SYKEHUSINNKJØP

Internrevisjonsrapport 01/2022

Internkontroll for informasjonssikkerhet og personvern – Fase 1

Internrevisjonen i Sykehusinnkjøp HF, 06.12.2022

Innholdsfortegnelse

Sammendrag

Denne rapporten er utarbeidet etter internrevisjon i Sykehusinnkjøp HF i perioden april til november 2022.

Formål med revisjonen

Formålet med revisjonen i fase 1 er å bekrefte at Sykehusinnkjøp har etablert styrende dokumenter for internkontroll for informasjonssikkerhet og personvern, og at disse er tilpasset foretakets størrelse, risiko og egenart.

Metoder og fokusområder

Internrevisjonen er gjennomført ved dokumentgjennomgang og intervjuer. Revisjonens fokusområder har vært; 1. Ledelsens styring og oppfølging, 2. Vurdering og håndtering av risiko, 3. Hendelseshåndtering og 4. Måling, evaluering og revisjon, og 5. Kompetanse, kulturutvikling og kommunikasjon.

Konklusjon

Sykehusinnkjøp har vedtatt et sett av overordnede, styrende dokumenter innen informasjonssikkerhet og personvern, og det gjennomføres generelle opplærings-aktiviteter innen temaet. De styrende dokumentene er imidlertid i liten grad tilpasset foretakets størrelse, risiko og egenart, ettersom de ikke knyttes til foretakets leveranser, prosesser og informasjonstyper. Beskrivelser av roller og ansvar har svakheter, og det mangler, eller er mangler ved, prosessbeskrivelser for sentrale aktiviteter i internkontrollen.

Anbefalinger

Internrevisjonen anbefaler Sykehusinnkjøp å:

1. Tilpasse styrende dokumenter til foretakets størrelse, risiko og egenart.
2. Påse at alle sentrale rolle- og stillingsbeskrivelser innen informasjonssikkerhet og personvern er beskrevet.
3. Påse at revidert utgave av beredskaps- og kriseplan omhandler informasjons-sikkerhet og personvern.
4. Prioritere fastsetting av nivå for akseptabel risiko for konfidensialitet, integritet, tilgjengelighet og robusthet, jf. styresak 56/2022.
5. Etablere prosessbeskrivelse for forvaltning av databehandleravtaler.
6. Etablere prosessbeskrivelse for forvaltning av protokoll over behandling av personopplysninger.
7. Inngå databehandleravtale der det mangler, og revidere/oppdatere databehandleravtaler inngått før personopplysningsloven ble endret i juli 2018.
8. Etablere og/eller revidere prosessbeskrivelse for sentrale aktiviteter i internkontrollen for informasjonssikkerhet og personvern, herunder: risiko- og sårbarhetsanalyser, personvernkonsekvensutredninger, risikohåndtering, gjennomføring av sikkerhetstiltak, og ledelsens gjennomgåelse.

1 Innledning

Denne rapporten er utarbeidet etter internrevisjon i Sykehusinnkjøp HF (Sykehusinnkjøp) i perioden april til november 2022. Internrevisor Christin Ilstad har vært oppdragsleder og revisjonssjef Janny Helene Aasen har hatt det overordnede ansvaret.

Revisjonen har bestått av:

- Melding om internrevisjon sendt 08.04.2022
- Dokumentgjennomgang av innhentede dokumenter
- Intervju med til sammen 10 personer i øverste ledelse, inkludert informasjonssikkerhetsleder, personvernombud og juridisk rådgiver personvern
- Oppsummeringsmøte 20.10.2022
- Rapportutkast sendt 11.11.2022, tilbakemelding mottatt 02.12.2022

1.1 Bakgrunn

Sykehusinnkjøp utøver en spesialisert og profesjonell innkjøpstjeneste for spesialist-helsetjenesten. Tjenesteproduksjonen er i stor grad digitalisert, noe som innebærer krav om god internkontroll for informasjonssikkerhet og personvern for å håndtere risiko.

Styret i Sykehusinnkjøp bestilte i sak 59/2017 etablering av internkontroll for informasjonssikkerhet i virksomheten, og etableringen ble satt i gang i slutten av 2017. Styret har blitt orientert om status for gjennomføring i 2017, 2018, 2019 og 2021. I oppdragsdokumentet 2019 punkt f) Informasjonssikkerhet og personvern, ble det understreket at helseforetaket skal ha et styringssystem for informasjonssikkerhet, og at kompetansen om digital sårbarhet skal styrkes blant egne ansatte. I styresak 115/2021, Risikovurderinger og tiltaksarbeid II-2021, ble personvernområdet vurdert til høy risikoscore.

