefalingen om å gjennomføre uavhengige gjennomganger av styringssystem for informasjonssikkerhet, og at det er etablert en prosess for hvordan tiltak skal følges opp. De uavhengige gjennomgangene omfatter imidlertid i mindre grad kontroll av implementerte sikkerhetstiltak. Revisjonen registrerer at det over tid er påpekt de samme svakhetene i de ulike gjennomgangene.

6.3.3 Systemeierens egenkontroll av sikkerhetstiltak

I ISO 27002 punkt 18.2.2 anbefales det at ledere identifiserer hvordan det jevnlig skal kontrolleres at krav til informasjonssikkerhet definert i policyer, standarder og annet relevant regelverk er oppfylt. ISO 27002 punkt 18.2.3 omhandler teknisk samsvar, og det framgår at informasjonssystemet regelmessig bør gjennomgås for å sikre samsvar med organisasjonens policyer og standarder for informasjonssikkerhet. Videre framgår at teknisk samsvar omfatter undersøkelse av operative systemer for å påse at sikkerhetstiltak for maskinvare og programvare er riktig ivaretatt. Gjennomganger av teknisk samsvar bør utføres av kompetent og autorisert personell, eller under tilsyn av slikt personell.

Av *Strategi for informasjonssikkerhet* går det fram at systemeieren årlig skal vurdere informasjonssikkerheten i systemet for å sikre at konfidensialitet, integritet og tilgjengelighet er ivaretatt. OD opplyser at systemeieren er ansvarlig for å utføre egenkontroll, og at systemeieren gjennom denne kontrollen skal forsikre seg om at rutiner fungerer etter hensikten, og foreslå

[164] Oljedirektoratet (2018) *Prosedyre for registrering av tiltak etter revisjon*, 29. september 2018.
[165] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.

eventuelle forbedringer.[166] Anbefalingen i ISO punkt 18.2.3 om gjennomgang av teknisk samsvar skal ifølge ODs SOA ivaretas av systemeierens årlige egenkontroll.

Dokumentanalyse viser at egenkontrollen består av 10 spørsmål som besvares med «ja», «nei» eller «ikke relevant». Systemeieren har også mulighet til å gi kommentar til hvert enkelt spørsmål i egenkontrollen. OD opplyser at spørsmålene i egenkontrollen skal besvares for alle systemer, og at de justerer spørsmålene ved behov fra år til år.[167] OD opplyser at det ikke er gjennomført egenkontroll av systemer i 2017. [168] Dokumentanalyse viser at det på revisjonstidspunktet ikke er gjennomført egenkontroll for 2018 for alle systemene. Av 76 systemer som er verdivurdert i styringssystemet, er det ifølge OD 62 som omfattes av egenkontrollen i 2018. OD opplyser at avviket i antallet skyldes at det ikke er behov for egenkontroll av systemer som ikke er i bruk, systemer som kun benyttes til analysearbeid, eller systemer hvor arbeidet med risikovurdering er påbegynt. Dokumentanalysen viser at det på revisjonstidspunktet er gjennomført egenkontroll for 55 av 62 systemer, og at det dermed ikke er gjennomført egenkontroll for 7 systemer.

I egenkontrollen for 2018 skal systemeieren vurdere om informasjonssikkerheten i systemet er ivaretatt. Videre stilles det blant annet spørsmål om tilganger er ajourført, om det foreligger oppdaterte system- og applikasjonsbeskrivelser, om informasjonssikkerhetshendelser/brudd er rapportert og håndtert, og om det er behov for ny eller oppdatert risikovurdering.[169]

Dokumentanalyse av egenkontroller utført av systemeierne for 2018 viser store variasjoner i besvarelsene. Systemeierne har i varierende grad benyttet kommentarfeltet, og besvarelsene deres indikerer at de har ulik oppfatning av hva spørsmålene innebærer. For eksempel viser egenkontrollen at bare 3 av 15 systemer har behov for risikovurdering selv om systemet i styringsverktøyet er verdivurdert til rødt og risikovurdering derfor skal gjennomføres ifølge ODs metode for verdi- og risikovurdering. Tilsvarende viser dokumentanalyse at systemeierne svarer forskjellig på like tilfeller på spørsmålet om informasjonssikkerhetshendelser, jf. omtale ovenfor i punkt 6.3.1.

