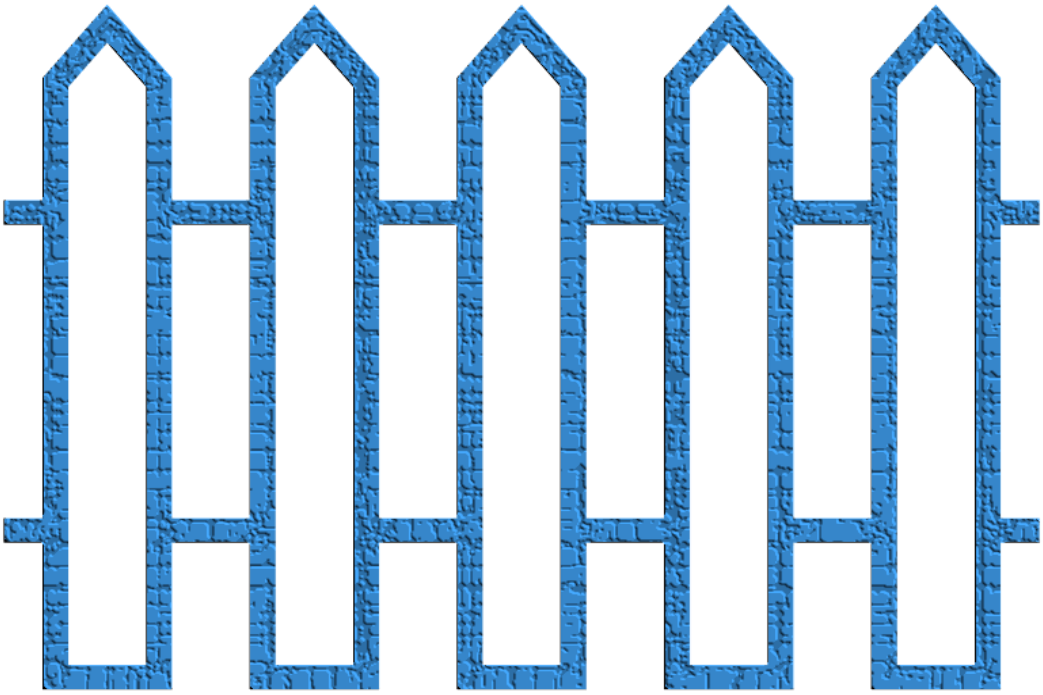
Internrevisjonen

INFORMASJONSSIKKERHEIT I HELSE VEST

Helse Vest RHF, desember 2024



Tittel:
Informasjonssikkerheit i Helse Vest

Publisert:
Desember 2024

Kontakt:
Internrevisjonen i Helse Vest RHF

Last ned rapporten på:
https://helse-vest.no/internrevisjon

Bilete:
Framside: Microsoft/Bjørn Munthe

Til lesarane av internrevisjonen sine rapportar:
Målgruppene for denne rapporten er styret og revisjonsutvalet på regionalt nivå, styra og ansvarlege i føretaka og institusjonane som har vore reviderte, og utførande fagfolk. Rapporten er eit offentleg dokument som skal vere tilgjengeleg òg for media og andre interesserte. Behova varierer, men dei som vil ha eit overblikk kan få det ved å lese innhaldslista og samandraget.

INNHALD

1 SAMANDRAG

Informasjonssikkerheit er avgjerande i helse- og omsorgssektoren som handterer store mengder sensitive data. Den raske digitaliseringa gir både nye moglegheiter og utfordringar. For å sikre at informasjonssikkerheita blir tilstrekkeleg ivareteken har internrevisjonen i denne revisjonen undersøkt om det er klare roller og ansvar for informasjonssikkerheit i Helse Vest, med særleg fokus på risikovurderingar og risikostyring. Vurderingane er i hovudsak basert på krava frå Normen, som byggjer på ulike lovkrav.

Dei siste åra har det vore aukande merksemd rundt informasjonssikkerheit, spesielt etter Riksrevisjonen sin rapport frå 2020 om førebygging av angrep mot IKT-system i helseføretaka. Dette har blant anna resultert i ein regional handlingsplan for informasjonssikkerheit, i tillegg var informasjonssikkerheit eit av topp fem risikoområde fram til april 2024, noko som viser at leiinga har hatt eit godt fokus på dette. Det regionale informasjonssikkerheitsutvalet er eit viktig fora for CISO-ane, og blir løfta fram som eit godt tiltak i føretaksgruppa. Dei administrerande direktørane er klare på at dei har det øvste ansvaret for informasjonssikkerheita, men revisjonen peiker likevel på at CISO sin forankring hos leiinga varierer mellom føretaka. Det er ikkje alle som har faste møtepunkt med administrerande direktør og/eller andre i leiinga. I tillegg er det variasjon i kor mykje ressursar føretaka har til oppgåvene CISO skal utføre.

Sjølv om rollene som dataansvarleg og databehandlar er avklara på eit overordna nivå, finst det indikasjonar på at ikkje alle relevante partar er fullt klar over kva desse rollene inneber. Føretaka må jobbe med å tydeleggjere rollene. Føretaka må også jobbe med å ha ei dokumentert oversikt over lokal IKT, som forskingsutstyr- og applikasjonar og medisinsk utstyr (MU). Helse Vest IKT ivaretar informasjonssikkerheit i felles IKT-infrastruktur, men frå føretaka si side er det ønskje om å ha betre innsyn i deira arbeid for å kunne vere sikker på sine oppgåver som dataansvarleg.

Ein vesentleg forbetringsmoglegheit er risikostyring, der føretaka gjer mange gode vurderingar (ROS-analysar), men manglar styring og oppfølging av risikoane. Det er få tiltaksplanar og oppfølgingsplanar. Det er vanskeleg å sjå kva som gjort for å redusera dei identifiserte risikoane. Eit anna problem er mangelen på eit aggregert risikobilete som kan gje betre innsikt til leiinga.

Tilrådingane er delt inn etter tema, og vi ser at nokre av føretaka allereie følgjer desse tilrådingane. For desse tilfella kan ein lese tilrådingane som oppmodingar om å fortsetje det pågåande arbeidet. Tilrådingane kan vere retta mot RHF-et åleine, HF-a (Helse Bergen, Helse Fonna, Helse Førde, Helse Stavanger, Sjukehusapoteka Vest) eller heile føretaksgruppa. I nokre tilfelle er dei også spesifikt retta mot Helse Vest IKT.

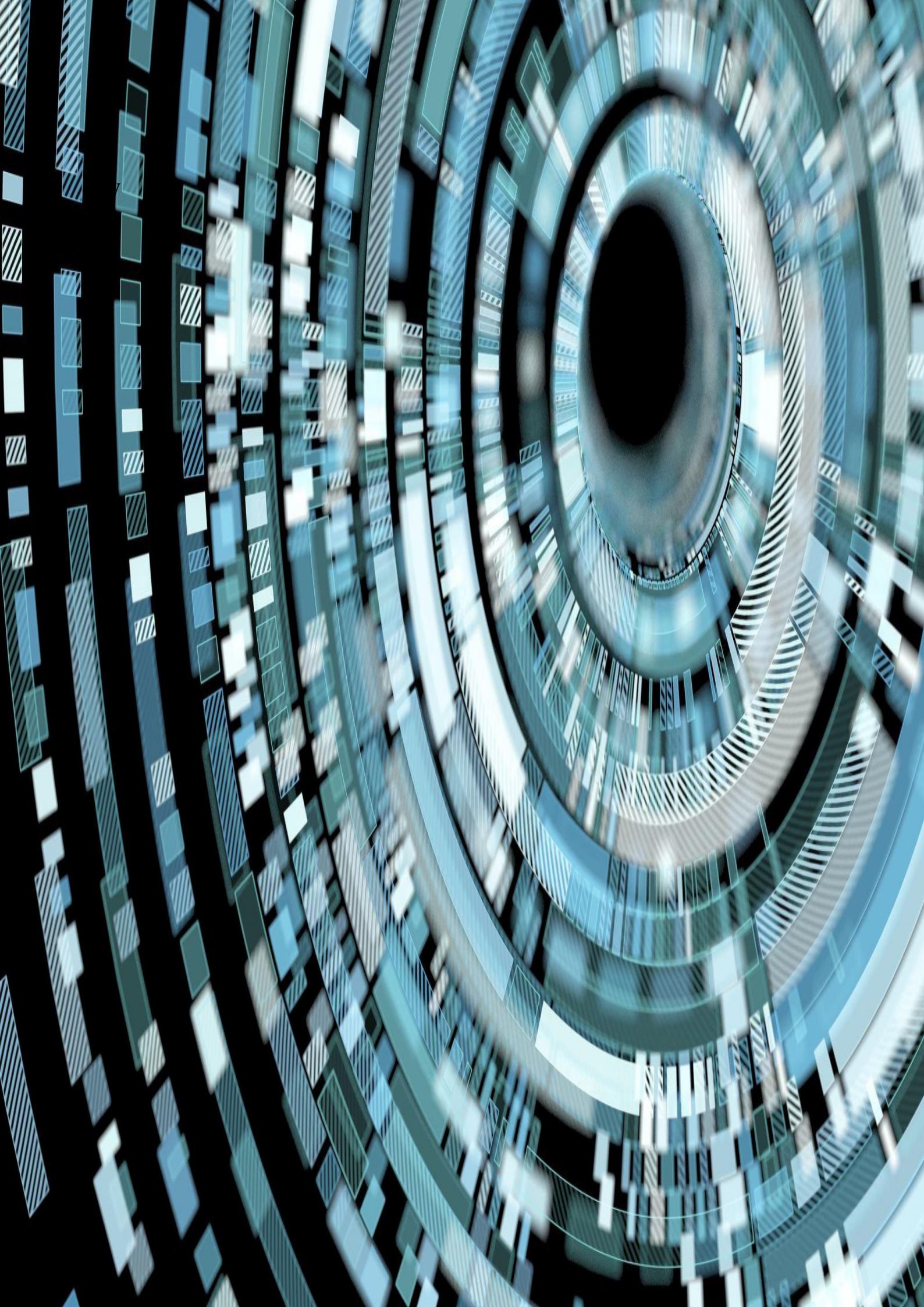
Når det gjeld øvste leiing og styre, bør RHF-et vurdere å nytte høvet til å stille eigne krav til informasjonssikkerheit i styringsdokument og andre relevante dokument. I tillegg bør RHF-et og HF-a etablere ei felles tilnærming til kva styresaker ein bør ha knytt til informasjonssikkerheit. Det er også tilrådd at føretaka gjennomfører ein eigen leiinga sin gjennomgang for informasjonssikkerheit, som bør handsamast som ei styresak. Tidspunktet for gjennomføringa, hyppigheita og innhaldet i denne gjennomgangen bør koordinerast i føretaksgruppa. Dette vil gjere det lettare å setje saman rapportane og nytte dei til vidare arbeid, samt sikre at rapportering om risiko knytt til informasjonssikkerheit skjer regelmessig, enten kvartalsvis eller tertialsvis, i tråd med den regionale handlingsplanen for informasjonssikkerheit. RHF-et og HF-a[1] bør også vurdere å utnytte administrerande direktør sin plass i styret til Helse Vest IKT, med innspel frå CISO til opne styresaker. Vidare bør føretaka sikre at det finst faste møtepunkt mellom CISO, administrerande direktør og andre i leiinga. Gjennom revisjonen ser vi at det er ulike synspunkt på om informasjonssikkerheit bør vere synleg i den nye styringsstrukturen for digitalisering. RHF-et bør løfte denne diskusjonen og endeleg avgjer om ein bør synleggjere det. Til slutt er det viktig at føretaka klargjer kva det inneber å vere dataansvarleg verksemd, og kva krav dette medfører.

Når det gjeld CISO sin rolle og ansvar, bør føretaka ha systematiske oversikter over statusen på innføringa av NSM sine grunnprinsipp. Dei bør også gjennomføre interne sikkerheitsrevisjonar, og aktivt arbeide med å ha oversikt over lokal IKT, medisinsk utstyr (MU) og teknisk utstyr (TU). Dette inkluderer førebyggande tiltak, som til dømes regionale fora for MU/TU og krav ved innkjøp.

Risikovurderingar og risikostyring er også eit viktig område. Føretaka bør arbeide med å forbetre metodikken knytt til risikovurderingar, og sørgje for at slike vurderingar blir gjennomførte når det er nødvendig. Det må sikrast at ROS-teamet har klare, skriftlege krav. Vidare bør føretaka vurdere om talet på deltakarar i ROS-analysane er riktig dimensjonert for å løyse oppgåva. Dei må også arbeide med korleis raude og gule risikoar blir handterte, inkludert oppfølging, evaluering av tiltak og oppdatering av ROS-analysane. Det er viktig at føretaka utarbeider planar for risikoreduserande tiltak, samt at desse planane blir kommuniserte på eit passande detaljnivå til leiinga. Føretaka bør dessutan etablere eit system som gir eit samla risikobilde på føretaksnivå. Helse Vest IKT og ROS-teamet bør klargjere og definere dei ulike rollene som er knytt til risikovurdering og risikostyring.

Desse tiltaka vil bidra til å styrkje informasjonssikkerheita i Helse Vest, og sikre betre kontroll med risiko og sårbarheiter. Internrevisjonen viser til kapittel 4 for punktvise tilrådingar frå revisjonen.

[1] Merk at administrerande direktør i Sjukehusapoteka Vest HF ikkje sit i styret til Helse Vest IKT AS, men alle administrerande direktørar i HF-a til sjukehusa



2 INNLEIING

2.1 Bakgrunn

Helse- og omsorgssektoren behandlar store mengder opplysningar som grunnlag for gode helse- og omsorgstenester, helseregistre, forsking og innovasjon. Eit utviklingstrekk i helse- og omsorgstenesta er den raske digitale utviklinga i samfunnet. Digitalisering kan bidra til meir tid til pasienten, at ein kan tilby tenester på nye måtar og at pasientar og brukarar kan delta og bidra meir i eigen behandling, i tillegg til at det kan spara ressursar i form av personell. Digitale løysingar og deling av helsedata gir eit behov for kompetanseutvikling hos personell og for å handtere digitale sikkerheitsutfordringar – som igjen blir styrka av globale hendingar og eit aukande digitalt trusselbilete.[2] Med bakgrunn i lovgiving, teknologisk utvikling og store enkelthendingar med mykje omtale har det i dei seinare åra vore auka merksemd rundt personvern og informasjonssikkerheit i helse- og omsorgssektoren[3]. Spesialisthelsetenesta utarbeider årleg ei felles trusselvurdering for å kartlegge det digitale trusselbildet, kor ein i 2023 sumerar opp med at ein kontinuerleg må styrkje mekanismar for å halde risikonivået stabilt[4], og i 2024 blir det peikt på at ein må jobba med fleire dimensjonar innan området for cybersikkerheit[5].

Det er ikkje berre i helse- og omsorgstenesta at informasjonssikkerheit har stor merksemd. The Institute of Internal Auditors (IIA) gir kvart år ut ein rapport (Risk in focus[6]) som sumerar opp topp 10 risikoar i verda, basert på resultata til ei undersøking som er distribuert til over 700 leiarar for internrevisjonar. Rapporten for 2024 har «Cyber security and data security» på første plass, det same har rapporten for 2025.