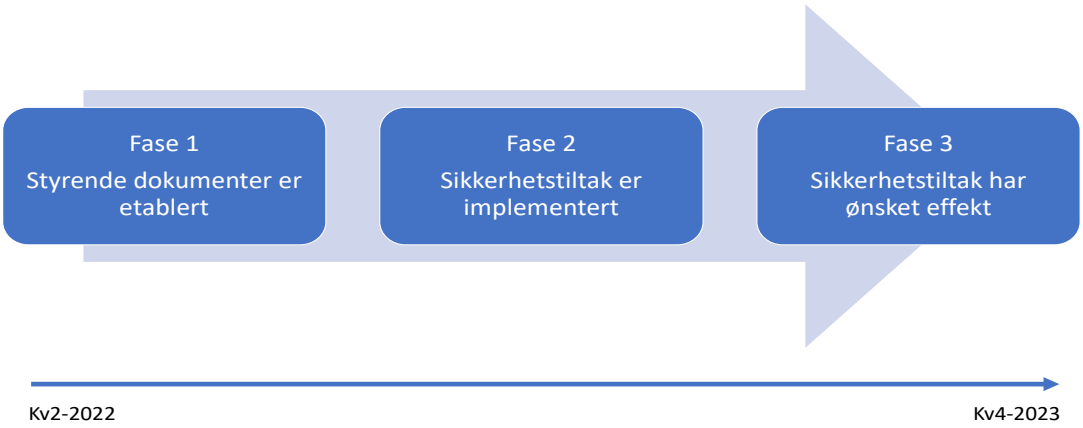
I ledermøtesak 58/2021 ble et sett av styrende dokumenter i System for informasjonssikkerhet og personvern første gang vedtatt, men på grunn av større endringer i de samme dokumentene gjennomførte ledergruppen en ny gjennomgang og godkjenning av dokumentene i sak 38/2022, med gyldighet fra 1. mai 2022. Disse dokumentene danner grunnlaget for denne revisjonen.

1.2 Overordnet formål og revisjonens tilnærming

Revisjonens overordnede formål er å bekrefte at foretaket har etablert en egnet internkontroll for informasjonssikkerhet og personvern.

Med bakgrunn i at arbeidet med å etablere internkontroll for informasjonssikkerhet og personvern i Sykehusinnkjøp fortsatt pågår, gjennomføres revisjonen i tre faser, jf. Figur 1. Denne revisjonsrapporten omhandler Fase 1.

Figur 1. Faseinndelt revisjon



2 Formål og revisjonskriterier

2.1 Formål med revisjonens fase 1

Formålet med revisjonen i fase 1 er å bekrefte at Sykehusinnkjøp har etablert styrende dokumenter for internkontroll for informasjonssikkerhet og personvern, og at disse er tilpasset foretakets størrelse, risiko og egenart.

2.2 Regelverk og veiledere

Følgende regelverk og veiledere er særlig aktuelle i denne revisjonen:

- LOV-2018-06-15-38 Lov om behandling av personopplysninger (personopplysningsloven)
- LOV-2018-06-01-24 Lov om nasjonal sikkerhet (sikkerhetsloven)
- FOR-2018-12-20-2053 Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften)
- LOV-2000-06-23-56 Lov om helsemessig og sosial beredskapsplan (helseberedskapsloven)
- FOR-2004-06-25-988 Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Digitaliseringsdirektoratet - Internkontroll i praksis – Informasjonssikkerhet: veiledningsmateriell for etablering og forbedring av internkontroll for informasjonssikkerhet.
- Norsk sikkerhetsmyndighet (NSM) - Grunnprinsipper for IKT-sikkerhet med tilknyttede tiltak.
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), versjon 6.0 med underliggende veiledere.
- ISO 27001: Internasjonal standard for implementering av et styringssystem for informasjonssikkerhet.

2.3 Fokusområder og revisjonskriterier

Fokusområdene som er lagt til grunn for internrevisjonens arbeid og vurderinger er basert på styringsaktivitetene beskrevet i Digitaliseringsdirektoratets veiledningsmateriell *Internkontroll i praksis – Informasjonssikkerhet* (heretter kalt *veiledningen*), ettersom Sykehusinnkjøp har lagt dette til grunn for sin etablering av internkontroll på området.

Revisjonskriteriene i fase 1 er innrettet mot å avklare i hvilken grad relevante styrende dokumenter er på plass:

1. Ledelsens styring og oppfølging
    a. Policy for informasjonssikkerhet og prinsipper for personvern er etablert.
    b. Roller og ansvar er beskrevet, og nøkkelpersoner er utnevnt.
    c. Fordeling av operativt ansvar innen informasjonssikkerhet og personvern mellom risikoeier, systemeier og tiltaksleverandør er beskrevet.
    d. Rutine for virksomhetsledelsens gjennomgang, som inkluderer informasjonssikkerhet og personvern, er etablert.
    e. Databehandleravtaler er inngått der det er nødvendig, og rutine for forvaltning er etablert.
    f. Protokoll over behandlinger av personopplysninger, og rutine for forvalting av protokollen er etablert.
    g. Foretaket har oversikt over IKT-systemer, infrastruktur og digitale tjenester.
    h. Foretaket har kartlagt eksterne krav i regelverk og avtaler.
    i. Foretaket har fastsatt nivå for akseptabel risiko for konfidensialitet, integritet, tilgjengelighet og robusthet.
    j. Foretaket har oversikt over nødvendige sikkerhetstiltak (fellessikring og tilleggssikring).
    k. Beredskaps- og kriseplaner for IKT-kritiske arbeidsoppgaver og funksjoner er utarbeidet.