OD opplyser at sikringskoordinatoren og IKT-sikkerhetsrådgiveren følger opp egenkontrollene. OD erfarer at systemeierne besvarer egenkontrollen ulikt, og opplyser at dette skyldes at systemene er forskjellige. OD vurderer å utarbeide en kort veiledning for hvordan egenkontrollen skal gjennomføres.[170]

Oppsummert viser revisjonen at OD ikke følger anbefalingen om å jevnlig kontrollere at krav til informasjonssikkerhet er oppfylt. OD har utarbeidet en metode for gjennomgang av sikkerhetstiltak og har forutsatt at systemeierens egenkontroll skal ivareta anbefalingen om å påse at sikkerhetstiltak er riktig ivaretatt. Revisjonen kan imidlertid ikke se at egenkontrollen har et omfang eller en kvalitet som er i samsvar med anbefalingene. Systemeierne har ikke gjennomført egenkontroll av sikkerhetstiltak for 2017, og heller ikke for enkelte systemer for 2018. Etter revisjonens vurdering er ikke systemeierens egenkontroll god nok til å påvise svakheter i systemet og for å iverksette forbedringstiltak. Revisjonen vurderer dermed ikke systemeierens egenkontroll som en dokumentert evaluering av implementerte sikkerhetstiltak.

6.3.4 Evaluering og forbedring av styringssystem for informasjonssikkerhet

Virksomheten bør evaluere virkningen av styringssystemet for informasjonssikkerhet, jf. ISO 27001 punkt 9.1. Standarden anbefaler videre i punkt 9.3 at ledelsen skal gjennomgå styringssystemet for informasjonssikkerhet jevnlig, for å sikre at det er velegnet, tilstrekkelig og virkningsfullt. Som bevis på resultatene fra ledelsens gjennomgang skal dokumentert informasjon oppbevares. I tillegg anbefaler standarden i kapittel 10 at virksomheten skal reagere på eventuelle avvik, innføre korrigerende tiltak og kontinuerlig forbedre virkningen av styringssystemet.

Ifølge *Strategi for informasjonssikkerhet* skal gjennomgangen av informasjonssikkerhet i OD inngå i et årlig møte mellom [redacted] og ledelsen. OD opplyser at grunnlaget for ledelsens årlige

---

[166] Oljedirektoratet (2014) *Strategi for informasjonssikkerhet*, oppdatert 23. august 2018. Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[167] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[168] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[169] Oljedirektoratet (2018) [redacted] *- systemeiers årlige egenkontroll 2018*. Spørsmålene i egenkontrollen er like for alle systemer.
[170] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.

gjennomgang av styringssystemet er utkast til rapport om sikkerhetstilstanden. Denne viser implementerte tiltak i tillegg til planlagte tiltak og forbedringsforslag.[171] Utkastet er utarbeidet av [redacted] og skal være basert på gjennomførte risikovurderinger, systemeiernes egenkontroll, innmeldte hendelser, eksterne gjennomganger og innhentet informasjon fra andre aktuelle lag/områder i OD, blant annet IKT, kriseberedskap, personvern og bygg/drift. I tillegg opplyser OD at [redacted] og [redacted] i arbeidet med styringssystemet foretar fortløpende evalueringer som også inngår som grunnlag til rapporten. [172]

Utkast til rapport om sikkerhetstilstanden blir først behandlet av den strategiske og den operative ledelsen som har resultatansvar for sikkerhet i OD. Rapporten oversendes deretter til oljedirektøren og de strategiske lederne for endelig godkjenning i ledermøte.[173] I forkant av behandlingen oversender sikringskoordinatoren saksframlegg og utkast til rapport til ledelsen. I møtene med ledelsen presenterer sikringskoordinatoren hovedpunktene fra rapporten, og ledelsen i OD har i behandlingen av rapporten for 2018 fått presentert at «ODs styringssystem for informasjonssikkerhet er etablert, implementert og driftes i styringsverktøyet [redacted], og systemet fungerer etter hensikt».[174] Siden rapporten er gradert begrenset i henhold til sikkerhetsloven, opplyser OD at det i møtereferatet kun vil framgå om ledelsen har godkjent rapporten, og eventuelt om noe må endres.[175] Rapport om sikkerhetstilstanden oversendes Olje- og energidepartementet etter at den er godkjent av ledelsen.