2.1.1 Riksrevisjonen

Riksrevisjonen har publisert to rapportar dei siste åra som er relevante for denne revisjonen; «Undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr» (Dokument 3:2 (2015:2016))[7] og «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-system» (Dokument 3:2 (2020-2021))[8]. Riksrevisjonen følgjer opp sistnemnte rapport i skrivande stund.

[2] Nasjonal helse- og samhandlingsplan 2024-2027 (Meld. St. 9 (2023–2024) (regjeringen.no))
[3] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse - Forord
[4] Trusselvurdering 2023 - Det digitale trusselbildet mot spesialisthelsetjenesten (helse-vest.no)
[5] Det digitale trusselbiletet mot spesialisthelsetenesta - Helse Vest IKT (helse-vest-ikt.no)
[6] Risk in Focus 2024 - IIA
[7] Undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr (riksrevisjonen.no)
[8] Dokument 3:2 (2020–2021) Rapport (riksrevisjonen.no)

Den første rapporten, «Undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr» offentleggjort i 2015, avdekte fleire kritiske manglar i helseføretaka si handtering av informasjonssikkerheit knytt til medisinsk-teknisk utstyr. Blant hovudfunna var at helseføretaka i liten grad hadde implementert nødvendige tiltak for å verne pasientinformasjon og sikre utstyret mot uautorisert tilgang og cyberangrep. Det blei påvist manglande risikovurderingar, utilstrekkelege sikkerheitsrutinar, og ein generell mangel på merksemd rundt dei spesifikke sikkerheitsutfordringane som følgjer med medisinsk-teknisk utstyr. Denne rapporten og saman med innstillinga til kontroll- og konstitusjonskomiteen (Innst. 186 S (2015-2016))[9] gav eit tydeleg signal om behovet for å betre informasjonssikkerheit i helseføretaka, spesielt med tanke på medisinsk-teknisk utstyr.

Den andre rapporten, «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer»[8], blei offentleggjort i 2020 og trakk tydelege linjer til rapporten som er omtalt over. Den gav ein grundig analyse av korleis norske helseføretak arbeider med å sikre sine IKT-system mot cyberangrep. Rapporten avdekkjer fleire utfordringar og manglar i helseføretaka sine sikkerheitstiltak, noko som set sensitive pasientdata og kritiske helsetenester i fare. Ein ser at samla sett trakk den nye rapporten linjer til den tidlegare rapporten ved å understreke at mens nokre forbetringar hadde skjedd, var framdrifta ikkje tilstrekkeleg rask eller omfattande. Riksrevisjonen konkluderte med at helseføretaka måtte intensivere sine innsatsar for å førebygge angrep mot IKT-system og betre informasjonssikkerheita, ikkje berre for medisinsk-teknisk utstyr, men i alle sine digitale system. Eit av dei mest framståande problema er mangelen på ein heilskapleg og systematisk tilnærming til informasjonssikkerheit. Det er stor variasjon i korleis dei ulike føretaka handterer og implementerer sikkerheitstiltak, noko som fører til at leiinga ved fleire helseføretak ikkje har tilstrekkeleg fokus på informasjonssikkerheit. Dette resulterer i manglande ressursar og prioritering på området. I tillegg er det mangel på gjennomgåande risikovurderingar og sikkerheitsstyringssystem. Mange helseføretak har ikkje oppdatert sine risikovurderingar, og det finst ikkje ei felles forståing av risikoar på tvers av organisasjonane. Dette gjer at sikkerheitstiltak ofte er reaktive snarare enn proaktive, noko som gjer helseføretaka sårbare for nye og uventa truslar.

For å betre førebygginga av angrep mot helseføretaka sine IKT-system, kjem Riksrevisjonen med fleire tilrådingar. Det er, blant anna, viktig at helseføretaka etablerer ein meir systematisk og heilskapleg tilnærming til informasjonssikkerheit, inkludert sterkare forankring hos leiinga. Regelmessige og omfattande risikovurderingar bør gjennomførast, og desse bør ligge til grunn for sikkerheitsarbeidet. Ein felles metode for risikovurdering bør etablerast for å sikre ei felles forståing av risikoar på tvers av helseføretaka.

I vår revisjonsrapport vil vi trekke parallellar til Riksrevisjonen sine rapportar, spesielt «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer»[8], både for å understreke funna, men òg vise utvikling frå rapportane blei offentleggjort og fram til vår revisjon.

[9] Innst. 186 S (2015–2016) - stortinget.no

Merk at vi berre vil trekke ut det som er relevant for vårt formål og våre problemstillingar, sjølv om det er mange moment i Riksrevisjonen sine rapportar som òg er viktige.

2.2 Formål og problemstillingar

Formålet med denne revisjonen er å undersøkje det er klare roller og ansvar for informasjonssikkerheit i Helse Vest, med særleg fokus på risikovurderingar og -styring.

Ut frå bakgrunn og formål vil prosjektet kartleggje og vurdere **følgjande problemstillingar**:

- Er det etablert roller og funksjoner for å ivareta ansvaret for informasjonssikkerheit i føretaksgruppa?
    - Er det tydeleg kven som er ansvarleg og kva oppgåver dei har og er ansvarlege for?
    - Har ein tilstrekkeleg med ressursar og kompetanse til å gjennomføre dei nødvendige oppgåvene som helseføretaka har krav om å utføre?

- Er det etablert koordinerte aktivitetar for å rettleie og kontrollere føretaka med omsyn til risiko knytt til informasjonssikkerheit?
    - Er det klare roller/ansvar knytt til risikostyring av informasjonssikkerheit?
    - Er det oversikt over system og teknologi i føretaka?
    - Har ein toleransegrenser for risiko, og er desse kommunisert i føretaka?
    - Finnes det ein standardmetode/prosess for risikovurdering i føretaksgruppa?
    - Har ein identifisert truslar, sårbarheiter og konsekvensar ved moglege uønskte hendingar?
    - Brukar ein risikovurderingar aktivt for å setje i gang tiltak for å redusere risikoane?
    - Har ein evalueringar av dei ulike risikoreduserande tiltaka?

- Korleis er øvste leiing si rolle innanfor informasjonssikkerheit under dette risikostyring?
    - Rapportering til leiinga (aggregert risikobilete)

2.3 Revisjonskriterium og metode

2.3.1 Revisjonskriterium

Revisjonskriterium er element som inneheld krav eller forventningar til revisjonsobjektet, og er brukt til å vurdere funna i dei undersøkingar som er gjennomført. Under lister vi opp dei mest sentrale revisjonskriterium som er nytta i denne revisjonen, men presiserer at lista ikkje er uttømmande.

Normen: Normen skal bidra til tilfredsstillande informasjonssikkerheit og personvern hos den enkelte verksemd, i felles system og infrastruktur, og i sektoren generelt[10]. Forskrift om standardar og nasjonale e-helseløysingar[11] pålegg verksemder som yter helse- og omsorgstenester etter spesialisthelsetenestelova å ta i bruk Helsenettet.

Helse Vest skal, gjennom å vere ein del av Norsk Helsenett[12], følgje Normen (Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren)[13]. Normen skal medverke til å etablere mekanismar der verksemdene kan ha gjensidig tillit til at behandling av helse- og personopplysningar blir gjennomførte på eit forsvarleg tryggingsnivå. Normen stiller krav som detaljerer og supplerer gjeldande regelverk[14]. Eit viktig mål i den gjeldande versjonen av Normen var å gjere den meir lesar- og brukarvennleg[3], og internrevisjonen har difor valt å referere til krava i Normen, framfor dei ulike lovkrava. Det kan vere krav som føretaka må etterleve knytt til både personvern og informasjonssikkerheit som ikkje kjem fram i Normen. Internrevisjonen vil påpeike at alle krava i Normen ikkje vil bli vurdert i denne i revisjonsrapporten, da det er avgrensa til formålet og problemstillingane.

Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipp for IKT-sikkerheit[15]: Føretaksgruppa har fått i oppdrag å følgje NSM sine grunnprinsipp for IKT-sikkerheit, ref. kap. 3.1.

Krav frå Helse- og omsorgsdepartementet (HOD) til RHF-et: RHF-et mottar oppdragsdokument normalt ein gong i året frå HOD med styringskrav[16]. Gjennom eit år er det òg føretaksmøte, kor HOD set rammer og mål for verksemda i føretaka[17].

2.3.2 Metode

Vi har gått gjennom ulike dokumenter, for eksempel rutinar, prosedyrar og styredokument. Vidare tok vi eit tilfeldig utval av risikoanalysar og gjekk gjennom desse. Det er gjennomført intervju med representantar frå Helse Vest RHF og dei fem helseføretaka, samt Helse Vest IKT. Intervjurespondentar omfattar administrerande direktørar, fagdirektørar, IKT-leiarar og leiarar for informasjonssikkerheit (heretter omtalt som CISO), samt enkelte rådgivarar. Vi har òg intervjua direktøren for e-helse i Helse Vest RHF. Vår samla vurdering er at metodebruk og kjeldetilfang har gitt eit tilstrekkeleg grunnlag til å svare på prosjektet sitt formål og problemstillingar.

[10] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Hva er Normen
[11] Forskrift om standarder og nasjonale e-helseløsninger - Lovdata
[12] Medlemskap i Helsenettet - Norsk helsenett (nhn.no)
[13] «Vilkår for medlemskap i helsenettet» - Norsk helsenett
[14] Om Normen - ehelse
[15] NSMs Grunnprinsipper for IKT-sikkerhet v2.1.pdf
[16] Oppdragsdokument - regjeringen.no
[17] Protokoller fra foretaksmøter - regjeringen.no

2.4 Omgrep og avgrensingar

2.4.1 Informasjonssikkerheit, personvern og pasienttryggleik

Informasjonssikkerheit og personvern er to omgrep som ofte blir brukt i samband med kvarandre, og det er ikkje utan grunn. Dei er nært knytte saman, men det er viktige skilnader mellom dei som ein må forstå og respektera.

Informasjonssikkerheit handlar om å verne informasjon mot uønskt tilgang, tap eller skade. Dette omfattar alle former for informasjon, uavhengig av om det er personopplysningar eller andre typar data. Omgrepet informasjonssikkerheit består av tre hovudpillarar, kjent som KIT-triaden: konfidensialitet, integritet og tilgjengelegheit[18].

I spesialisthelsetenesta betyr konfidensialitet at sensitive data, som pasientinformasjon, ikkje skal vere tilgjengeleg for uautoriserte, eller personell utan tenestleg behov. Alle tilsette, ikkje berre dei som behandlar pasientar, har eit ansvar for å overhalde teieplikta for å hindre at konfidensiell informasjon kjem på avvegar. Integritet handlar om at informasjonen som er lagra i helseføretaket sine system, skal vere korrekt og påliteleg. Feil eller uautoriserte endringar i slik informasjon kan få alvorlege konsekvensar, som at ein pasient får feil behandling. Tilgjengelegheit inneber at den nødvendige informasjonen alltid er tilgjengeleg når tilsette i helsevesenet treng den for å utføre sine arbeidsoppgåver. Informasjonssikkerheit omfattar også kravet om at all informasjon må bli lagra forsvarleg og ikkje bli delt med andre enn dei som har eit legitimt behandlingsansvar[19],[8].

I revisjonen vår vil vi nytte oss mest av omgrepet informasjonssikkerheit, men ser at dette overlappar med omgrepet IKT-sikkerheit. **IKT-sikkerheit** handlar om å beskytte IKT-system, samvirket mellom systema, tenestene som blir levert av systema, og informasjonen som ein behandlar i systema. Måla for IKT-sikkerheit er gjerne dei same som for informasjonssikkerheit. Ein skal beskytte informasjonen, og informasjonssystem, og soleis sikre at informasjonen ikkje blir endra utilsikta eller av uvedkomande og at den er tilgjengeleg ved behov[8].

Personvern fokuserer spesifikt på å beskytte individets rett til privatliv, retten til å bestemme over eigne personopplysningar og å sikre at personopplysningar blir behandla i samsvar med lovverket. I praksis inneber dette at personopplysningar skal bli behandla på ein lovleg, rettferdig og transparent måte, og at individet har visse rettar knytt til korleis opplysningane om dei sjølv blir behandla. Informasjonssikkerheit er derfor ein viktig del av det å sikre personvernet, men det er ikkje avgrensa til berre dette området.[20] Samtidig er det vanskeleg å ha godt personvern utan god informasjonssikkerheit i botn.

[18] Whitman, M. E. & Mattford, H. J. (2017). Principles of information security (6. Utg.). Cengage Learning.
[19] Direktoratet for e-Helse - Strategi for digital sikkerhet i helse- og omsorgssektoren - Vurdering av behov og innretning (IE-1064)
[20] Lov om behandling av personopplysninger (personopplysningsloven) - - Lovdata

Eit omgrep som knyter personvern og informasjonssikkerheit saman er **personopplysningssikkerheit**. Eit brot på personopplysningssikkerheita er i personvernforordninga definert som utilsikta eller ulovleg tilinkjegjering, tap, endring, ulovleg spreiing av eller tilgang til personopplysningar som er overført, lagra eller på annan måte behandla[21].

Pasienttryggleik handlar om at helseføretaka skal tilby helsetenester av høg kvalitet for å forhindre, førebygge og redusere uønskte hendingar eller skader som kan oppstå på grunn av svakheiter i helsesystemet. Det er avgjerande at pasientar ikkje blir utsett for skade som følgje av feil eller manglar[22]. Pasienttryggleik inkluderer også sikkerheit for dei digitale systema som helseføretaket nyttar, slik at alle pasientar får nødvendig helsehjelp[23].

Informasjonssikkerheit har ofte blitt sett på som eit teknisk problem for IT-avdelinga, mens pasienttryggleik har vore eit ansvar for helsepersonell. Det er viktig å forstå at informasjonssikkerheit ikkje berre er eit teknisk problem, men eit felles ansvar for alle tilsette, inkludert helsepersonell[24]. Eit brot på informasjonssikkerheita kan få alvorlege konsekvensar for pasientane, som at helsepersonell ikkje får tilgang til kritiske system og dermed ikkje kan gi nødvendig behandling[24]. Eit eksempel er frå universitetssjukehuset i Düsseldorf i 2020, der ein pasient mista livet på grunn av eit cyberangrep (ransomware)[25]. Helsetenesta er bygd på prinsippet om rett behandling, på rett stad, til rett tid (Meld. st. 47, 2009)[26]. For å oppnå dette må informasjonssikkerheit integrerast i alle ledd av helsetenester[24]. Trass i dette ser mange på informasjonssikkerheit som abstrakt, sidan brot på denne ikkje alltid fører til umiddelbare fysiske skadar. Likevel kan slike brot føre til alvorlege konsekvensar for både pasientens helse og vår tillit til helsevesenet.

2.4.2 Andre omgrep som blir brukt i revisjonen

CISO (Chief Information Security Officer): Leiar for informasjonssikkerheit i føretaket.

Føretaksgruppa: Alle føretaka i Helse Vest; Helse Vest RHF, Helse Bergen HF, Helse Fonna HF, Helse Førde HF, Helse Stavanger HF, Sjukehusapoteka Vest HF og Helse Vest IKT AS.