2. Vurdering og håndtering av risiko
    a. Retningslinje for risikostyring knyttet til informasjonssikkerhet og personvern inkludert mal for risikovurdering er etablert.
    b. Prosedyrer og maler for håndtering av risiko inkludert eventuelle sikkerhetstiltak (beslutning, gjennomføring og oppfølging) er etablert.
    c. Det er etablert retningslinjer for oppfølging av risiko etter hendelser.

3. Hendelseshåndtering
    a. System for hendelses- og avvikshåndtering som dekker informasjonssikkerhet og personvern er etablert.

4. Måling, evaluering og revisjon
    a. Prosedyrer og maler for måling, evaluering og forbedring er definert.

5. Kompetanse og kulturutvikling
    a. Behov for opplæring er kartlagt.
    b. Opplæringsplan tilpasset foretakets behov foreligger.
    c. Styrende dokumenter blir kommunisert og tilgjengeliggjort.

3 Metoder

Følgende metoder er benyttet i revisjonsoppdraget:

Dokumentgjennomgang:

Dokumenter mottatt fra Sykehusinnkjøp, eller innhentet fra foretakets websider, er gjennomgått og vurdert opp mot revisjonskriteriene og benyttet i forberedelser til intervjuene. Se Vedlegg 1 – Dokumentoversikt.

Intervju:

Til sammen er ti personer intervjuet: administrerende direktør, direktør for virksomhetsstyring og økonomi, direktør for forretningsutvikling, organisasjonsdirektør, divisjonsdirektør - divisjon sør-øst, divisjonsdirektør – divisjon nasjonale tjenester og divisjon nord, divisjonsdirektør - divisjon vest, samt informasjonssikkerhetsleder, personvernombud og juridisk rådgiver personvern.

4 Observasjoner og vurderinger

4.1 Ledelsens styring og oppfølging

4.1.1 Observasjoner

4.1.1.1 Føringer, policy og prinsipper

I *veiledningen* står følgende: *Føringene bør si noe overordnet om formålet med informasjonsbehandlingen og informasjonssikkerhet, og hvilken betydning det har for virksomhetens oppgaver og tjenester. Omfang, struktur og ressursinnsats på styringen må være tilpasset virksomheten. Man må ha en overordnet oversikt over virksomheten, rammevilkårene for det den driver med og kunnskap om omgivelsene den befinner seg i. En slik oversikt bidrar til å gjøre virksomheten i stand til å få tilpasset utformingen av styringsaktivitetene til sitt behov.*

I dette delkapittelet omtales observasjoner knyttet til kriteriene 1 a, h og k, jf. kap. 2.4.

System for informasjonssikkerhet i Sykehusinnkjøp består av et hoveddokument og syv vedlegg. Under dette fokusområdet har vi sett på hoveddokumentet, vedlegg nummer 1, 3 og 5, samt vedleggene *Prinsipper for behandling av personopplysninger i Sykehusinnkjøp HF* og *Behandling av personopplysninger i Sykehusinnkjøp HF*.

Gjennomgang av disse viser at dokumentene er veldig generelle i sin karakter, og i liten grad tilpasset Sykehusinnkjøp sin egenart. Det fremkommer for eksempel ikke hva Sykehusinnkjøp sine kjerneaktiviteter er, ordene «anskaffelse» og «avtaleforvaltning» nevnes ikke, og det gis få beskrivelser av hvilke data eller informasjonstyper som trenger beskyttelse. Begrepet «foretaket» benyttes i all hovedsak fremfor «Sykehusinnkjøp». Flere av de vi intervjuet ga uttrykk for de samme refleksjonene.

Andre observasjoner vi har gjort er:

- *Vedlegg 1 Regelverk for informasjonssikkerhet* lister relevante lover, men uten å si noe om på hvilken måte de ulike regelverkene må tas hensyn til i etableringen av internkontrollen.
- *Vedlegg 3 Strategi for informasjonssikkerhet* gjengir tekst fra Nasjonal sikkerhetsmyndighet uten tilpasning til Sykehusinnkjøp sin egenart.
- *Vedlegg 5 Informasjonssikkerhetsinstruks* beskriver felles sikkerhetsregler for alle medarbeidere i foretaket, men kapittel 2.4 er imidlertid noe uferdig.

Det foreligger en krise- og beredskapsplan datert mars 2020. Trusselbildet relatert til informasjonssikkerhet og personvern omtales ikke i planen, men det henvises til de overordnede risiko- og sårbarhetsvurderingene av helse- og omsorgssektoren gjort av Helsedirektoratet i 2015, 2017 og i 2019. Dokumentet beskriver ikke hvordan Sykehusinnkjøp skal håndtere ulike type krisesituasjoner. I kapittel 4.2.3 står det at dette «må beskrives detaljert i situasjonsspesifikk plan/kriseplan». Internrevisjonen har fått opplyst at det jobbes med revidering av planen, for blant annet å ivareta det økende trusselbildet innen informasjonssikkerhet og personvern. Arbeidet er forsinket, men skal leveres i løpet av 2022. Tjenesteleverandører vil bli trukket inn i dette arbeidet.