Dokumentanalyse av saksfremlegg og referater fra operativt og strategisk ledermøte viser at utkast til rapport om sikkerhetstilstanden for 2017 og 2018 er godkjent av ledelsen før oversendelse til departementet. Oversendte saksfremlegg til ledermøtene viser ikke til vedlegg utover utkast til rapport om sikkerhetstilstanden.[176] Referater fra møter der oljedirektøren, strategisk ledelse og operativ ledelse deltar viser ikke diskusjonen fra møtene, men det framgår at kommentarer skal innarbeides i rapporten.[177]

OD opplyser at årlig rapport om sikkerhetstilstanden gir en god oversikt over status i sikkerhetsarbeidet, evalueringer og planer fremover. I rapport om sikkerhetstilstanden for 2017 og 2018 framgår at OD vurderer «at den generelle sikkerhetstilstanden i OD er svært god».[178] I likhet med ledelsen i OD har departementet i rapporten for 2018 fått opplyst at «ODs styringssystem for informasjonssikkerhet er etablert, implementert og driftes i styringsverktøyet [redacted], og systemet fungerer etter hensikt». I rapporten for 2018 konkluderes det videre med at det jevnlig gjennomføres risikovurderinger som grunnlag for ODs forebyggende sikkerhetstiltak, og at OD har etablert en god grunnsikring hvor det iverksettes forebyggende sikkerhetstiltak fortløpende ved behov. Tilsvarende opplyser OD i årsrapporten for 2017 å ha etablert et styringssystem for informasjonssikkerhet basert på ISO 27001 og Difis veiledningsmateriell.

Oppsummert viser revisjonen at OD følger anbefalingen ved at det er utarbeidet en metode for årlig gjennomgang av styringssystem for informasjonssikkerhet. Utkast til rapport om sikkerhetstilstanden er utgangspunkt for gjennomgangen, og den skal være basert på interne og eksterne vurderinger av sikkerhetsarbeidet. Grunnlaget rapporten skal bygge på, er imidlertid mangelfullt eller ikke gjennomført, jf. omtale ovenfor i punkt 6.1.4, 6.3.1, 6.3.2 og 6.3.3.

7. Konklusjoner

Oljedirektoratet (OD) har en sentral rolle i forvaltningen av olje- og gassressursene på norsk kontinentalsokkel og utøver forvaltningsmyndighet i forbindelse med tildeling av areal og i forbindelse med leting etter og utvinning av petroleumsforekomster. I flere IKT-systemer behandler OD

---

[171] Oljedirektoratet (2014) *Strategi for informasjonssikkerhet*, oppdatert 23. august 2018. Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[172] Riksrevisjonen (2019) *Referat fra møter med OD om styringssystem 27. november, 12. og 13. desember 2018*, verifisert av OD 25. januar 2019.
[173] Oljedirektoratet (2019) *Svar fra OD 11. februar 2019*, e-post fra Riksrevisjonen 7. februar 2019.
[174] Oljedirektoratet (2019) *Sikkerhetstilstanden i OD 2018*, presentasjon av 10. januar 2019.
[175] Oljedirektoratet (2019) *Svar fra OD 11. februar 2019*, e-post fra Riksrevisjonen 7. februar 2019. Rapport om sikkerhetstilstanden er i utgangspunktet gradert begrenset i henhold til sikkerhetsloven, men OD har i ettertid nedgradert enkeltelementer i rapporten, jf. verifisert referat fra møter med Oljedirektoratet 27. november 2018, 12. desember 2018 og 13. desember 2018.
[176] Oljedirektoratet (2019) *Sikkerhetstilstanden i OD 2018*, saksfremlegg SL 14. januar 2019. Oljedirektoratet (2018) *Sikkerhetstilstanden i OD 2017*, saksfremlegg SL 8. januar 2018.
[177] Oljedirektoratet (2019) *Møtereferat SL*, 14. januar 2019. Oljedirektoratet (2018) *Møtereferat SL*, 8. januar 2018.
[178] Oljedirektoratet (2018) *Utdrag rapport om sikkerhetstilstanden 2017*, oversendt til Olje- og energidepartementet 12. januar 2018. Oljedirektoratet (2019) *Utdrag rapport om sikkerhetstilstanden 2018*, oversendt til Olje- og energidepartementet 15. januar 2019.

informasjon som ikke bør komme på avveie, og som eksterne aktører kan være interessert i. Dette er blant annet politisk, børssensitiv og forretningssensitiv informasjon.

Som en offentlig virksomhet har OD ansvar for å beskytte informasjonen som forvaltes, jf. forvaltningsloven, eForvaltningsforskriften og reglementet for og bestemmelser om økonomistyring i staten. Betydningen av å ha et godt styringssystem for informasjonssikkerhet, for å beskytte informasjon som virksomheten behandler, øker i takt med digitaliseringen i offentlig forvaltning. Riksrevisjonen påpekte i sin rapportering for 2013 og 2016 vesentlige svakheter på informasjonssikkerhetsområdet i OD. Kontroll- og konstitusjonskomiteen forutsatte at departementet umiddelbart iverksatte tiltak.