Informasjonssikkerheit: Omtalt i delkapittelet over. Handlar om å verne informasjon mot uønskt tilgang, tap eller skade.

Normen: Omtalt i kapittel 2.3.1. «Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren» er ein standard som fastset krav til informasjonssikkerheit og personvern.

[21] Hva er et brudd på personopplysningssikkerheten? | Datatilsynet
[22] Pasientsikkerhetsvisitter - Itryggehender (itryggehender24-7.no)
[23] Kvalitet, kvalitetsforbedring og pasientsikkerhet - Det medisinske fakultet (uio.no)
[24] Sunder, S. (2023). Informasjonssikkerhetskultur i spesialisthelsetjenesten - En sosio-teknisk casestudie av Akershus universitetssykehus, Masteroppgave i Informasjonssikkerhet, NTNU
[25] «Tysk kvinne døde etter ransomeware-angrep mot sykehus», Computerworld, 21. september 2020. https://www.cw.no/dataangrep-hacking-losepengevirus/tysk-kvinne-dode-etter-ransomeware-angrep-mot-sykehus/425156
[26] Meld. st. 47 (2009) Samhandlingsreformen, Rett behandling – på rett sted – til rett tid.

NSM sine grunnprinsipp for IKT-sikkerheit: Omtalt i kapittel 2.3.1. Det er ei samling med prinsipp og tiltak for å beskytte informasjonssystem mot uautorisert tilgang, skade eller misbruk[27].

Risikovurdering: Ein systematisk prosess for å identifisere, analysere og evaluere risikoar som kan påverke informasjonssystema. Risikovurdering inkluderer identifikasjon av truslar, sårbarheiter og konsekvensar[28].

Risikostyring: Prosessen med å planleggje, gjennomføre og evaluere tiltak for å handtere risikoar identifisert gjennom risikovurderingar. Risikostyring inkluderer å setje i verk tiltak for å redusere risiko, samt overvaking og rapportering av risikobiletet[29].

SU: Informasjonssikkerheitsutvalet i Helse Vest, sjå kapittel 3.2.2.

2.4.3 Avgrensingar

Revisjonen vil omfatte heile føretaksgruppa i Helse Vest; Helse Vest RHF, Helse Stavanger HF, Helse Fonna HF, Helse Bergen HF, Helse Førde HF, Sjukehusapoteka Vest HF og Helse Vest IKT. Revisjonen har avgrensingar som er nødvendige for å sikre fokus og gjennomføring innanfor dei gitte rammene i mandatet.

Denne revisjonen handlar om informasjonssikkerheit, og ikkje personvern. Sjølv om personvern er ein viktig del av det større bildet, vil denne revisjonen særleg sjå på korleis Helse Vest sikrar alle typar informasjon mot risikoar som kan true konfidensialitet, integritet og tilgjengelegheit. Denne avgrensinga er viktig for å kunne gjennomføre ein grundig og målretta revisjon. Formålet og problemstillingane handlar om overordna styring, kontroll og system – internrevisjonen vil for eksempel ikkje undersøkje detaljerte sikkerheitstiltak. Med dagens bruk av IKT er styring og kontroll med informasjonssikkerheita kritisk for dei fleste aktivitetar i ei verksemd. Det handlar om systematiske styringsaktivitetar som skal sørgje for at relevante risikoar blir vurdert, at nødvendige og formålstenlege sikkerheitstiltak blir etablert, og at det systematisk blir kontrollert og fylgt opp at tiltaka og styringsaktivitetane faktisk fungerer som venta.[30]

I revisjonen vil vi òg ha ei tidsmessig avgrensing ved å vurdere gjeldande praksis. Dette betyr at funna vil vere basert på noverande situasjon og tiltak. Samtidig vil vi trekkje linjene tilbake til tidlegare revisjonar, rapportar og dokument for å sjå korleis arbeidet har utvikla seg.

[27] Hva er NSMs grunnprinsipper for IKT-sikkerhet? - Nasjonal sikkerhetsmyndighet
[28] Risikovurdering (arbeidstilsynet.no)
[29] Veileder til samfunnssikkerhetsinstruksen - regjeringen.no
[30] Hvorfor styring av informasjonssikkerhet? | Digdir

2.5 Overordna om rollane som dataansvarleg og databehandlar i Helse Vest

Helse Vest IKT er eit aksjeselskap som er 100 % eigd av Helse Vest RHF. Ved slutten av 2023 var det 715 tilsette i føretaket på kontor i Førde, Bergen, Haugesund og Stavanger, inkludert mindre avdelingskontor på Voss, Odda, og Stord[31]. Helse Vest IKT sine kundar er både dei offentlege sjukehusa i Helse Vest, og fleire private leverandørar av helsetenester i regionen. I styret til Helse Vest IKT sit dei administrerande direktørane for Helse Førde HF, Helse Bergen HF, Helse Fonna HF og Helse Stavanger HF. I tillegg består styret av erfarne eksterne styremedlem, og dessutan representantar frå dei tilsette i Helse Vest IKT. Administrerande direktør i Helse Vest RHF er leiaren i styret. Merk at administrerande direktør i Sjukehusapoteka Vest HF ikkje sit i styret til Helse Vest IKT.

To sentrale roller for informasjonssikkerheit er dataansvarleg (behandlingsansvarleg i personvernforordninga) og databehandlar. I personvernforordninga artikkel 4 nr. 7 blir behandlingsansvarleg definert slik: *««behandlingsansvarlig» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett»*. Definisjonen i Normen er følgjande: «*Dataansvarlig er den som alene eller sammen med andre virksomheter bestemmer formålet med behandlingen av helse- og personopplysninger og hvilke midler som skal benyttes*»[32].

Personvernforordninga definerer databehandlar som «*en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige*» i artikkel 4 nr. 8. «*En databehandler er en virksomhet som behandler helse- og personopplysninger på vegne av dataansvarlig*»[33] er definisjonen i Normen.

Helse Vest RHF, har det overordna ansvaret – «sørgje-for-ansvaret» - for spesialisthelsetenestene i regionen, inkludert styring av informasjonssikkerheit. Kvart enkelt helseføretak har ansvar for sine eigne data og behandlinga av desse, noko som inneber at dei er **dataansvarlege** for dei pasient- og personopplysningane dei samlar inn. Som dataansvarlege må HF-a sørgje for at behandling av personopplysningar skjer i tråd med gjeldande lover og forskrifter inkludert helseregisterlova[34], personopplysningslova m/personvernforordninga[35], E-forvaltningsforskrifta[36] og pasientjournallova[37].

[31] Om Helse Vest IKT - Helse Vest IKT (helse-vest-ikt.no)
[32] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap. 2.2. Dataansvarliges ansvar
[33] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap. 2.3. Databehandlers ansvar
[34] Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) - Lovdata
[35] Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata
[36] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) - Lovdata
[37] Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) - Lovdata

Helseføretaka, som **dataansvarlege**, har eit sjølvstendig ansvar for at informasjonssikkerheita blir oppretthalden lokalt. Helseføretaka har eigne lokale IKT-løysingar som ikkje er del av Helse Vest IKT si forvalting. Dette omfattar for eksempel utstyr og system innanfor forsking, medisinsk utstyr (MU) og teknisk utstyr (TU).

Helse Vest IKT er **databehandlar**, og behandlar data på vegner av HF-a etter instruks frå dei dataansvarlege, jf. databehandlaravtalen mellom Helse Vest IKT og deira kundar[38]. Helse Vest IKT har ansvar og styringsmyndighet for å drifte felles IT-løysingar og infrastruktur som blir nytta av alle helseføretaka. Dette omfattar system som elektroniske pasientjournalar, e-post og andre IT-tenester som er nødvendige for dagleg drift. I tillegg har dei ansvar for overvaking av infrastrukturen, identifisering av sikkerheitshendingar, og å setje i verk tiltak for å hindre uautorisert tilgang eller tap av data.

Databehandlaravtalar[38] mellom den enkelte verksemd i Helse Vest og Helse Vest IKT regulerer forholdet mellom dataansvarleg og databehandlar. Avtalane sikrar at Helse Vest IKT set i verk nødvendige tekniske og organisatoriske tiltak for å verne personopplysningane. Samhandlinga mellom Helse Vest IKT som databehandlar og helseføretaka som dataansvarlege er avgjerande for å sikre at både teknologiske og organisatoriske tiltak til ei kvar tid møter krava til personvern og informasjonssikkerheit.

[38] eHåndbok - SLA bilag 14 - Databehandleravtale

3 ANALYSE

3.1 Forventingar frå RHF til helseføretaka og Helse Vest IKT

HOD har stilt krav til RHF-et om informasjonssikkerheit[39], og i styringsdokumenta for 2024 blir dette vidareformidla til både HF-a (kapittel 7.2[40]) og til Helse Vest IKT (kapittel 4.2[41]):

> «Det blir vist til tidlegare stilte krav om oppfølging av Riksrevisjonen sin revisjon av helseføretaka si førebygging av angrep mot sine IKT-system, jf. Dokument 3:2 (2020–2021) og til tidlegare krav om å arbeide systematisk med innføring av Nasjonal sikkerheitsmyndigheit (NSM) sine grunnprinsipp for IKT-sikkerheit. Det er viktig at helseføretaka fører vidare arbeidet med å følgje opp krava som blei stilt for 2023 om forebyggande tiltak og tiltak for å handtere og gjenoppbygge funksjon etter tilsikta eller utilsikta hendingar mot eigen infrastruktur, IKT-system og viktige verdiar.»

Med følgande punkt:

> «Helse Vest RHF ber helseføretaka, i samarbeid med Helse Vest IKT, om:
>
> - At tiltak for beskyttelse mot vondsinna dataangrep og truslar mot kritisk infrastruktur blir vidareutvikla i tråd med trusselbildet og basert på gjennomførte analysar av risiko- og sårbarheit»

RHF-et har gitt tydelege oppgåver knytt til informasjonssikkerheit til HF-a og Helse Vest IKT i styringsdokumenta i 2024 gjennom sitt «sørgje-for-ansvar», ref. kapittel 2.5. Det har i tillegg blitt stilt krav til informasjonssikkerheit tidlegare år, og spesielt etter at Riksrevisjonen publiserte rapporten «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-system» ref. kapittel 2.1.1. Internrevisjonen ser at arbeidet med informasjonssikkerheit og IKT-sikkerheit set fart etter denne rapporten frå Riksrevisjonen, eksempelvis å inkludere informasjonssikkerheit som eit av topp 5 risikoområde, sjå kapittel 3.2.2. Eit av funna i Riksrevisjonen sin rapport handla om at RHF-a hadde stilt få eigne krav til HF-a og dei regionale IKT-leverandørane, og at RHF-a i stor grad har vidareformidla krava som departementet har stilt i føretaksmøta.

[39] Protokoll frå føretaksmøte Helse Vest RHF - 16. januar 2024
[40] Styringsdokument Helse Fonna 2024 (kapittelet er likt for alle HF-a)
[41] Styringsdokument Helse Vest IKT 2024

Det blir opplyst i intervju til internrevisjonen at ein kan vere betre på å stille eigne krav frå RHF-et sin side, ikkje berre gjennom årlege styringsdokument, men òg gjennom til eksempel handlingsplan for informasjonssikkerheit og i fora som dei regionale direktørmøta.

Internrevisjonen erfarer at innføringa av NSM sine grunnprinsipp for IKT-sikkerheit er eit pågåande arbeid. I dokumentførespurnaden knytt til revisjonen bad ein om å få tilsendt oversikt over føretaka sin evne til å etterleve NSM sine grunnprinsipp for IKT-sikkerheit. Innføringa er eit pågåande arbeid, og det er fleire av tiltaka ein bør gjere regionalt, likevel reagerer internrevisjonen på at ikkje alle føretaka har ein systematisk oversikt over status. Eit føretak viser til at styringssystemet har metadata om grunnprinsippa, men internrevisjonen stiller spørsmål til om dette er ein fullgod oversikt. Helse Vest IKT er blant dei som har ein systematisk oversikt, fleire av dei andre føretaka bør likevel gjere ein sjølvstendig vurdering av om dei oppfyller prinsippa da dei sjølv er dataansvarlege, ref. kap. 2.5 og kap. 3.4.3.

3.2 Tonen frå toppen

Normen skal bidra til å understøtte gode helsetenester, god pasienttryggleik, kvalitetssikring, helsepersonellet si læring, godt personvern og pasientens helseteneste[10]. Leiing og styre må ha eit heilskapleg fokus som inkluderer både pasienttryggleik og informasjonssikkerheit for å sikre at pasientane får best mogleg behandling og vern.

3.2.1 Regional handlingsplan for informasjonssikkerheit

Helse- og omsorgsdepartementet (HOD) fylgde opp Riksrevisjonen sin revisjon med krav knytt til dei regionale helseføretaka i føretaksmøtet 14.01.2021 med følgjande;

> «Føretaksmøtet bad dei regionale helseføretaka om å:
>
> – utvikle ein regional handlingsplan for arbeidet med informasjonssikkerheit som og omfattar langsiktige tiltak. Planen skal presenterast på felles tertialoppfølgingsmøte i oktober 2021.»

Arbeidet med den regionale handlingsplanen for informasjonssikkerheit starta i 2021, og første versjon blei vedtatt av styret i RHF-et 30.09.2021[42]. Ein større revisjon av handlingsplanen blei godkjent i direktørmøtet i RHF-et 10.06.2024[43]. HOD har lagt til grunn at helseregionane skal ha ein rullerande handlingsplan med rapportering innan 1. mai kvart år.

[42] Styresak 084/21 i Helse Vest RHF - Vedl.1 Regional handlingsplan for informasjonssikkerhet i Helse Vest
[43] Sak til direktørmøtet 10.06.2024 «Oppsummering fra arbeidet med Topp 5 risiko – Informasjonssikkerhet og Revisjon av Regional handlingsplan for informasjonssikkerhet»

Fleire av CISO-ane i føretaka opplyser i intervju at dei har fått inn tiltak i handlingsplanen på dei områda dei meiner har størst behov for forbetring. Eit føretak seier at handlingsplanen er eit av dei viktigaste bidraga frå RHF-et knytt til informasjonssikkerheit. Internrevisjonen vil nemne fleire tiltak frå den regionale handlingsplanen gjennom rapporten, enkelte tiltak kan likevel vere både relevante og viktige sjølv om dei ikkje blir løfta fram her.

3.2.2 Leiinga i RHF-et og regionalt informasjonssikkerheitsutval

Styringsdokumenta og den regionale handlingsplanen for informasjonssikkerheit, ref. kapittel 3.1 og 3.2.1, etablerer ein tone frå toppen knytt til informasjonssikkerheit. Vidare tydeleggjorde RHF-et kor viktig informasjonssikkerheit er da dei inkluderte det som eit av topp 5 risikoområde i Helse Vest i 2020[44] fram til april 2024. For alle fem risikoområda blei det oppretta eigne arbeidsgrupper som hadde relevant kompetanse, i tillegg til nærleik og kjennskap til det aktuelle risikoområdet. Arbeidsgruppa, som hadde sitt siste møte 26. april 2024, jobba blant anna med den regionale handlingsplanen for informasjonssikkerheit. Framtidig revisjon og oppfølging av den regionale handlingsplanen fortset i regionalt informasjonssikkerheitsutval (SU).