4.1.1.2 Roller, ansvar og nøkkelpersonell

I *veiledningen* står følgende: *Ansvaret for informasjonssikkerhet og tilhørende internkontrollarbeid bør som hovedregel følge linjen. Det er sikring av måloppnåelse som er formålet med internkontrollen, og ansvaret for det ligger i linjen. For å understøtte både virksomhetsleder og linjen, må virksomheten tidlig etablere tilstrekkelige fellesfunksjoner, støttefunksjoner og samarbeidsgrupper. Sammen med linjen utgjør dette det som kalles sikkerhetsorganisasjonen i virksomheten.*

I dette delkapittelet omtales observasjoner knyttet til kriteriene 1 b og c, jf. kap. 2.4.

Dokumentet *Vedlegg 4 Organisering av informasjonssikkerhetsarbeidet* lister en rekke roller innen informasjonssikkerhet og personvern «som skal være etablert og beskrevet i styringssystemet» (Medulla). Internrevisjonen har etterspurt rollebeskrivelsene i Medulla tilhørende vedlegg 4, samt noen sentrale stillingsbeskrivelser. Vi konstaterer at ingen av rollene som er listet under er beskrevet i Medulla, men det foreligger enkelte beskrivelser i andre dokumenter:

- Informasjonssikkerhetsleder: Rollebeskrivelse er ikke utarbeidet. I *System for informasjonssikkerhet og personvern* fremkommer det at myndighet for

informasjonssikkerhet er delegert fra administrerende direktør til informasjonssikkerhetsleder.
- IT sjef: Stillingsbeskrivelse er ikke utarbeidet.
- Personvernombud: Rollen er beskrevet i dokumentet *Behandling av personopplysninger*, men beskrivelsen har enkelte mangler sammenlignet med *personopplysningslovens* artikkel 39 om å informere og gi råd, og å drive holdningsskapende tiltak og opplæring, jf. også Datatilsynets beskrivelse av personversombudets oppgaver.
- Juridisk rådgiver Personvern: Stillingsbeskrivelse omtaler ikke oppgaver innen personvern.
- Systemeier og systemansvarlig: Rollene er beskrevet i vedlegg 4. Det skilles ikke mellom situasjoner hvor Sykehusinnkjøp selv forvalter systemet og der hvor systemet forvaltes av andre.
- Virksomhetsarkitekt: Rollen er ikke beskrevet i vedlegg 4.

Rollen som informasjonssikkerhetsleder har blitt ivaretatt av IT-sjef. Internrevisjonen har i intervju diskutert faren for rollekonflikt. I oppsummeringsmøtet er vi blitt informert om at rollen som informasjonssikkerhetsleder er tildelt annen ressurs i oktober 2022.

Oppdatert fordeling av rollene som systemeier og systemansvarlig ble besluttet av ledergruppen i september 2022.

I *vedlegg 4, pkt. 4.4* er det beskrevet en modell for endringsstyring av IKT-tjenester, med et IKT-utviklingsråd og et IKT-sikkerhetsråd, og mandat er utarbeidet for begge rådene. Vi har merket oss at:

- IKT-sikkerhetsråd skal ivareta krav til informasjonssikkerhet og personvern i virksomhetens arbeidsprosesser og IKT-tjenester. Faste medlemmer er informasjonssikkerhetsleder, personvernombud og juridisk rådgiver personvern. Rådet er aktivt, men det jobbes med forbedringer av det operative arbeidet med innkalling, saksbehandling og referat.
- IKT-utviklingsråd skal ivareta samspillet mellom virksomhetens arbeidsprosesser og IKT-tjenester. Rådet gjennomførte sitt første møte den 3. oktober 2022.

4.1.1.3 Databehandleravtaler

Krav til databehandleravtale er regulert i *personopplysningsloven.* Datatilsynet[1] sier på sine nettsider følgende om databehandleravtaler: *«Alle virksomheter som benytter seg av en underleverandør har plikt til å ha en databehandleravtale. Den skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysningene.»*

I dette delkapittelet omtales observasjoner knyttet til kriterium 1 e, jf. kap. 2.4.

[1] https://www.datatilsynet.no/om-datatilsynet/oppgaver/

Sykehusinnkjøp har utarbeidet oversikt over alle databehandleravtaler og status på disse. Vi har fått opplyst at oversikten vedlikeholdes av informasjonssikkerhetsleder. Oversikten viser at databehandleravtalene med Sykehuspartner HF og Helse Vest IKT AS har status «Utgått». I intervju er det opplyst at det pågår reforhandling med Sykehuspartner HF. Når det gjelder Helse Vest IKT AS ble det opplyst at ansvars- og oppgavefordelingen er definert i en samarbeidsavtale, ikke en databehandleravtale, og at denne samarbeidsavtalen er under reforhandling.

Ved gjennomgang av tilsendte databehandleravtaler med Helse Nord IKT HF og Sykehuspartner HF, ser internrevisjonen at disse i stor grad tilfredsstiller minstekrav til innhold. De er imidlertid basert på ulike maler med ulikt detaljeringsnivå. Begge avtaler er fra begynnelsen av 2018, og er dermed inngått i forkant av at ny personopplysnings-lov trådde i kraft. I intervju er det opplyst at alle databehandleravtaler har behov for oppdatering, og at dette vil bli prioritert fremover.