Riksrevisjonen har for 2018 gjennomført en revisjon av sikring mot dataangrep i OD som omfatter styringssystem for informasjonssikkerhet og sikkerhetstiltak på utvalgte områder. Styringssystemet for informasjonssikkerhet skal hjelpe ledelsen og virksomheten til å ha systematisk internkontroll på området. Videre skal det medvirke til at virksomheten velger riktige sikkerhetstiltak, og sørge for at de valgte løsningene blir evaluert og om nødvendig forbedret.

Målet med revisjonen har vært å kontrollere om OD arbeider systematisk med å forhindre dataangrep og oppdage urettmessig tilgang til IKT-systemer. Revisjonen har lagt til grunn at OD baserer informasjonssikkerhetsarbeidet på ISO 27000-standardene for å etterleve kravene til internkontroll. For å utdype anbefalinger i ISO-ene har revisjonen i tillegg benyttet veiledere fra NSM og aktuelle bransjestandarder.

Revisjonen konkluderer med at OD har etablert grunnlaget for et systematisk arbeid med informasjonssikkerheten, men på grunn av vesentlige mangler i gjennomføringen er det risiko for at noen får urettmessig tilgang til IKT-systemer dersom OD blir rammet av et dataangrep.

Styring av informasjonssikkerhet for å planlegge sikkerhetstiltak
ODs styrende dokumenter for informasjonssikkerhet gir rammer for et systematisk arbeid med å forhindre dataangrep og oppdage urettmessig tilgang til IKT-systemer. Verdivurdering av informasjon skal danne grunnlag for videre arbeid med risikovurderinger og planlegging av sikkerhetstiltak. OD har gjennomført verdivurdering, men metoden som er benyttet, kan medføre at viktige risikovurderinger ikke blir gjennomført. Risikostyring skal bidra til at det iverksettes tiltak slik at sensitiv informasjon ikke blir tilgjengelig for uvedkommende. OD har i liten grad gjennomført risikovurderinger, og implementerte sikkerhetstiltak er dermed ikke basert på en systematisk vurdering av risiko.

Gjennomføring av sikkerhetstiltak
Valg av sikkerhetstiltak er avhengig av virksomhetens generelle tilnærming til risikostyring og hvordan tiltak samlet kan gi god nok beskyttelse. Mangler i verdivurdering, risikostyring og evaluering kan medføre at OD har svakheter i arbeidet med sikkerhetstiltak.

OD har i liten grad utarbeidet dokumenter som skal vise hvordan sikkerhetstiltak skal implementeres og systemene skal driftes. OD har implementert flere av de anbefalte sikkerhetstiltakene i NSMs grunnprinsipper for IKT-sikkerhet. ODs IKT-systemer har likevel svakheter som kan utnyttes i forbindelse med dataangrep, ettersom enkelte sikkerhetstiltak ikke fungerer som forutsatt eller ikke er implementert.

Oppfølging og evaluering av styringssystem og sikkerhetstiltak
For å sikre at styringssystemet for informasjonssikkerhet og sikkerhetstiltak fungerer som forutsatt, har OD etablert prosesser for evaluering. Grunnlaget for den samlede evalueringen av sikkerhetsarbeidet skal blant annet være risikovurderinger, innmeldte hendelser, systemeierens egenkontroll og uavhengige gjennomganger. Grunnlaget for ODs vurderinger er imidlertid mangelfullt siden blant annet risikovurderinger i liten grad er gjennomført og systemeierens egenkontroll ikke evaluerer om implementerte sikkerhetstiltak fungerer som forutsatt.

OD dokumenterer den årlige evalueringen av sikkerhetsarbeidet i utkast til rapport om sikkerhetstilstanden, som oversendes departementet når den er godkjent av ODs ledelse. Statusen som rapporteres, er imidlertid ikke i samsvar med funn påvist i revisjonen. I rapportene om sikkerhetstilstanden for 2017 og 2018 er det blant annet rapportert «at den generelle sikkerhetstilstanden i OD er svært god». I ODs overordnede risikovurderinger for 2019, som er oversendt departementet, har OD tilsvarende orientert om at risikoen knyttet til arbeidet med informasjonssikkerhet er lav, og at risikoen for etterretningsvirksomhet vurderes som moderat på grunn av robuste sikkerhetstiltak i OD.