I september 2022 tilsette RHF-et eigen CISO, som blei leiar for SU. Dette er eit utval for alle CISO-ane i Helse Vest, inkludert CISO frå Haraldsplass Diakonale Sjukehus, ein felles representant for dei seks andre private verksemdene, eit medlem som representerer det medisintekniske miljøet og eit medlem med juridisk kompetanse[46]. Seinast i styremøte 13. februar 2024 bad styret i RHF-et om at administrerande direktør vidarefører regionalt samarbeid om informasjonssikkerheit[45]. Utvalet har ulike oppgåver, blant anna å opptre som eit informasjonssikkerheitsfagleg rådgivande organ for verksemdene, bidra inn i risikovurderingar på informasjonssikkerheitsområde og å kvalitetssikre utførte ROS-analysar[46]. SU forvaltar felles regionalt malverk for styringssystem for informasjonssikkerheit og personvern[46]. Alle CISO-ane i Helse Vest seier i intervju at dette er eit viktig møtepunkt, og det blir spesielt framheva av dei minste føretaka. Dei seier òg at tilsetting av eigen CISO i RHF-et var positivt.

3.2.3 Styra i verksemdene

Krav til informasjonssikkerheit er gitt i ulike lovar, og verksemdene er ansvarlege for å følgje desse. Styret er det øvste styringsorganet i verksemdene[47], og har det øvste ansvaret for forvaltninga av føretaket, jf. helseføretakslova §28. Internrevisjonen meiner det er relevant for styra å få tilstrekkeleg informasjon for å kunne ta informerte avgjersler, i dette tilfelle knytt til informasjonssikkerheit. Internrevisjonen har gått gjennom protokollar og innkallingar til styremøte i RHF-et, HF-a og i Helse Vest IKT for å danne eit inntrykk av kor ofte og i kva form temaet informasjonssikkerheit er på agendaen.

[44] Styresak 135/20 Topp 5 risiko for felles risikostyring i Helse Vest
[45] Styresak 015/24 Regional handlingsplan informasjonssikkerheit i Helse Vest
[46] «Mandat for regionalt utvalg for informasjonssikkerhet» i styringssystema for informasjonssikkerhet og personvern i alle verksemdene
[47] Styrearbeid i regionale helseforetak (regjeringen.no)

Vi har ikkje laga statistikk over gjennomgangen vår, men har merka oss nokre punkt:

- Føretaka har leiinga sin gjennomgang, dette er omtalt i kapittel 3.7, og i fleire av føretaka blir leiinga sin gjennomgang behandla i styremøte, men det er likevel ikkje tilfelle i alle føretaka (merk at leiinga sin gjennomgang er ein orienteringssak i styret, og det er leiinga som eig saka)

- Spesialisthelsetenesta si årlege trusselvurdering[4,5] er styresak i nokre av føretaka

- Helse Vest IKT skil seg ut ved å ha informasjonssikkerheit på agendaen kvart møte, som er forventa med tanke på at dei skal levere produkt og tenester til HF-a på IKT-området

- Enkelte føretak har andre saker i møta; for eksempel den regionale handlingsplanen for informasjonssikkerheit, risikorapportering inkludert informasjonssikkerheit, status på IKT-område og arbeidet med informasjonssikkerheit

Oppsummert er det varierande kva informasjon dei ulike styra får. Det manglar ei heilskapleg tilnærming i styra på tvers av føretaksgruppa. I styresak 085/21 i RHF-et står det følgjande: «Styrene i Helse Vest bør i første kvartal hvert år orienteres om hovedtrekkene i ledelsens årlige gjennomgang av informasjonssikkerhet, jf. det regionale styringssystemet for informasjonssikkerhet». Internrevisjonen finn ikkje dette igjen i styringssystemet, men er einige i at dette er ei av sakene styra bør ha, i tillegg til at dei ulike føretaka bør samkøyre kva tid på året dei har leiinga sin gjennomgang for informasjonssikkerheit.

3.2.4 Leiinga i verksemdene

Leiinga i føretaka har leiinga sin gjennomgang, sjå kapittel 3.7. I intervju med CISO-ane og leiarar for IKT stilte internrevisjonen spørsmål om korleis dei meiner tonen frå toppen hos leiinga i deira føretak er knytt til informasjonssikkerheit. Dei fleste intervjuobjekta uttrykker seg positivt, men samtidig blir det peika på at det kan vere vanskeleg å nå fram til heile leiinga. Ein CISO seier i intervju at leiinga er opptatt av informasjonssikkerheit viss det har oppstått ei hending, og ein annan uttrykker at det er hans jobb å få dei til å bli det.

I Helse Bergen har dei kvartalsvise møte i sikkerheitsrådet som administrerande direktør leiar, og CISO førebur saker. Administrerande direktør i Helse Bergen ber om innspel frå leiar for IKT og CISO til styresakene som skal opp i Helse Vest IKT før møta. Dette viser eit engasjement frå administrerande direktør, samtidig som ein ser at dei som jobbar med informasjonssikkerheit i Helse Bergen har god forankring hos leiinga. Innspela gir moglegheit for å kunne påverke avgjersler som blir tatt i Helse Vest IKT. I intervju blir det sagt at CISO i Helse Bergen sjølv har invitert seg inn i møte med administrerande direktør for å oppdatere om enkeltsaker – ut over faste møte. Dette blir tatt godt imot. CISO har òg møte med fagdirektør i Helse Bergen kvar veke, og opplever at ho er engasjert og oppteken av temaet.

CISO i Helse Fonna legg vekt på at deira fagdirektør er spesielt engasjert og har temaet høgt på agendaen. CISO i Helse Fonna har ikkje faste møtepunkt med verken administrerande direktør eller fagdirektør, men møter fagdirektør frå sak til sak. Merk at internrevisjonen likevel er av oppfatning av at CISO har god forankring i Helse Fonna. I Helse Førde har CISO og leiar for IKT månadlege møte med administrerande direktør kor dei rapporterer pågåande problemstillingar.

Sjukehusapoteka Vest lager årlege aksjonsplanar kor informasjonssikkerheit er inkludert, med rapportering to gonger i året. I Helse Vest IKT har dei «Ledermøte informasjonssikkerhet» anna kvar veke med nokre av avdelingsleiarane og administrerande direktør. CISO i Helse Stavanger har ad-hoc rapportering, for eksempel gjeldande HelseCERT[48] sine inntrengingstestar, men ingen «formelle» møte. Internrevisjonen ser at CISO i Helse Stavanger ikkje har ei tydeleg forankring hos leiinga. Gjennom intervju kjem det og fram at andre i føretaksgruppa ønsker ei sterkare forankring for CISO i Helse Stavanger. CISO i RHF-et har heller ikkje faste og formelle møtepunkt med administrerande direktør, men dei har møte frå sak til sak.

I Riksrevisjonen sin rapport skriv dei at dei administrerande direktørane gav uttrykk for at leiinga og styra i aukande grad er oppteken av informasjonssikkerheit, i tillegg til at CISO-ane opplever å ha støtte hos toppleiinga og andre leiarar internt[8], men samtidig peiker dei på at det er viktig med sterkare forankring hos leiinga, som nemnt i kapittel 2.1.1. Internrevisjonen registrerer at det er variasjon i den formaliserte kontakten mellom CISO og leiinga i helseføretaka. Dette kan vere ei medverkande årsak til at kjennskapen til informasjonssikkerheitsarbeidet i den øvste leiargruppa kan opplevast noko varierande. Helse Fonna og Helse Bergen ønskte å ha informasjonssikkerheit med vidare som eit av topp 5 risikoområda, jf. kap. 3.2.1. Helse Vest IKT skreiv at dei ikkje hadde forslag til nye område, men at dei hadde ønskje om å vidareføre forbetringsarbeidet innanfor informasjonssikkerheit i eit regionalt samarbeid.

I intervju har vi spurt både administrerande direktørar og fagdirektørar om deira syn på pasienttryggleik og informasjonssikkerheit. Det blir uttrykt at desse heng saman og det er vanskeleg å sjå opp mot kvarandre, samtidig som dei set pasienttryggleik øvst. Dei er likevel klare på at informasjonssikkerheit er ein høg prioritet hos dei, og at ein er avhengig av god informasjonssikkerheit i sjukehusa. Fleire seier at dette vil bli meir og meir tydeleg som følgje av digitaliseringa og at bruk av teknologi aukar i føretaka.

3.2.5 Oppsummering av funn knytt til tonen frå toppen

Det er fleire positive funn knytt til tonen frå toppen. Den regionale handlingsplanen for informasjonssikkerheit, eigen CISO i RHF-et og SU er viktig for heile føretaksgruppa. Vidare får dei ulike styra fleire saker knytt til informasjonssikkerheit, men det er varierande frå føretak til føretak, og det er ingen heilskapleg tilnærming til dette på tvers av styra i Helse Vest.

[48] HelseCERT er det nasjonale senteret til helse- og omsorgssektoren for cybertryggleik og tilbyr sikkerheitstenester gjennom Nasjonalt beskyttelsesprogram (NBP)

Ei tilnærming kan vere å diskutere i SU kva styra har behov for, og erfaringar med kva styret er interessert i og har nytte av. I intervju er dei fleste positive knytt til tonen frå toppen i leiinga i føretaket, men internrevisjonen ser kor viktig det er med god forankring hos leiinga. Faste møtepunkt med administrerande direktør eller andre i leiinga kan bidra til dette.

Helse Bergen nyttar seg spesielt av styreplassen i Helse Vest IKT ved at blant anna CISO kan komme med innspel til dei opne styresakene. Det er positivt med faste møtepunkt for CISO og administrerande direktør eller andre i toppleiinga, men det er ingen føretaksovergripande praksis i Helse Vest på dette. Dette kan vere ein medverkande årsak til variasjon i kor godt informasjonssikkerheitsarbeidet er forankra i toppen frå føretak til føretak.

Til slutt er både administrerande direktørar og fagdirektørar klare på at det er vanskeleg å velje mellom informasjonssikkerheit og pasienttryggleik, da desse heng saman, sjølv om dei fleste peiker på at pasienttryggleik står øvst. Internrevisjonen opplever at dei er engasjerte rundt temaet i intervjua.

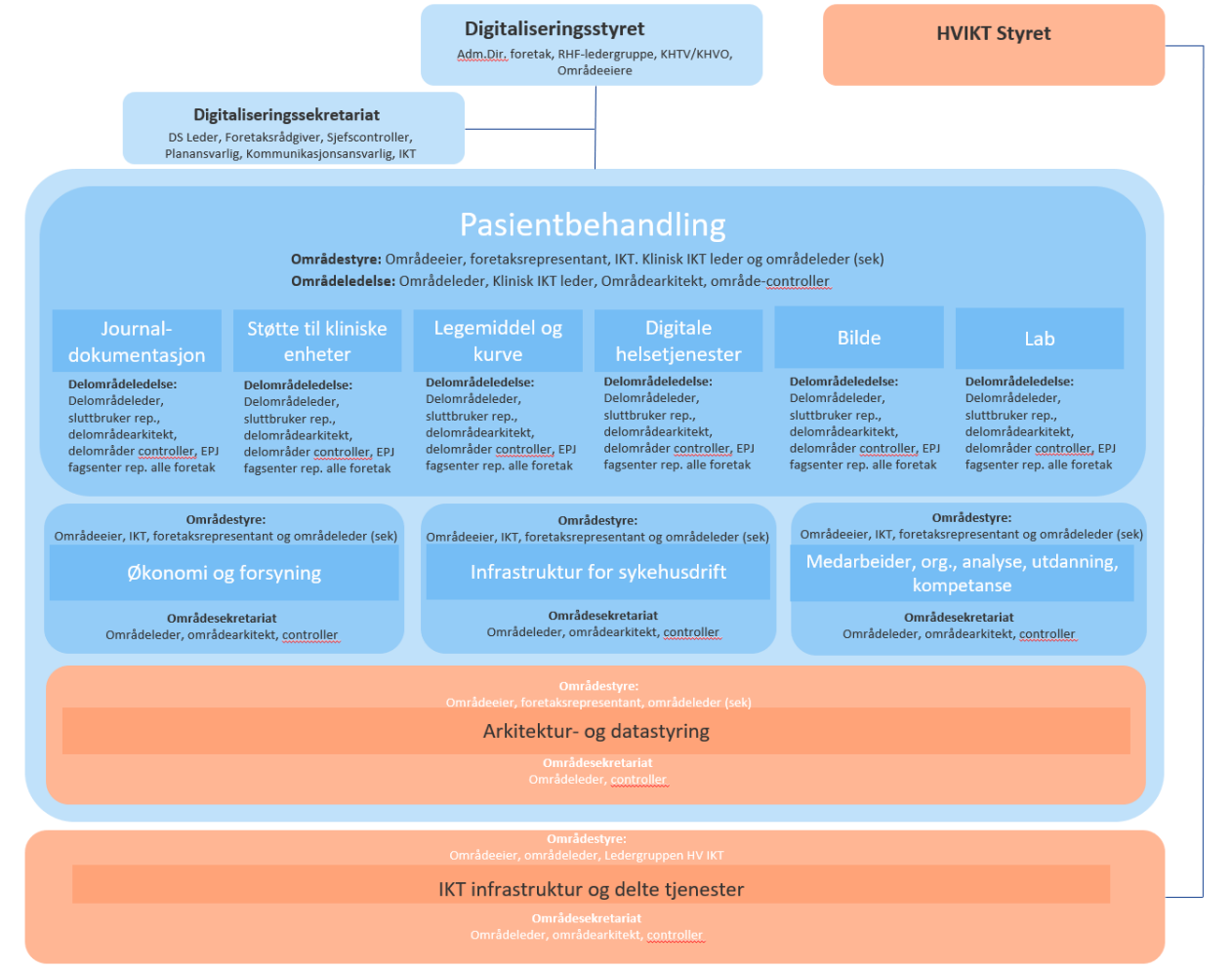
3.3 Styringsstruktur for digitalisering

Startpunktet for etablering av den nye styringsstrukturen blei satt da direktørmøtet godkjente digitaliseringsstyret 15. mai 2023. I same møte blei det utpeikt områdeeigarar. I Digitaliseringsstyret blei områdestyra godkjent den 12. juni 2023, og områda gjekk inn i sitt første driftsår i 2024. Styret i RHF-et fekk ei orientering av administrerande direktør om den nye styringsstrukturen for digitalisering 14. juni 2023[49]. Målet med endringa er at Helse Vest sin styringsstruktur for digitalisering skal støtte kontinuerleg forbetring, slik at føretaka i Helse Vest er i stand til å møte framtidige krav til kapasitetsutfordringar. Før vi legg fram funn vil vi i dei neste avsnitta beskrive styringsstrukturen med informasjon frå den interne SharePoint-sida som handlar om dette.