Ved sammenligning av *Oversikt over databehandleravtaler* med dokumentet *Applikasjonstjenester,* hvor personopplysningsklassen er vurdert til «Særlig» eller «Generell», konstaterer internrevisjonen at enkelte databehandleravtaler mangler, noe som også er bekreftet i intervju.

Det foreligger ikke en prosessbeskrivelse for forvaltning av databehandleravtaler. Dokumentet *Behandling av personopplysninger* sier at det er et «lederansvar å påse at det inngås databehandleravtaler». I dokumentet *Vedlegg 4 Organisering av sikkerhetsarbeidet* står det at systemeier skal «bidra til at det inngås skriftlige databehandleravtaler», mens systemansvarlig skal «sikre at avtaler er oppdaterte». Sykehusinnkjøp har videre flere systemeiere og systemansvarlige inn mot samme IKT-leverandør, men det fremkommer ikke av rollebeskrivelsene hvordan ansvaret for databehandleravtaler skal håndteres i slike tilfeller.

4.1.1.4 Protokoll over behandling av personopplysninger

Krav til protokoll over behandling av personopplysninger er regulert i *personopplysningsloven.* Datatilsynet sier på sine nettsider følgende om protokollen: *«Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktivitetene de har ansvar for».* Protokollen skal kunne legges frem på anmodning fra tilsynsmyndigheten.

I dette delkapittelet omtales observasjoner knyttet til kriterium 1 f, jf. kap. 2.4.

Sykehusinnkjøp har etablert en protokoll over behandling av personopplysninger basert på Datatilsynets mal. Gjennom intervju er det opplyst at protokollen forvaltes av informasjonssikkerhetsleder. Det er også opplyst at personvernombud og juridisk rådgiver personvern ikke har vært involvert i utarbeidelse eller kontroll av protokollen. I oppsummeringsmøtet den 20. oktober ble det informert om at protokollen har vært fremlagt for IKT-sikkerhetsråd.

Det foreligger ikke en prosessbeskrivelse for forvaltning av protokollen. Dokumentet *Behandling av personopplysninger* sier imidlertid at det er et «lederansvar å sørge for at det føres protokoll over behandling av personopplysninger innenfor sine respektive ansvarsområder».

4.1.1.5 Informasjonstyper, risikonivå og sikkerhetstiltak

I *veiledningen* står følgende: *For at en risikoeier skal kunne arbeide effektivt med informasjonssikkerhet på sitt ansvarsområde, må vedkommende ha god oversikt over hvilke oppgaver og tjenester som utføres, og informasjonsbehandlingen i disse (...). Som del av risikovurderingen identifiseres konkrete risikoer, risikoene analyseres mht. konsekvens, sannsynlighet og risikonivå, og det vurderes om risikoen er akseptabel, eller om risikoen må håndteres gjennom sikkerhetstiltak.*

I dette delkapittelet omtales observasjoner knyttet til kriteriene 1 g, i og j, jf. kap. 2.4.

I dokumentet *Vedlegg 2 Sikkerhetsmål og akseptabel risiko for informasjonssikkerhet* fremkommer det at formålet «er å etablere sikkerhetsmål og nivå for akseptabel risiko». Gjennomgang av dokumentet viser at det inneholder generelle beskrivelser som ikke er tilpasset Sykehusinnkjøp sin virksomhet og egenart. I styresak 56/2022og i intervju er det opplyst at kartlegging av typiske oppgave- og informasjonstyper, beskrevet som «virksomhetens leveranser og tjenester», med tilhørende klassifisering og fastsetting av nivå for akseptabel risiko for konfidensialitet, integritet, tilgjengelighet og robusthet gjenstår. Resultatet fra dette arbeidet vil gi grunnlag for å beslutte, og få oversikt over, nødvendige sikkerhetstiltak. Det er opplyst at disse aktivitetene vil skje innen utgangen av 2022, og i etterkant av at nye systemeiere er operative (jf. 4.1.1.2). Informasjonssikkerhetsleder har imidlertid gjort en foreløpig klassifisering, som fremkommer i dokumentet *Applikasjonstjenester*. Internrevisjonen har også fått opplyst at det gjenstår å utarbeide operative prosessbeskrivelser for gjennomføring av sikkerhetstiltak.

4.1.2 Internrevisjonens vurderinger

Internrevisjonen vurderer det som en svakhet at de styrende dokumentene for internkontroll for informasjonssikkerhet og personvern i liten grad er tilpasset Sykehusinnkjøps størrelse, risiko og egenart, i og med at de ikke knyttes til foretakets leveranser, prosesser og informasjonstyper.

Det er uheldig at beskrivelser av roller og ansvar til dels mangler, eller er mangelfulle, hva angår tydelighet på ansvar innen informasjonssikkerhet og personvern. Internrevisjonen anser det imidlertid som positivt at rollen som informasjons-sikkerhetsleder er høsten 2022 tildelt en annen ressurs enn IT-sjef for å redusere risikoen for rollekonflikter. Det er videre positivt at IKT-utviklingsråd er etablert, og at det jobbes med forbedringer av det operative arbeidet i IKT-sikkerhetsråd.

Vi vurderer at det er en svakhet at Sykehusinnkjøp ikke har kartlagt oppgave- og informasjonstyper, med tilhørende klassifisering og fastsetting av nivå for akseptabel risiko. Dermed er grunnlaget for å beslutte nødvendige sikkerhetstiltak mangelfullt.