[49] Styresak 056/23 i Helse Vest RHF - Vedl.9 Gjennomgang av styringsstruktur for digitalisering

3.3.1 Digitaliseringsstyret, områdestyra, digitaliseringssekretariatet og områdeleiing

Følgjande figur viser områdeinndelinga i styringsstrukturen for digitalisering:



Figur 1: Områdeinndeling - Styringsstrukturen for digitalisering[50]

Styringsstrukturen består av eit digitaliseringsstyre som er det øvste styringsorganet for det felles regionale arbeidet med digitalisering. Styret er samansett av representantar frå alle føretaka og for dei tillitsvalde[51] for å sikre at digitaliseringsprosjekt og strategiar blir implementerte i tråd med både lokale behov og regionale løysingar. Blant deira oppgåver og ansvar er det å eige den overordna visjonen, retninga og planane for Helse Vest, sette overordna mål, godkjenne områdeoppdrag og å avgjere korleis finansieringa skal bli fordelt mellom områda i tråd med økonomiprosessane som gjeld, med meir.

[50] Områdeinndeling – Styringsstruktur for digitalisering

[51] Digitaliseringsstyret er samansett av AD i Helse Vest RHF, AD i helseforetakene, Helse Vest IKT og Sjukehusapoteka Vest, ledergruppen i Helse Vest RHF, samt HKTV og HKVO

Under Digitaliseringsstyret er det ulike områdestyre, kor kvart områdestyre samlar digitaliseringsaktiviteten innanfor sitt område i ein felles struktur i samsvar med områdeoppdraget frå Digitaliseringsstyret. Områdestyra skal blant anna gje innspel til Digitaliseringsstyret om innhald i områdeoppdrag, ha ansvar for dei økonomiske rammene i området og arbeide mot at avgjersler blir tatt på det lågaste formålstenlege nivå med rett klinisk eller teknisk kompetanse. Samansettinga skal spegla ansvarsforholda i linjestrukturen i føretaka, og ressursane som er med skal ha rett avgjerdsmakt på formålstenlege nivå i linjestrukturen. Rollene vil bestå av representantar frå HF-a og Helse Vest IKT (for teknisk systemkompetanse), i tillegg til brukarrepresentant og områdearkitekt.

Digitaliseringssekretariatet er det rådgivande organet til Digitaliseringsstyret, og består av leiar, ansvarleg for kontrollarar, strategisk rådgivar, teknisk systemansvarleg og rådgivar frå kvart av føretaka. Dei samarbeider med, og har tilgang på ressursar frå, Arkitektur- og datastyring ved behov for kompetanse innan verksemdsarkitektur og data- og informasjonsforvaltning[52].

Områdeleiinga skal ivareta den daglege leiinga av området på vegner av områdeeigar/områdestyret i tråd med mandat, føringar og oppdrag gitt av områdestyret, og er satt saman av områdeleiar, områdearkitekt, kontrollar og eventuelle tilleggsressursar ved behov[52].

3.3.2 Dei ulike områda og plassering av informasjonssikkerheit

Styringsstrukturen har områda arkitektur- og datastyring, pasientbehandling, infrastruktur for sjukehusdrift, økonomi og forsyning, MOT (medarbeidar, organisasjon og teknologi) og IKT-tenester[52].

Innanfor IKT-tenester (IKT-infrastruktur og delte tenester) har ein delområde som er strategiske tenester, utviklingstenester, støttetenester, digital plattform, små og mellomstore system, byggstøtte IKT, privat sky, mobilitet og IKT-infrastruktur. I delområdet IKT-infrastruktur ligg informasjonssikkerheit, blant anna saman med drift av nettverk, server, lagring og IKT-utstyr. Heile området IKT-tenester (IKT-infrastruktur og delte tenester)ligg til Helse Vest IKT, det gjelder både områdestyret og områdeleiinga. Det at ikkje alle dei dataansvarlege verksemdene ligg her er ein svakheit.

[52] Digitalisering i Helse Vest – Hjemmeside – SharePoint-side om digitalisering i Helse Vest

I den regionale handlingsplanen for informasjonssikkerheit[43] har ein mål om å integrere informasjonssikkerheit og personvern i styringsstrukturen. Eit tilhøyrande tiltak er at Helse Vest skal sørgje for at informasjonssikkerheit blir reflektert på ein hensiktsmessig måte i områdestrukturen, slik at ein ivaretar den verksemdsovergripande styringsaksa for å støtte sikker og stabil drift av tenester og infrastruktur. Internrevisjonen meiner dette er eit viktig tiltak. Den nye styringsstrukturen legg opp til at føretaka i aukande grad skal jobba meir smidig i leveransane, og eit anna tiltak i den regionale handlingsplanen for informasjonssikkerheit er at krav og evne til å levere på god informasjonssikkerheit og godt personvern må bli ivaretatt ved bruk av smidige metodar.

3.3.3 Kommentarar frå intervju og skriftlege tilbakemeldingar

I intervju med administrerande direktørar og fagdirektørar har internrevisjonen stilt spørsmål om deira syn på den nye styringsstrukturen for digitalisering. Dei løfter fram fleire ting, avgjersler blir tatt på eit lågare nivå, som er positivt, men som gjerne utfordrar systemet per no. Dei er spente på korleis dette vil fungere i praksis, men reknar endringa som positiv. Ein av dei administrerande direktørane løftar fram at det er ein viss fare for at den nye strukturen likevel kan mangle eigarskap i føretaka og bli oppfatta som styrt frå RHF-et. I intervju med CISO og leiar for IKT i alle føretaka blir det påpeika at informasjonssikkerheit er lite synleg i styringsstrukturen, og at dette er diskutert i SU. Det blir blant anna uttalt i intervju at informasjonssikkerheit kjem inn som infrastrukturteneste frå Helse Vest IKT, og at dette er altfor seint. Både administrerande direktør i RHF-et og direktør for e-helse løftar fram at styringsstrukturen ikkje har plassert inn «støttefunksjonar» som informasjonssikkerheit. Det blir da peikt på at ein eksempelvis ikkje har integrasjon og løysingsutvikling i strukturen. Støttefunksjonane skal likevel vere tilgjengelege for alle områda i den nye strukturen. Ein CISO seier at informasjonssikkerheit er (blant anna) ein støttefunksjon som bør vere representert under område for IKT-tenester slik at dei kan gi støtte på tvers av tekniske delområde. Vidare seier han at informasjonssikkerheit òg er ein strategisk viktig funksjon som skal sørgje for at verksemda følgjer lover og regler, dermed meiner han at det òg er behov for representasjon inn i område som Arkitektur- og datastyring.

3.3.4 Oppsummering av funn knytt til den nye styringsstrukturen for digitalisering

Internrevisjonen reviderer ikkje den nye styringsstrukturen for digitalisering i stort, men ønskjer å belyse plassering av informasjonssikkerheit. Både gjennomgang av dokumenter som ligg på intranett knytt til styringsstrukturen og intervju viser at informasjonssikkerheit ikkje er tydeleg plassert, og at det kjem for seint inn. Internrevisjonen meiner tiltaka i den regionale handlingsplanen er hensiktsmessige og bør bli gjennomført. Eit argument for at informasjonssikkerheit bør bli løfta fram i styringsstrukturen, sjølv om ikkje andre støttefunksjonar blir det, er at alle verksemdene er dataansvarlege og må følgje dei krav som følgjer med dette. Internrevisjonen har òg merka seg at fleire ulike intervjuobjekt seier at alle tilsette har eit ansvar for informasjonssikkerheita, samtidig som at det kan vere vanskeleg å nå alle med bodskapet. Å plassere inn informasjonssikkerheit i den nye styringsstrukturen kan bidra til å synleggjere kor viktig det er. Det er ulike synspunkt på om informasjonssikkerheit bør vere synleg i den nye styringsstrukturen for digitalisering. RHF-et bør løfte denne diskusjonen og endeleg avgjer om ein bør synleggjere det.

3.4 Ansvar, organisering, kompetanse og ressursar

3.4.1 Administrerande direktør og CISO – ansvar, organisering og oppgåver

Helsedirektoratet sin «Rettleier for leiing og kvalitetsforbetring i helse- og omsorgssektoren»[53] slår fast at det er avgjerande for eit godt styringssystem at det ikkje er tvil om kvar ansvar, oppgåver og styresmakt er plassert i ei verksemd. Det er øvste leiing i verksemda som har ansvaret for å sørgje for at verksemda følgjer gjeldande krav til informasjonssikkerheit, og at informasjonsbehandlinga i verksemda gir eit sikkerheitsnivå som er eigna med omsyn til risikoen og kva art behandlinga har[54].

I alle intervjua med CISO og leiar for IKT i føretaka seier dei uoppfordra at det er administrerande direktør som har det øvste ansvaret, og alle administrerande direktørar i Helse Vest bekreftar det same. Dette er òg skriftleg nedfelt i dokumentet «Roller og organisering av arbeid med informasjonssikkerheit og personvern» som ligg i styringssystema i Helse Vest[55].

Normen presiserer at større verksemder bør ha eigen leiar for informasjonssikkerheit eller sikkerheitsorganisasjon knytt opp mot leiinga i verksemda[56]. RHF-et, Helse Fonna og Helse Stavanger har alle ein tilsett som er 100% dedikert til arbeidet med informasjonssikkerheit som CISO. CISO i Helse Stavanger presiserer likevel at dei ikkje har hatt ein ordentleg diskusjon på om stillinga reelt sett er 100%, da han innehar fleire oppgåver som kjem i tillegg til dei som ligg i styringssystemet. Sjå lenger ned i kapittelet for ei opplisting av oppgåvene som ligg i styringssystemet. RHF-et har i tillegg ein jurist som jobbar mellom 30-50% med temaet. I Helse Førde har dei 50% av ei stilling til informasjonssikkerheit/CISO, og i SAV mellom 40 og 60% av ei stilling. I Helse Bergen har dei ein CISO og ein rådgivar for informasjonssikkerheit. Internrevisjonen ser at det er varierande kor CISO er plassert i organisasjonen, for eksempel under IKT eller fag og forsking. Internrevisjonen erfarer at sjølve plasseringa ikkje nødvendigvis er avgjerande for arbeidet til CISO, men at det er viktigare å sørgje for god forankring hos leiinga. Ein kan likevel argumentere for at eit tiltak for god forankring hos leiinga kan vere plassering av CISO nærare administrerande direktør, for å redusere avstanden mellom desse rollene.

Helse Vest IKT gjorde ei endring i 2022 kor dei flytta CISO frå seksjon for IKT-sikkerheit og over i stab (administrativt under avdeling for fellesteinestar) i og med at CISO sitt ansvarsområde famnar bredt på tvers av alle avdelingar. Det blir likevel stilt spørsmål i intervju av enkelte HF om ein burde ha CISO i leiinga hos Helse Vest IKT, og om informasjonssikkerheit i stort er hensiktsmessig plassert i Helse Vest IKT. Internrevisjonen har undersøkt litteratur om CISO sin plassering i organisasjonar, og det er vanskeleg å konkludere og anbefale kor plasseringa bør vere.

[53] Leiing og kvalitetsforbetring i helse- og omsorgstenesta - Helsedirektoratet
[54] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap. 2 Ledelse og ansvar
[55] «Roller og organisering av arbeidet med informasjonssikkerhet og personvern» i styringssystema for informasjonssikkerheit og personvern i alle verksemdene
[56] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap 2.1. Roller og ansvar for informasjonssikkerhet og personvern

Ein ser likevel at det er fleire internasjonale teknologiselskap som har CISO i toppleiinga, for eksempel Apple og Microsoft. Leiinga i Helse Vest IKT bør diskutere og vurdere om dette ville vore hensiktsmessig, og eventuelt kva fordelar og ulemper som følgjer med dette.

CISO i Helse Vest IKT viser til ein analyse KPMG gjorde i 2023. KPMG nytta seg av ENISA (European Union Agency for Cybersecurity) sitt rammeverk CSIRT Maturity Framework. Rammeverket beskriv krav og forventingar til eit sikkerheitssenter. Her skil organisering i Helse Vest IKT seg ut ved at det er eit stort gap mellom situasjonen no og kor ein ønskjer å vere. Internrevisjonen har ikkje dette i sitt prosjektmandat for revisjonen, men vel likevel å poengtere det i rapporten. Internrevisjonen merkar seg, som nemnt i kapittel 3.2.4, at CISO i Helse Vest IKT har møte anna kvar veke med deler av leiinga. Internrevisjonen stiller spørsmål til om alle relevante avdelingsleiarar er med i dette møte. Vidare meiner vi at ein kan argumentere for at styrking av heile organiseringa knytt til IKT-sikkerheit kan vere ein positiv drivar for forankringa hos leiinga.

Alle CISO-ane i Helse Vest opplyser om at dei har moglegheit til å rapportere direkte til administrerande direktør. Det er ikkje ein «fasit» på kva ein CISO har for oppgåver, men Digdir har laga ei kompetansebeskriving av rolla «fagansvarleg informasjonssikkerhet» som dei skriv svarar til rolla som CISO. «Fagansvarleg informasjonssikkerhet» skal ha hovudansvar for å vere pådrivar og å støtte leiinga og organisasjonen elles i arbeidet med informasjonssikkerheit. Dette arbeidet inkluderer blant anna å jobbe med internkontroll, opplæring og kompetanse, bevisstgjering av andre tilsette og risikovurdering- og handtering knytt til området informasjonssikkerheit.[57]

I føretaka sine styringssystem har dei dokumentet «Roller og organisering av arbeidet med informasjonssikkerhet og personvern»[55] som beskriv arbeidsoppgåvene til CISO:

- «Bistå med å vurdere risiko knyttet til informasjonssikkerhet, herunder risiko knyttet til leverandører og samarbeidspartnere.
- Følge opp uønskede hendelser knyttet til informasjonssikkerhet
- Utarbeide og vedlikeholde dokumenter i virksomhetens interne styringssystem for informasjonssikkerhet og personvern
- Årlig forberede og følge opp «Ledelsens gjennomgang» av informasjonssikkerhet
- Gjennomføre sikkerhetsrevisjoner
- Delta i Regionalt informasjonssikkerhetsutvalg
- Bistå med rådgivning og opplæring i god sikkerhetskultur i virksomheten
- For virksomheter underlagt sikkerhetsloven vil denne rollen være tilsvarende datasikkerhetsleder (DSL)»

[57] Rolle: Fagansvarlig informasjonssikkerhet | Digdir

RHF-et har i tillegg følgjande punkt:

- «Lede regionalt informasjonssikkerhetsutvalg
- Å bistå systemeier med å utføre sine arbeidsoppgaver
- Å utarbeide, inngå og følge opp tjenesteavtaler om drift og vedlikehold av informasjonssystemene
    - Gjelder ikke medisinsk teknisk utstyr eller teknisk utstyr, hvor det er henholdsvis medisinsk teknisk avdeling og teknisk avdeling i helseforetakene som har ansvaret for drift og vedlikehold
- Å følge opp informasjonssikkerhet og personvern hos partnere, leverandører og databehandlere på et overordnet nivå.»

Internrevisjonen meiner at dokumentet som beskriv oppgåvene til CISO i Helse Vest er i samsvar med «dei typiske» oppgåvene som ein CISO har, jf. Digdir. Gjennom revisjonen har internrevisjonen fått bekrefta at CISO-ane meiner desse oppgåvene er sine. Internrevisjonen ser kor viktig det er med forankring hos leiinga for å kunne utføre alle oppgåvene. CISO-rolla er sjølvstendig, og støtte frå leiinga og administrerande direktør er nødvendig for å kunne gjere ein god jobb.

3.4.2 Sikkerheitsrevisjonar

Ei av oppgåvene til CISO er å gjennomføra sikkerheitsrevisjonar. Eit av krava i Normen er at leiinga i verksemda skal følgje opp at ein ivaretar sikkerheita ved å gjennomføre minimum årlege sikkerheitsrevisjonar, i tillegg til at det skal vere ein godkjent plan for sikkerheitsrevisjonar[58]. Alle føretaka har retningslinjer om sikkerheitsrevisjonar i sitt styringssystem.

I Riksrevisjonen sin rapport «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer»[8] har dei ein tabell kor det kjem fram at det berre var 1 av 4 føretak i Helse Vest som gjennomførte sikkerheitsrevisjonar i 2017 og i 2018. Internrevisjonen bad om gjennomførte sikkerheitsrevisjonar frå føretaka i dokumentførespurnaden knytt til denne revisjonen. SU har gjennomført ein regional, felles revisjon («Sikker lagring») som blei lagt fram for direktørmøte i 2023. I svaret til RHF-et i dokumentførespurnaden frå internrevisjonen skriv dei at planen er å gjennomføre ein årleg revisjon av minst ei fellesløysing levert av Helse Vest IKT, men det er per no ikkje gjennomført for 2024. Det er varierande i kva grad føretaka har gjennomført sikkerheitsrevisjonar, og det er eit område kor det er eit stort forbetringspotensiale. I den regionale handlingsplanen for informasjonssikkerheit[43] er eit mål å kontrollere at sikkerheitstiltak er tilstrekkelege og at krav blir etterlevd gjennom revisjonar kor dei ansvarlege er RHF-et og SU. Dei tilhøyrande tiltaka er «Interregionalt samarbeid om revisjon av felles underleverandører», «Sikkerhetsrevisjon av regional fellesløsning» og «Vurdere å etablere internrevisjonskapasitet i Helse Vest IKT AS».

[58] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap. 5.4.6. Sikkerhetsrevisjon

Internrevisjonen ser på desse tre tiltaka som viktige, men samtidig kunne ein med fordel hatt alle føretaka som ansvarlege i kombinasjon med mål eller tiltak om å gjennomføre fleire mindre sikkerheitsrevisjonar i det enkelte føretaket. Internrevisjonen meiner at sikkerheitsrevisjonar på klinikkar, avdelingar og så vidare kan bidra til å bevisstgjere helsepersonell og andre tilsette på temaet informasjonssikkerheit. Dei færraste føretaka har ein godkjent plan for sikkerheitsrevisjonar, enkelte har sikkerheitsrevisjonar inkludert i føretaket sin plan for internrevisjonar generelt. For at sikkerheitsrevisjonane skal vere nyttige må ein i tillegg til kapasitet for gjennomføring sørgje for at det er ressursar til å følgje opp funna i etterkant.

3.4.3 Ansvarsfordeling mellom Helse Vest IKT og føretaka

Sentralt for informasjonssikkerheit (og personvern) er som nemnt i kapittel 2.5 rollene dataansvarleg og databehandlar. Begge parter har eit sjølvstendig ansvar for informasjonssikkerheit. Alle verksemdene i Helse Vest er dataansvarlege, Helse Vest IKT er regionen sin sentrale databehandlar for de dataansvarlege i Helse Vest. I styringssystema, i dokumentet «Roller og organisering med informasjonssikkerhet og personvern», står det at Helse Vest IKT har ansvar for følgjande oppgåver:

- «Sikre at teknisk IKT-sikkerhet er ivaretatt for informasjonssystemer som forvaltes i henhold til SLA-avtalen
- Forvalte tilganger, autorisasjoner og roller i henhold til bestilling fra virksomhetene
- Ivareta informasjonssikkerhet i teknisk IKT-infrastruktur i henhold til SLA-avtalen, samt sørge for at det tilfredsstiller krav, reguleringer og god praksis for informasjonssikkerhet i infrastruktur (Normen, NSM grunnprinsipper, etc.)
- Gjennomføre risikovurdering av teknisk utstyr, infrastruktur, applikasjoner og informasjonssystemer
- Utarbeide beredskapsplaner for IKT-infrastruktur og ta ledelsen i IKT-relaterte beredskapssituasjoner
- Utarbeide og vedlikeholde teknisk sikkerhetsdokumentasjon for IKT-infrastrukturen
  Ivareta rollen som databehandler i henhold til etablert databehandleravtale, og gjennom denne bistå virksomhetene med leverandøroppfølging på vegne av virksomhetene»[55]

CISO i Helse Bergen peiker på at lista over oppgåver som Helse Vest IKT har ansvar for manglar relevante punkter frå tenesteavtalen[59]. Følgjande oppgåver står i SLA-avtalen bilag 5, punkt 4.6 Sikkkerhet: «Leverandøren skal løpende sikre IKT tjenestene og underliggende infrastruktur / systemer på taktisk nivå, bl.a. med

- PEN-test (inntrengningstest) og andre 3.parts evalueringer
- Risikovurderinger: Gjennom metodisk og strukturert tilnærming vurdere risiko på nye eller nåværende tjenester
- Fungere som ad-hoc rådgiver innenfor området (informere, påvirke) og foreslå risikoreduserende tiltak
- Ha ansvar for sikkerhetsarkitektur innenfor sitt leveranseområde»

[59] SLA bilag 5 punkt 4.6. sikkerhet

Ansvaret Helse Vest IKT har knytt til IKT-infrastruktur blir nærare omtalt i kapittel 3.5.2. Undersøkinga til Riksrevisjonen viste at det var uklarleikar mellom IKT-leverandørane og helseføretaka om kven som skulle gjennomføra konkrete informasjonssikkerheitstiltak. I mange tilfelle var det uklart kven som skulle gjere nødvendig opprydding og forbetringstiltak, samt uklart korleis ein skal fordele ansvaret for ivaretaking av informasjonssikkerheit i medisinsk-teknisk utstyr.[8] I intervju opplever vi at leiar for IKT og CISO-ar uttrykker at dei er klar over ansvarsfordelinga, men det er likevel moment i enkelte intervju som tilseier at ein er noko ueinige i oppgåvene, for eksempel oversikt over IKT, sjå kapittel 3.5. CISO i Helse Vest IKT meiner ansvarsfordelinga fungerer bra, men at ein aukande mengde anskaffingar skjer utan Helse Vest IKT. Anskaffingar blir løfta fram i kapittel 3.5.6.

3.4.4 Kompetanse og ressursar

Alle føretaka seier i intervju at dei gjerne skulle hatt fleire ressursar for å auke kapasiteten på informasjonssikkerheit. Ein CISO uttrykker at arbeidet med informasjonssikkerheit blir tyngre og tyngre, utan at dei får anledning til å bruke meir tid på det. Eit anna føretak seier at det kanskje ikkje hadde nytta med ekstra ressursar, da dei meiner at avgjersler blir tatt regionalt, og at dei bruker mykje tid på å få ein sterkare stemme i det regionale arbeidet. Intervju med personar frå RHF-et presiserer at den påstanden handlar meir om at dei må ta eit større ansvar for informasjonssikkerheit i føretaket sitt, og ikkje lene seg på Helse Vest IKT, ref. deira rolle som dataansvarleg (sjå kapittel 2.5, 3.4.3 og 3.5). Internrevisjonen ser at dette kan henge saman med kva forankring CISO har hos leiinga, og at det er lettare å gjennomføra ulike arbeidsoppgåver om ein har støtte hos leiinga i føretaket. I riksrevisjonen sin rapport sa alle CISO-ane som blei intervjua ved dei utvalde helseføretaka at støtte hos leiinga er viktig for å få gjennomført nødvendige tiltak[8].

Helse Vest IKT leverer produkt og tenester til alle HF-a på IKT-området, og har dermed fleire ressursar som jobbar med IKT-sikkerheit. Rekruttering har tidvis vore krevjande for Helse Vest IKT. Eit tiltak, initiert av CISO, har vore å senke formelle inngangskrav til kandidatar og heller utdanne dei via eit intensivt opplæringsprogram på 12 veker for å utvide tilfanget av kandidatar og dermed moglegheitene til Helse Vest IKT[60]. CISO seier i intervju at han er positiv til erfaringa med dette så langt.

Svakheiter knytt til kompetanse blir i liten grad trekt fram i intervjua, Sjukehusapoteka Vest har eit ønskje om å kunne leige inn CISO-kompetanse frå Helse Vest IKT, men det blir problematisert av Helse Vest IKT med tanke på at det handlar om å leige ut kompetanse (og ansvar) frå eit juridisk rettssubjekt til eit anna.

[60] – Vi rustar opp sikkerheitslaget vårt (sharepoint.com)

3.4.5 Oppsummering av funn knytt til ansvar, organisering, kompetanse og ressursar

Det er ingen tvil i føretaka om at administrerande direktør har det øvste ansvaret for informasjonssikkerheit. Vidare har alle føretaka ein person som har oppgåvene og ansvaret som CISO, men det varierer om denne personen innehar andre arbeidsoppgåver i tillegg. Ressursane varierer mellom føretaka, avhengig av størrelse. Dei fleste uttrykker at dei ønskjer meir ressursar og kapasitet, men det er få som trekker fram svakheiter knytt til kompetanse. Oppgåvene til CISO kjem klart fram i styringssystemet, og desse samsvarer med dei typiske oppgåvene ein CISO har. Helse Vest har forbetringspotensiale knytt til gjennomføring av sikkerheitsrevisjonar, og dette gjeld fleire av føretaka. Internrevisjonen ser at det er vesentleg med god forankring hos leiinga for å kunne gjere ein god jobb. Ansvarsfordelinga mellom føretaka og Helse Vest IKT er tydelegare no enn når Riksrevisjonen gjorde sin revisjon i 2020, men internrevisjonen ser likevel indikasjonar på at det framleis ikkje er heilt klart. Føretaka må vere bevisste på si rolle og sitt ansvar som dataansvarleg.

3.5 Oversikt over IKT

3.5.1 Innleiing og avklaring av omgrep

I NSM sine grunnprinsipp for IKT-sikkerheit står det at kartlegging av einingar og programvare er viktig for å få oversikt over kva verksemda har. Ein bør kunne finne det som er styrt av verksemda sjølv, legitime einingar med avgrensa rettar og ukjende einingar.[61] Normen peiker på at ein skal ha oversikt over IKT-system, infrastruktur, digitale tenester og anna informasjon med betyding for informasjonssikkerheita – og at denne oversikta *bør* vera dokumentert[62]. Riksrevisjonen skreiv i sin rapport at det var mangelfull kontroll med einingar og programvare, og at det manglar ein fullgod oversikt over maskiner og programvare i eigne nettverk, som er ein føresetnad for å sikre desse[8]. I dei neste avsnitta gjer vi greie for nokre omgrep frå ulike kjelder, og i delkapitla under ser vi om Helse Vest har dei nødvendige oversiktene.

Den totale IKT-strukturen i Helse Vest kan grovt delast i to delar: **IKT-infrastruktur og system/applikasjonar** med tilhøyrande integrasjonar som brukarane nyttar. **IKT-infrastruktur** omfattar all maskinvare som nettverksutstyr, serverar, lagringssystem, PC-ar, nettbrett og mobiltelefonar, samt grunnleggjande programvare som operativsystem og antivirus. For å illustrere omfanget, har Helse Vest 240 eksterne nettverkssamband, 1 600 nettverkskomponentar, over 100 000 aktive nettverksportar, over 16 000 trådlause aksesspunkt, om lag 31 000 PC-ar, 4 100 serverar (der over 3 200 er virtualiserte), og 15 petabyte lagringskapasitet[63,64].

[61] NSMs Grunnprinsipper for IKT-sikkerhet v2.1.pdf – Kapittel 1.2 «Kartlegg enheter og programvare»
[62] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap. 3.3. Oversikt over teknologi og behandling av helse- og personopplysninger
[63] Styresak 085/21 i Helse Vest RHF - Styringsstruktur informasjonssikkerheit Helse Vest
[64] Oversikt frå styresak 08/21 (fotnote 61) er oppdaterte med tal frå Helse Vest IKT 22.10.24 kor dette er relevant

System/applikasjonar omfattar blant anna elektronisk pasientjournal (DIPS), legemiddelløysinga Meona, Digitalt media arkiv (Sectra), HR-system (Agresso) og økonomisystemet SAP. Vidare har ein godt over 1 000 ulike system og applikasjonar i Helse Vest, fordelt på i overkant av 240 store, om lag 150 mellomstore og nærare 700 små system[63].

Medisinsk utstyr (MU) er utstyr og programvare som er laga for å diagnostisere, behandle eller overvake sjukdommar eller tilstandar hos menneske. **Teknisk utstyr (TU)** er IKT som er integrert i byggtekniske løysingar, som alarmsystem, tilgangskontroll, straumstyring og automatiserte driftsanlegg. **Lokal IKT** er utstyr og system som blir forvalta av det enkelte helseføretaket.[63] Ansvaret for drift av teknisk utstyr og medisinsk utstyr ligg til føretaka, men ein del oppgåver og tenester blir satt ut til Helse Vest IKT.

3.5.2 Infrastruktur

Helse Vest IKT har hovudansvaret for den sentrale IKT-infrastrukturen som er felles for helseføretaka i regionen. Dette inkluderer drift, vedlikehald og utvikling av dei digitale systema og nettverka som blir nytta på tvers av helseføretaka. Dei har ei overordna rolle i å sikre at systema fungerer, og å sørgje for at medisinsk utstyr (MU) og teknisk utstyr (TU) kan vere knytt til nettverket og at utstyret ikkje representere ein uakseptabel risiko for dei andre systema/applikasjonane som eksisterer i same nettverk. Dette blir avklart i styresak 085/21 i Helse Vest RHF 30.09.2021[63]. Helseføretaka er likevel ansvarleg for informasjonssikkeheit for system og integrasjonar som etablert på felles IKT-infrastruktur, jf. deira rolle som dataansvarleg. Merk at føretaka kan ha ein mindre del av sin IKT-infrastruktur som dei forvaltar sjølv. Eksempelvis løftar Helse Bergen fram i sin leiinga sin gjennomgang for informasjonssikkerheit for 2024 at tal på mobiltelefonar i bruk i føretaka aukar, og fleire av desse blir ikkje forvalta av Helse Vest IKT. Dei ventar at talet vil fortset å auke og at det kan utgjer ein risiko.

CISO i Helse Bergen peiker på at dei opplever at det er uklarheiter rundt styringa av informasjonssikkerheit i felles IKT-infrastruktur, kor både ansvar og oppgåver er lagt til Helse Vest IKT utan særleg involvering av sjukehusa. Dette kan vere utfordrande med tanke på føretaka sine roller som dataansvarleg. CISO i Helse Stavanger viser til styresaka i Helse Vest RHF kor rollene som dataansvarleg og databehandlar blei avklart[63], og at Helse Vest IKT har ansvar og *styringsmyndigheit* for IKT-infrastruktur. Han meiner at dette kan utfordre et typisk forhold mellom databehandlar og dataansvarleg kor databehandlar vanlegvis berre følgjer instruks.