Det er uheldig at Sykehusinnkjøp mangler, har mangelfulle eller utgåtte databehandleravtaler for sentrale deler av sin drift, og at det ikke er utarbeidet prosessbeskrivelser for forvaltning av databehandleravtaler og for forvaltning av protokoll over behandling av personopplysninger.

4.2 Vurdering og håndtering av risiko

I *veiledningen* står følgende: *Vurdering av risiko er «hjertet» i internkontrollen (…). Innen informasjonssikkerhet og personvern handler risiko primært om operasjonell risiko – hva som kan skje ved gjennomføring av oppgaver, leveranse av tjenester og bruk av digitale systemer. Håndtering av risiko er «hendene» i internkontrollen. Det handler om å velge blant flere alternativer for å behandle risiko (redusere, unngå, dele eller akseptere), og iverksette og forvalte det som blir besluttet.*

4.2.1 Observasjoner

I dette delkapittelet omtales observasjoner knyttet til kriteriene 2 a, b og c, jf. kap. 2.4.

Sykehusinnkjøp har en beskrivelse av risikostyringsprosessen, som inkluderer vurderinger både på strategisk nivå og enhetsnivå, *Utfør helhetlig risikostyring*. Det fremkommer imidlertid ikke at informasjonssikkerhet og personvern skal inkluderes i risikovurderingen.

Gjennom intervju og i styresak 56/2022, har internrevisjonen fått informasjon om at risikovurderingen gjøres hvert tertial. Informasjonssikkerhet og personvern er identifisert som et risikoområde, og er dermed med i vurderingene. Det ble likevel uttrykt behov for å konkretisere hvordan internkontroll for informasjonssikkerhet og personvern skal inkluderes fremover, og behov for å involvere tjenesteleverandører.

Vi har også fått opplyst i intervju at det mangler prosessbeskrivelser med maler for personvernkonsekvensutredning (DPIA) og for risiko- og sårbarhetsanalyser (ROS), og at DPIA og ROS i liten grad gjennomføres. I følge dokumentet *Behandling av personopplysninger* er gjennomføring av DPIA og ROS et lederansvar. Det fremkommer også at juridisk avdeling har hovedansvar for å utføre DPIA der dette er nødvendig, uten at det er tydelig hvem som skal initiere arbeidet. I oppsummeringsmøtet den 20. oktober ble det opplyst at Sykehusinnkjøp skal benytte e-helsedirektoratets mal for DPIA, men at det gjenstår å dokumentere dette i en prosessbeskrivelse.

I dokumentet *Behandling av personopplysninger* fremkommer det at en eventuell tidligere DPIA må revurderes ved avvik i behandling av personopplysninger. Det er imidlertid ikke etablert en prosessbeskrivelse for revurdering knyttet til informasjons-sikkerhet av risiko etter hendelser, men internrevisjonen har fått opplyst at ITIL-

rammeverket[2] legges til grunn. Det gjøres gjennomganger i etterkant, og her involveres tjenesteleverandør når dette er aktuelt.

4.2.2 Internrevisjonens vurderinger

Internrevisjonen vurderer det som en svakhet at prosessbeskrivelsen for risikostyring på foretaks- og enhetsnivå ikke er tydelig på at informasjonssikkerhet og personvern skal inkluderes, og at det mangler prosessbeskrivelser for personvernkonsekvens-utredning og for risiko- og sårbarhetsanalyser.

4.3 Hendelseshåndtering

I *veiledningen* står følgende: *Overvåking og hendelseshåndtering er «vakta» i internkontrollen (…). Man avdekker ikke alt som kan skje i en risikovurdering, og det er sjeldent økonomisk forsvarlig å forsøke å forhindre alle uheldige hendelser. Som del av risikohåndteringen blir det derfor etablert tiltak som har som formål å systematisk oppdage, håndtere og redusere konsekvensene av informasjonssikkerhetshendelser.*

4.3.1 Observasjoner

I dette delkapittelet omtales observasjoner knyttet til kriterium 3 a, jf. kap. 2.4.

Sykehusinnkjøp har en prosessbeskrivelse for registrering og håndtering av prosessavvik i Medulla, *Registrer og håndter prosessavvik*. Det fremkommer ikke spesifikt at avvik knyttet til informasjonssikkerhet og personvern er inkludert. Dokumentet *Behandling av personopplysninger* oppgir at Medulla skal benyttes som system for registrering og håndtering av avvik innen personvern, men det fremkommer ikke hvem som har ansvar for håndtering av meldte avvik.

I intervjuer framkom følgende om hvordan avvik relatert til informasjonssikkerhet og personvern blir meldt:

- IKT-Support mottar avvik som gjelder informasjonssikkerhet via e-post.
- Personvernombudet mottar avvik relatert til personvern og behandler disse i samarbeid med juridisk rådgiver personvern og andre berørte.

4.3.2 Internrevisjonens vurderinger

Internrevisjonen vurderer det som uklart hvordan avvik eller forbedringsforslag relatert til informasjonssikkerhet og personvern skal meldes og håndteres.