Helseføretaka har ansvar for planlegging, utvikling og drift av bygg og anlegg, inkludert MU og andre fasilitetar som er nødvendige for at sjukehusa skal fungere. Når det blir bygd nye sjukehus eller større prosjekt blir sett i gang, blir det ofte etablert prosjektstyre eller samarbeidsorgan der både dei lokale helseføretaka og RHF-et er involvert, men hovudansvaret ligg lokalt. Helse Vest IKT vil likevel samarbeide tett med dei lokale helseføretaka for å sikre at den digitale infrastrukturen blir ivaretatt i byggjeprosessen, slik at alle IKT-løysingar fungerer som dei skal frå første dag sjukehuset blir tatt i bruk.

Det blei ikkje lagt vekt på dette temaet i intervju, men likevel var det eit av føretaka som løfta fram at sjølv om ansvarsforholda på mange måtar er avklarte, så kan ein oppfatte at det er uklare grenselinjer mellom kva helseføretaka skal gjere og kva Helse Vest IKT skal gjere i byggeprosjekt. Ved nybygg og større installasjonar har det vore nokre uklarleikar rundt kven som har ansvaret for å sikre at infrastrukturen fungerer slik som tiltenkt. Ansvaret er likevel forsøkt avklart i styresak 085/21 i RHF-et[63], og ein kan da problematisere om denne informasjonen har nådd alle relevante partar. Internrevisjonen vel å ta med dette i rapporten fordi det er store byggeprosjekt i regionen, og at ein da kan hindre gjentakingar. Dette kan gi indikasjonar på at ein har avklart dei ulike ansvara og rollene øvste nivå, men at det ikkje er like godt etablert lenger nede i organisasjonen og føretaksgruppa.

3.5.3 Medisinsk utstyr og teknisk utstyr

Riksrevisjonen undersøkte risikoen knytt til IKT-sikkerheit ved MTU[65] i norske sjukehus i begge rapportane som er omtalt i kapittel 2.1.1. Dei avdekte fleire store svakheiter, spesielt knytt til manglande styring og kontroll. Mange sjukehus hadde utdatert medisinsk utstyr som ikkje kunne oppdaterast med nødvendige sikkerheitsoppdateringar, noko som auka risikoen for hacking og tekniske feil. Dette utgjorde ein potensiell fare for pasienttryggleiken. I tillegg var det svakheiter i korleis sjukehusa vurderer risiko og rutinar for vedlikehald og oppdatering av utstyret. Det mangla tilstrekkeleg oversikt over kva system som var kopla til MTU, noko som gjer det vanskeleg å sikre seg mot truslar. Riksrevisjonen tilrådde at helsesektoren styrkjer den sentrale styringa av IKT-sikkerheit for MTU. Vidare anbefalte dei at ein bør oppdatera gammalt utstyr eller at det blir bytt ut slik at det oppfyller moderne sikkerheitskrav. Dei tilrådde at sjukehusa gjennomfører grundigare og meir regelmessige risikovurderingar for å redusere moglege farar.

I styresaka som er nemnt i dette delkapittelet[63] illustrerer dei omfanget av MU, TU og lokal IKT med utgangspunkt i Helse Bergen og Helse Fonna, altså eit stort og eit middels stort føretak[66]. Helse Bergen forvaltar delar av sin eigen IKT-infrastruktur, i tillegg til system levert av Helse Vest IKT. Dette inkluderer medisinsk og teknisk utstyr ved einingar som Medisinteknisk avdeling, Laboratorieklinikken, Teknisk avdeling, Kreftavdelinga, og i forskingsprosjekt. Medisinteknisk avdeling administrerer rundt 44 000 einingar for medisinsk utstyr og tilknytte IKT-system, med ein infrastruktur på ca. 60 serverar, 200 PC-ar og 110 brukarar. Spesialiserte einingar, som Kreftavdelinga, har eigne IKT-system, ofte i samarbeid med Helse Vest IKT AS, for å møte spesialiserte behov. Dei mindre føretaka har ikkje eit så stort omfang av MU/TU som Helse Bergen, men likevel har eksempelvis Helse Fonna MU med om lag 7 500 utstyrseiningar på sjukehuset og 10 500 behandlingshjelpemiddel, men alt er ikkje nettverkstilkopla. Rundt 350 einingar er registrerte i utstyrsportalen. TU har ca. 400 registrerte einingar i utstyrsportalen, inkludert videokamera, tekniske anlegg som SD-anlegg, inngangskontroll, bygningsautomatisering, betalingsterminalar og diverse alarmsystem[63].

[65] Merk at Riksrevisjonen bruker forkortelsen MTU, medan Helse Vest nyttar seg av MU. MTU = medisinsk-teknisk utstyr og MU = medisinsk utstyr. Store deler av sektoren elles har òg gått over til dette. Internrevisjonen nyttar MTU der ein omtalar Riksrevisjonen sine rapportar.
[66] Merk at tala er frå 2021, men er framleis aktuelt for å illustrere omfanget

Dette viser at sjølv om MU og TU er ein liten del av den totale porteføljen, så er omfanget som er lokalt forvalta stort. Mykje av utstyret er pasientnært, og kritisk for god behandling.

3.5.4 Forsking

Internrevisjonen har merka seg at forsking nyttar eigne system/IKT og verken føretaka eller Helse Vest IKT har særleg kontroll eller eigarskap over desse – internrevisjonen meiner at det utgjer ein risiko knytt til informasjonssikkerheit i føretaksgruppa.

I Riksrevisjonens rapportar, både dei som er omtalt i delkapittel 2.1.1 og ein rapport som blei offentleggjort i januar 2024 «Informasjonssikkerhet i forsking innenfor kunnskapssektoren» [7,8,67], er forsking, og særleg bruken av IKT i forskingssamanheng eit viktig tema. Dei peikar på at medisinsk forsking i sjukehus ofte nyttar MTU og IKT-system som handterer store mengder sensitive data. Dette skaper eit særleg behov for solide sikkerheitsmekanismar for å verne pasientdata og forskingsresultat. Rapportane viser til at forskingsprosjekt ofte bruker IKT-utstyr som kan vere dårleg integrert i dei overordna sikkerheitssystema på sjukehusa. Dette kan føre til risiko for sikkerheitsbrot, anten ved uautorisert tilgang eller ved svikt i tekniske system. I tillegg blir det nemnt at mange forskingsprosjekt blir drivne med utstyr som ikkje nødvendigvis følgjer dei same sikkerheitsskrava som anna medisinsk utstyr, noko som ytterlegare aukar risikoen. Dette blir og bekrefta i intervju med fleire av føretaka. I intervju med CISO og jurist i RHF-et blir det løfta fram at Helse Vest IKT leverer det kundane vil ha, og at det er lite spesifikt knytt til forsking. Helse Vest IKT sjølv seier at dei trenger IKT-infrastruktur knytt til forsking, men at det ikkje er satt av ressursar til det, at det verker tilfeldig og ikkje satt i system som gir eit risikobilete dei ikkje ønskjer å ha. Helse Bergen seier òg at dette er eit veldig svakt område. Internrevisjonen merkar seg vidare at forsking ikkje er nemnt i den regionale handlingsplanen for informasjonssikkerheit[43]. Direktør for e-helse i RHF-et seier at det er eit område som har sterk tilknyting til universitetsmiljøa med eigne løysingar og system, som gjer det enda vanskelegare å handtere med tanke på informasjonssikkerheit.

3.5.5 Føretaka sitt arbeid med å ha oversikt

Internrevisjonen deltok i møte i SU 25.04.2024 kor gjennomgang av dokumentførespurnaden for revisjonen var eit tema. Følgjande punkt (ikkje uttømmande liste) var inkludert i førespurnaden:

- Prosess for å kartleggje einingar og programvare som er i bruk i føretaket
- Oversikt over einingar og programvare som er i bruk i føretaket
- Prosess for å kartleggje leveransar, informasjonssystem og understøttande IKT-funksjonar
- Oversikt over leveransar, informasjonssystem og understøttande IKT-funksjonar
- Prosess for å kartleggje informasjonsbehandling og dataflyt i føretaket
- Oversikt over informasjonsbehandling og dataflyt i føretaket

[67] Sensitive forskningsdata kan komme på avveie (riksrevisjonen.no)

SU stilte spørsmål til desse punkta, og viste til at helseføretaka er store, komplekse organisasjonar som gjer at det er vanskeleg å få desse oversiktene. Eit føretak sa i møte at dei ikkje har oversikt, og eit anna sa at det ikkje handlar om at dei ikkje har oversikta, men at det er veldig store og komplekse punkt.

Eit tiltak i den regionale handlingsplanen for informasjonssikkerheit[43] er kjøp av verktøy for deteksjon av einingar i nettverket, for å oppnå målet om å ha evne til å automatisk detektere og identifisere all utstyr som er kopla til nettverket. Ein hadde opphavleg ikkje finansiering til det, men i møte i SU 17. oktober 2024 blei det orientert om at Helse Vest IKT har fått det i budsjettet for 2025, budsjettet er per no ikkje vedtatt. SU har nominert ein person til å hjelpe Helse Vest IKT med anskaffinga. I handlingsplanen blir det poengtert at denne løysinga vil vere til stor nytte for alle HF-a med utstyr kopla i datanettet, MU, TU og IKT-utstyr, -system og -tenester som blir forvalta lokalt i verksemdene[43]. Eit mål i handlingsplanen handlar om å ha oppdatert oversikt over eigen IKT-infrastruktur med tiltaka «etablere og vedlikeholde lokal oversikt over IKT» og å «etablere hensiktsmessige integrasjoner». Internrevisjonen meiner det er viktig at dette inngår i den regionale handlingsplanen.

Svara på dokumentførespurnaden varierer, fleire peiker på at det meste som er i bruk er registrert og forvalta av Helse Vest IKT, men likevel er det òg eit føretak som kommenterer at det er for komplekst å svare på. Helse Stavanger skriv at dei baserer seg på at lokale einingar/arbeidsområde har sine lokale oversikter, og at dei ventar på den regionale løysinga som bygger på Helse Vest IKT sin Assyst før dei kan samle informasjonen. Helse Bergen har ulike oversikter, og viser til at dei ventar seg at dei ulike områda i styringsstrukturen vil ha eit ansvar for prosesser for kartlegging av leveransar, informasjonssystem og understøttande IKT-funksjonar. I Helse Fonna har ein oversikt over lokalt forvalta MU i Excelark.

Gjennom intervju med dei ulike føretaka ser vi at fleire av føretaka jobbar med å få oversikt over lokal IKT, men at det er ein tung prosess. CISO og jurist i RHF-et framhevar at ein må ta ansvar for å dokumentere ei foreløpig oversikt over lokal, fram til den regionale løysinga kjem. Det er ulikt i kva grad føretaka gjer dette. I Helse Bergen legg dei vekt på at dei har lite lokal IKT (ca. 10%), men som poengtert i kapittel 3.5.2 kan ein liten del lokal IKT utgjer eit stort omfang. Mangel på ressursar blir framheva, og føretaket sjølv meiner dei ikkje har kapasitet til å gjere dette. I Helse Fonna har dei om lag 5% lokal IKT, og dei opplever å ha god kontroll på MU, men ikkje like god kontroll på TU. Helse Førde seier òg at det er lite som er lokalt forvalta, MU har blitt betre på å opplyse kva dei har av system, medan teknisk er så som så. I Helse Stavanger har dei ulike avdelingane oversikt, men det er ikkje ein fullstendig oversikt for heile føretaket. Helse Vest IKT seier dei har ein veg å gå når det gjeld å få oversikt over alt, og at ein er avhengig av å samarbeide med HF-a om det. Internrevisjonen meiner føretaka bør jobbe med å få ein oversikt over lokal IKT, sjølv om dette kan vere ein stor og tung jobb. Dette som følgje av rolla ein har som føretak som dataansvarleg, ref. kapittel 2.5 og 3.4.3.

Det er sårbarheiter og gamal teknologi knytt til MU, dette løftar Helse Bergen fram i intervju. Sjukehusapoteka Vest viser vidare til at ein kan nytte IKT som aldri har blitt risikovurdert. Likevel blir det og uttrykt av direktør for e-helse i RHF-et at ein nyttar seg av empiri i form av meldte avvik, og at ein da kan sjå kva som er risikoane knytt til eldre IKT. Avvikshandtering er ikkje ein del av formålet og problemstillingane i denne internrevisjonen, og vi har derfor ikkje undersøkt dette ytterlegare.

Internrevisjonen ser vidare at det kan vere utfordringar knytt til ansvarsfordelinga mellom ulike avdelingar i helseføretaka. Det er oppretta regionale fora for MU og TU, og fleire løftar fram i intervju at dei håper at dette vil bidra til betre kontroll og at ein blir klar over ulike svakheiter. Internrevisjonen meiner CISO må samarbeide med dei som handterer oversikt og innkjøp av MU og TU i føretaka for å sikre informasjonssikkerheit på området. Føretaka bør samarbeide med Helse Vest IKT ved innkjøp. Støtte og forankring hos leiinga vil òg her vere ein fordel, jf. kap. 3.2.5.

3.5.6 Anskaffingar

Eit anbefalt tiltak i NSM sine grunnprinsipp for IKT-sikkerheit er å integrere sikkerheit i prosessen for anskaffingar i verksemda.[68] I intervju er det fleire av føretaka som framhevar at det er svakheiter knytt til anskaffingar. CISO i Helse Vest IKT seier at det er ein aukande mengde anskaffingar som skjer utan involvering av Helse Vest IKT. Internrevisjonen ser på dette som ein svakheit.

Anskaffingar og avtaleforvaltning er i alle hovudsak organisert inn under Sykehusinnkjøp HF. Sykehusinnkjøp er eigd av dei RHF-a og leier anskaffingsprosessane innanfor nesten alle område i spesialisthelsetenesta, for eksempel IT-utstyr, legemiddel og MU. Sjølv om Sjukehusinnkjøp er leiar for innkjøpsprosjekta gjer dei det i tett samarbeid med spesialistgrupper sett saman av relevant fagpersonell frå HF-a[69].

I den regionale handlingsplanen for informasjonssikkerheit[43] er eit mål å sikre at det blir stilt gode krav til informasjonssikkerheit og personvern i anskaffingar av IKT-einingar, -ustyr, -tenester og -system. Det er viktig å avklare kva løysinga/systemet skal bli brukt til på forhånd. Det er fleire tiltak knytt til dette målet; «revidere IT-krav», «revisjon av MU-krav og TU-krav», «revidere krav til informasjonssikkerhet og personvern ved anskaffelser» og å «gjøre kravene tilgjengelige for virksomhetene, og gi opplæring og støtte i bruk av obligatoriske sikkerhetskrav i virksomhetene». Tiltaka inneber eksempelvis reviderte, regionale TU- og MU-innkjøpsmalar i MU-IKT- og TU-IKT-fora, og at desse må bli kommunisert til relevante partar. Internrevisjonen meiner dette er hensiktsmessige tiltak knytt til anskaffingar.