4.4 Måling, evaluering og revisjon

I *veiledningen* står følgende: *Måling, evaluering og revisjon er «kontrolløren» i internkontrollen. Formålet er å gi ledere bedre kunnskap om tilstanden på eget*

[2] **Information Technology Infrastructure Library** (**ITIL**) er et rammeverk eller antologi for kvalitetssikring av leveranse, drift og støtte innen IT-sektoren

ansvarsområde (...). Slik kunnskap oppnås gjennom ulike kombinasjoner av målinger, undersøkelser, evalueringer og revisjoner, både ved etablering og bruk av tiltak.

4.4.1 Observasjoner

I dette delkapittelet omtales observasjoner knyttet til kriterium 1 d og 4 a, jf. kap. 2.4.

I hoveddokumentet *Styringssystem for informasjonssikkerhet og personvern* fremkommer det at «*systemet skal inngå i foretakets internkontroll, hvor informasjonssikkerhet er eget fagområde som skal omfattes av: revisjon, avvikshåndtering og ledelsens gjennomgåelse*».

Sykehusinnkjøp har en prosessbeskrivelse for ledelsens gjennomgåelse, *Utfør ledelsens gjennomgåelse,* jf. blant annet NS ISO 9001:2015. Det fremkommer ikke spesifikt av prosessbeskrivelsen at internkontroll for informasjonssikkerhet og personvern skal omfattes av ledelsens gjennomgang, jf. krav i *Virksomhetssikkerhetsforskriften* og anbefaling i *veiledningen*. Ledelsens gjennomgåelse gjennomføres to ganger per år, men internkontroll for informasjonssikkerhet og personvern er per nå ikke eksplisitt adressert. Vi har fått opplyst at eventuelle avvik som er registrert tas med i vurderingene.

Gjennom intervju fremkommer det at Sykehusinnkjøp har en ambisjon om årlig revisjon av styringssystemet for informasjonssikkerhet og personvern, og at temaet vil inngå i ledelsens gjennomgåelse fremover.

Vi har videre fått opplyst at Sykehusinnkjøp ikke enda har vurdert å etablere egne måleindikatorer for informasjonssikkerhet og personvern.

4.4.2 Internrevisjonens vurderinger

Internrevisjonen vurderer det som en svakhet at prosessbeskrivelsen *Utfør ledelsens gjennomgåelse* ikke er tydelig på at internkontroll for informasjonssikkerhet og personvern skal omfattes av ledelsens gjennomgang, jf. krav i *Virksomhetssikkerhets-forskriften* og anbefaling i *veiledningen.*

Veldefinerte måleindikatorer kan gi ledelsen verdifull styringsinformasjon som grunnlag for å vurdere om prosesser fungerer hensiktsmessig, eller om det er behov for tiltak. Internrevisjonen vurderer at Sykehusinnkjøp med fordel kan ta stilling om det skal etableres måleindikatorer for informasjonssikkerhet og personvern.

4.5 Kompetanse, kulturutvikling og kommunikasjon

I *veiledningen* står følgende: *Kompetanse- og kulturutvikling er «læreren» i internkontrollen. Tilstrekkelig kompetanse og god sikkerhetskultur er nødvendig for at styring av informasjonssikkerhet skal fungere. Kommunikasjon er «limet» i internkontrollen. God kommunikasjon legger til rette for læring, er essensielt for hendelseshåndtering og er det som gjør en virksomhet i stand til å jobbe samlet med informasjonssikkerheten.*

4.5.1 Observasjoner

I dette delkapittelet omtales observasjoner knyttet til kriterium 5 a, b og c, jf. kap. 2.4.

Internrevisjonen har fått opplyst at det gjennomføres obligatoriske introduksjonskurs for nyansatte, og oppfriskningskurs for eksisterende ansatte, som begge inkluderer tematikk innen informasjonssikkerhet og personvern. Det ble også gjennomført obligatoriske kurs på tematikken under *Sikkerhetsmåneden* i oktober 2021.

Det gjennomføres i tillegg obligatoriske workshops ledet av juridisk rådgiver personvern. Vi har fått opplyst at workshopene er praktisk rettet mot etterlevelse av krav og dilemmaer relatert til personvern, og at deltakerne opplever disse som nyttige.

Det finnes ingen oversikt over om alle har gjennomført obligatoriske kurs/workshops, men det planlegges å innføre et verktøy som vil legge til rette for dette fremover.

I arbeidet med kompetanse og kulturutvikling innen informasjonssikkerhet og personvern har Sykehusinnkjøp lagt til grunn at kompetansebygging er nødvendig for alle ansatte. Det er gjennomført en generell kompetansekartlegging, som internrevisjonen oppfatter vil danne grunnlag for å utarbeide flere tiltak og planer for kompetansebygging fremover.

I tillegg til ovennevnte kursaktiviteter/workshops har vi fått opplyst at informasjon om arbeidet med etablering av internkontrollen gis gjennom intranett og gjennom digitale allmøter.

4.5.2 Internrevisjonens vurderinger

Internrevisjonen vurderer at Sykehusinnkjøp gjennomfører tilfredsstillende opplærings- og informasjonsaktiviteter i denne fasen av etableringen av internkontroll for informasjonssikkerhet og personvern, men foretaket kan med fordel dokumentere at obligatoriske kursaktiviteter blir gjennomført.

5 Konklusjon og anbefalinger

5.1 Konklusjon

Sykehusinnkjøp har vedtatt et sett av overordnede, styrende dokumenter innen informasjonssikkerhet og personvern, og det gjennomføres generelle opplærings-aktiviteter innen temaet. De styrende dokumentene er imidlertid i liten grad tilpasset foretakets størrelse, risiko og egenart, ettersom de ikke knyttes til foretakets leveranser, prosesser og informasjonstyper. Beskrivelser av roller og ansvar har svakheter, og det mangler eller er mangler ved prosessbeskrivelser for sentrale aktiviteter i internkontrollen.

5.2 Anbefalinger

Internrevisjonen anbefaler Sykehusinnkjøp å:

1. Tilpasse styrende dokumenter til foretakets størrelse, risiko og egenart.
2. Påse at alle sentrale rolle- og stillingsbeskrivelser innen informasjonssikkerhet og personvern er beskrevet.
3. Påse at revidert utgave av beredskaps- og kriseplan omhandler informasjons-sikkerhet og personvern.
4. Prioritere fastsetting av nivå for akseptabel risiko for konfidensialitet, integritet, tilgjengelighet og robusthet, jf. styresak 56/2022.
5. Etablere prosessbeskrivelse for forvaltning av databehandleravtaler.
6. Etablere prosessbeskrivelse for forvaltning av protokoll over behandling av personopplysninger.
7. Inngå databehandleravtale der det mangler, og revidere/oppdatere databehandleravtaler inngått før personopplysningsloven ble endret i juli 2018.
8. Etablere og/eller revidere prosessbeskrivelser for sentrale aktiviteter i internkontrollen for informasjonssikkerhet og personvern, herunder: risiko- og sårbarhetsanalyser, personvernkonsekvensutredninger, risikohåndtering, gjennomføring av sikkerhetstiltak, og ledelsens gjennomgåelse.

Vedlegg 1 - Dokumentoversikt

Dokumenter som er gjennomgått i forbindelse med revisjonen listes under.

Styresaker Sykehusinnkjøp:

- Styresak 54-2022 Risikovurderinger og tiltaksarbeid per 1. tertial 2022 og ledelsens gjennomgåelse per 2. kvartal 2022
- Styresak 56-2022 Status informasjonssikkerhet og personvern

Foretaksinterne dokumenter:

- System for informasjonssikkerhet og personvern, mottatt 28.04.2022, ver. 1.0:
  - System for informasjonssikkerhet og personvern (hoveddokument), ver. 1.0
  - Vedlegg 1 Regelverk for informasjonssikkerhet, ver. 1.0
  - Vedlegg 2 Sikkerhetsmål og akseptabel risiko for informasjonssikkerhet, ver. 1.0
  - Vedlegg 3 Strategi for informasjonssikkerhet, ver. 1.0
  - Vedlegg 4 Organisering av informasjonssikkerhetsarbeidet, ver. 1.0
  - Vedlegg 5 Informasjonssikkerhetsinstruks, ver. 1.0
  - Prinsipper for behandling av personopplysninger i Sykehusinnkjøp HF, ver. 1.0
  - Behandling av personopplysninger i Sykehusinnkjøp HF, ver. 1.2
  - Mandat IKT-sikkerhetsråd, ver. 1.0
  - Mandat IKT-utviklingsråd, ver. 1.0
- Oversikt over databehandleravtaler, mottatt 28.04.2022
- Databehandleravtale Helse Nord IKT, signert februar 2018, mottatt 28.04.2022
- Bilag til Helse Nord IKT behandleravtale, mottatt 05.10.2022
- Databehandleravtale Sykehuspartner, signert mai 2018, mottatt 28.04.2022
- Protokoll over behandling av personopplysninger, mottatt 28.04.2022
- IKT-Arkitektur, mottatt 28.04.2022
- Applikasjonstjenester, mottatt 28.04.2022
- IKT-infrastruktur, mottatt 28.04.2022
- IKT-tjenestekatalog, mottatt 28.04.2022
- Arbeidsoppgaver juridisk rådgiver, mottatt 12.09.2022
- Stillingsbeskrivelser for organisasjonsdirektør, direktør for økonomi og virksomhetsstyring og direktør for forretningsstyring, mottatt 15.09.2022
- Rollebeskrivelser i Medulla tilhørende vedlegg, mottatt 15.09.2022
- Oppdatert fordeling av systemeierrollen og prosesseierrollen per september 2022, mottatt 05.10.2022
- Organisasjonskart Sykehusinnkjøp HF, mottatt 05.10.2022
- Prosessbeskrivelse «Utfør ledelsens gjennomgåelse», rev. 3, mottatt 05.10.2022
- Prosessbeskrivelse «Utfør helhetlig risikostyring», rev. 1, mottatt 05.10.2022
- Prosessbeskrivelse «Registrer og håndter prosessavvik», rev. 2, mottatt 05.10.2022
- Krise og beredskapsplan for Sykehusinnkjøp HF, ver. 1.0, mottatt 05.10.2022
- Referat IKT-utviklingsråd 03.10.2022, utkast, mottatt 03.11.2022