[68] NSMs Grunnprinsipper for IKT-sikkerhet v2.1.pdf – kapittel 2.1, anbefalt tiltak 2.1.1.
[69] Om oss - Sykehusinnkjøp HF (sykehusinnkjop.no)

Det er viktig å inkludere temaet informasjonssikkerheit så tidleg så mogleg, og at denne kompetansen er med gjennom heile anskaffinga, samt i den løpande forvaltinga av avtalane. I tillegg til å samarbeide med Helse Vest IKT ved innkjøp, som nemnt i kapittel 3.5.5.

3.5.7 Oppsummering av funn knytt til oversikt over IKT

Funna våre indikerer at det framleis står att ein stor jobb med å forbetre forvaltninga av både lokal IKT (inkludert infrastruktur), forsking og medisinsk utstyr (MU) i helseføretaka. Fleire tiltak er pågåande, men mykje arbeid står att.

Det er viktig å merke seg at mesteparten av IKT i Helse Vest er sentralt forvalta, og sjølv i eit stort helseføretak som Helse Bergen HF utgjer lokal IKT under 10% av den totale porteføljen. Likevel kan dette området, som påpeika av Riksrevisjonen, utgjere eit risikoområde for informasjonssikkerheit både lokalt, og i Helse Vest. Til liks med lokal IKT og forsking, så har både MU og TU (teknisk utstyr) ein lokal forankring som gjer at området i stor grad fell utanfor sentral forvaltning. Både forsking og MU/TU er gjerne organisert i eigne avdelingar, som gjer det vanskelegare for CISO å bli inkludert i deira arbeid. Føretaka må også her vere klar over rolla si som dataansvarleg. Sjølv om Helse Vest IKT har informasjonssikkerheit i IKT-infrastruktur som ein del av sine arbeidsoppgåver bør RHF-et løfte diskusjonen om korleis føretaka skal vere involvert, og bli orientert om dette arbeidet. Internrevisjonen meiner det er viktig å inkludere temaet informasjonssikkerheit så tidleg så mogleg i anskaffingar, og at denne kompetansen er med i heile prosessen. Føretaka bør òg involvere Helse Vest IKT i anskaffingane.

3.6 Risikostyring

Dette kapittelet handlar om risikostyring av informasjonssikkerheit i føretaksgruppa, inkludert roller og ansvar, metodikk som blir nytta, krav til risikovurderingar, toleransegrenser, tiltak, oppfølging, oppdatering, evaluering og rapportering. NSM presiserer at manglande styringsstruktur og prosesser for risikovurdering kan føre til at leiinga ikkje får tilstrekkeleg informasjon til å prioritere og styre verksemda sitt arbeid med sikkerheit[70].

Internrevisjonen fekk ei liste over ein populasjon som inkluderte alle risiko- og sårbarheitsanalysane (ROS) som er gjennomført og fasilitert av ROS-teamet i Helse Vest i notid og fleire år tilbake i tid. Vi tok eit tilfeldig utval[71] og fekk tilgang til dei utvalde analysane i SharePoint. Dette har gitt oss nyttig informasjon til både intervju og vurdering av korleis risikostyringa av informasjonssikkerheit er i Helse Vest.

[70] Kartlegg styringsstrukturer, leveranser og understøttende systemer - Nasjonal sikkerhetsmyndighet (nsm.no)
[71] Metode: Tilfeldig utvalg-funksjon i MS-Excel

3.6.1 Roller og ansvar knytt til risikostyring

Under har vi samla dei relevante rollane for risikostyringa knytt til informasjonssikkerheit, med beskriving av deira ansvar:

- **Systemforvaltar:** Ansvarleg for drift og vedlikehald av eit system der systemeigaren representerer fleire verksemder. Ansvarleg for å ivareta dei spesifikke krava verksemda har til systemet og sørgje for at alle involverte verksemder oppfyller sine forpliktingar i samsvar med avtalen.[72]

- **Risikoeigar/systemeigar:** Den ansvarlege leiar («eigar») av eit informasjonssystem. Det er systemeigar som er bestiller, og som avgjer formålet med innsamling og bruk av informasjon i eit informasjonssystem.[72] Har ansvar for å avgjere om ein risiko er akseptabel.

- **Systemansvarleg:** Har ansvaret for å koordinere og administrere implementeringa, drifta og vedlikehald av systemet.

- **Risikoansvarleg**: Risikoar i raudt eller gult område skal ha ein risikoansvarleg, og personen har da ansvaret for oppfølging av tiltak, men kan delegere gjennomføringa[73] til **tiltaksansvarleg**.[74]

- **ROS-team:** Ligg i seksjon for IKT-sikkerheit i Helse Vest IKT. Desse fasiliterer lokale og regionale (to eller fleire føretak) analysar for føretaka med planleggingsmøte, gjennomføring med arbeidsmøte og rapport.

- **SU**: Regionalt informasjonssikkerheitsutval får tilsendt endelege ROS-rapportar til gjennomgang i møte.

3.6.2 Metodikk

Det er typisk systemforvaltarar og systemeigarar som legg inn bestillinga til ROS-teamet. ROS-analysane blir gjennomført ved at ein har eit (i nokre tilfelle fleire) arbeidsmøte med presentasjon av systemet og idémyldring for å identifisere uønskte hendingar som kan oppstå.

I arbeidsmøte er det fleire deltakarar, for eksempel CISO-ar, personvernombod, brukarar av systemet og systemeigarar. Ein vurderer sannsyn for at hendinga vil skje frå svært liten til svært stor (1-5). I samband med denne vurderinga ser ein på tiltaksstatus, interne/autoriserte ressursar, eksterne/uautoriserte ressursar og frekvens.

[72] Dokument «Ordliste og definisjoner» i Styringssystemet for informasjonssikkerhet og personvern
[73] Henta frå SharePoint-sida HVI-ROS: «Ditt ansvar som systemeier» / «Risikovurdering – sentrale begrep og ansvar»
[74] Dokument «Risikostyring» i Styringssystemet for informasjonssikkerhet og personvern

Vidare vurderer ein konsekvensen frå ubetydeleg til svært alvorleg/kritisk (1-5) både knytt til tilgjengelegheit, konfidensialitet, integritet, personvernkonsekvens, HMS/pasienttryggleik og omdømme.[75] Dette er i tråd med Normen[76]. Summen av sannsyn og konsekvens blir presentert i ei risikomatrise med fargene grøn, gul og raud. I arbeidet med risikovurderingar som er fasilitert av ROS-teamet kan ein sjå risikomatrisa før ein har gjort risikoreduserande tiltak, og ei ny matrise etter at desse er gjennomført. Risikomatrisa til ROS-teamet er den same som den felles risikomatrisa som er behandla i direktørmøte[77]. All dokumentasjon knytt til ROS-analysane for informasjonssikkerheit ligger på SharePoint.

Risikovurderingane og arbeidsmøta er ressurskrevjande med mange deltakarar (i intervju blir det opplyst at det kan vere så mange som 40 deltakarar i eit møte). Fleire uttrykker at ein burde endre metodikken og korleis ein arbeider. Det blir foreslått i intervju at ein kunne hatt sjekklister med kva som er innfridd/bør vere innfridd før fasilitering, og kva ein bør sjå nærare på i eit (mindre) arbeidsmøte.

Poenget er at ein ikkje burde ha behov for å gjere risikovurderingar for å kome fram til at ein eksempelvis må tilgangsstyre eit system. Merk at det er ein forenkla risikovurdering som er sjekklistebasert utan at ROS-teamet fasiliterer gjennomføringa, men denne er berre mogleg å bruke om det gjelder små fagsystem med få brukarar og pasientar.

I eit intervju blir det sagt at det er ein viss grad av subjektivitet i ROS-analysane, til tross for at ein har standardisert metodikk. Mange deltakarar i ROS-analysane er noko som kan bidra med å redusere subjektiviteten på vurderingane som blir gjort. Utfallet av analysane er avhengig av kven som er med. Det er likevel viktig å få fram at fleire seier at kompetansen til ROS-teamet er god og at dei fasiliterer ROS-analysane på ein god måte. I intervju er det likevel ein som kommenterer at det er viktig at ROS-teamet klarer å holde fokus på dei riktige risikoane, spesielt på grunn av alle deltakarane som er med i møta og som kan lufte sine bekymringar. Nokre av desse risikoane kan gå utanfor informasjonssikkerheit og personvern.

I den regionale handlingsplanen for informasjonssikkerheit[43] er eit punkt om forbedra risikostyring, der målet er å ha ein forbedra og meir effektiv risikostyring for informasjonssikkerheit og personvern. Ein ønskjer å forbetre ROS-prosessar og verktøy for å styrke risikostyringa, inkludert betre eigarskap og oppfølging av risiko og tiltak, og å samanstille risiko på verksemdnivå. Dei skriv at det er nødvendig å avklare grenseoppgangen mot styringsstruktur for digitalisering når det kjem til risikoar som går på tvers av dei ulike verksemdene sine ansvarsområde.

[75] Risikomatrise: Risikovurdering satt i system (sharepoint.com)
[76] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap.3.4. Risikovurdering og risikohåndtering
[77] Direktørmøte i Helse Vest RHF 21.08.2023

Det er laga to tiltak; «Synergi for risikostyring, sammen med modulen Cyber Risk i Synergi» som blir omtalt i kapittel 3.6.9, og «Revidere metodikk for ROS» i handlingsplanen[43]. Det siste tiltaket er nødvendig for å tilpasse ROS-prosess og metodikk til å understøtte behova til verksemda. Dette inneber gjennomføring av risikovurderingar, handtering og oppfølging av risikoar i etterkant. Verksemdene må sørgje for at ein ivaretar ei heilskapleg risikostyring for informasjonssikkerheit. Det bør vidare bli sett i samanheng med tertialsvis/kvartalsvis rapportering på risiko for informasjonssikkereit i den ordinære oppfølginga av verksemda. Handlingsplanen viser og til den forenkla ROS-metodikken, som er omtalt tidlegare i delkapittelet, kor dei bør sjå om det er element av denne som kan bli brukt i fleire ROS-analysar saman med formalisering av oppfølging av forenkla risikovurderingar. Representanten frå ROS-teamet seier i intervju at dei har behov for fleire skriftlege krav som dei kan halde seg til.

3.6.3 Krav til gjennomføring av risikovurderingar

I Normen er det følgande krav til gjennomføring av risikovurderingar:

«Virksomheten skal gjennomføre risikovurderinger, og de skal som minimum gjennomføres før:

- etablering av eller endring i behandling av helse- og personopplysninger
- etablering av nye systemer eller registre som inneholder eller benytter helse- og personopplysninger
- det etableres organisatoriske, tekniske eller andre endringer med betydning for informasjonssikkerheten
- det etableres eller endres tilgang til helseopplysninger mellom virksomheter»[76]

Internrevisjonen stiller spørsmål om det faktisk blir gjennomført risikovurderingar ved alle dei nemnte tilfella som står i Normen. På SharePoint kan ein lese om risikovurderingar generelt, og ei fane har overskrifta «Om risikovurdering». Her merkar internrevisjonen seg at det står «Ved *innføring av nytt system* er det systemeiers ansvar å påse at risiko- og sårbarhetsanalyse er gjennomført, og påse iverksetting av nødvendige tiltak». Det blir sagt i intervju at ein burde hatt fokus på å risikovurdere dei systema som allereie er i bruk, ein har eksempelvis gamle system som kanskje aldri har blitt risikovurdert. Internrevisjonen merkar seg likevel at Helse Vest IKT skriv i leiinga sin gjennomgang for 2023 at risikovurdering ser ut til å ha blitt ein naturleg del av innføring eller *endring* av system.

I Sjukehusapoteka Vest sin leiinga sin gjennomgang for informasjonssikkerheit for 2023 viser dei til ein prosess som heiter «Ivareta endringskontroll». Dette handlar om å ivareta vurdering og gjennomføring av ein endring på eit system gjennom endringsmelding. Her kjem prosessen «planlegg og gjennomfør risikovurdering». Fagdirektør i Sjukehusapoteka Vest bekreftar i intervju at dei gjennomfører risikovurderingar ved endringar.

Helse Vest IKT nyttar ITIL-rammeverket[78], og har ein prosess for endringar. Denne prosessen skal sørgje for at alle endringar mot produksjonssette tenester blir styrt for å redusere risiko for negative konsekvensar[79]. Endringsprosessen inneber blant anna å gjere ein risikovurdering av endringa[80].

3.6.4 Toleransegrenser

Det er leiinga som skal fastsette kriterium for å akseptere risiko[54], og kva som er akseptabel og uakseptabel risiko for verksemda[81]. Alle føretaka har policy for akseptabel risiko[82] i sitt styringssystem. Risikoar som er grøne i risikomatrisa er akseptable, dei gule er ikkje akseptable og ein må vurdere om det er behov for risikoreduserande tiltak, mens dei raude risikoane ikkje er akseptable og ein skal gjennomføra tiltak for å få risikoen på eit akseptabelt nivå. I løpet av arbeidsmøte med ROS-teamet blir det peika ut risikoansvarlege som skal følgje opp dei gule og røde risikoane. For dei gule risikoane blir det ei vurdering av kost/nytte om ein skal gjennomføre risikoreduserande tiltak, i tråd med Normen[83].

Sjølv om det er fastsett grenser for akseptabel risiko er det ulikt kva som blir akseptert og dokumentert. Fleire element blir tatt opp i intervju, blant anna at dokumentasjon på kva som er akseptert og kven som har akseptert er ei svakheit, at ein kan redusere ein risiko frå raud til gul utan å dokumentere om noko er gjort og at system blir tatt i bruk utan at dei raude risikoane er godkjent av systemeigar. Ein CISO opplyser i intervju at dei har opplevd at både sannsyn og konsekvens er justert, utan at det er dokumentert kvifor. Fagdirektørar, som ofte er systemeigarar, opplyser likevel i intervju at dei er nøye på at system som har raude risikoar ikkje skal bli tatt i bruk. I intervju med ein CISO og ein IKT-sjef seier dei at ein ikkje går i gang med system som har «altfor mange raude risikoar». Riksrevisjonen fann ut at CISO-ane i HF-a meinte at dei som aksepterte risikoane i verksemda ikkje alltid var bevisst på ansvaret sitt, i tillegg til at det i mange tilfelle var uklart kven som kunne akseptere risikoen og at mange ikkje veit kva det inneber å vera systemeigar[8].

3.6.5 Risikoreduserande tiltak

Å etablere eller justere tiltak for å redusere risiko er sentralt i risikostyring[84]. Har ein kome fram til at det skal bli gjennomført risikoreduserande tiltak, skal desse kome fram i ein eigen plan med tydeleg frist og kven som er tiltaksansvarleg for gjennomføring. Denne planen skal vere forankra hos leiinga[76].

[78] ITIL, Information Technology Infrastructure Library, skildrar dei ulike områda for arbeidsprosessar hos ein IT-leverandør (jf. Styringsdokumentet til Helse Vest IKT for 2024, fotnote 40 i revisjonsrapporten)
[79] Endringsprosessen – Hjem – SharePoint-side
[80] Endringsveilederen - Helse Vest IKT
[81] NSMs Grunnprinsipper for IKT-sikkerhet v2.1.pdf Anbefalt tiltak ID 1.1.4
[82] «Nivå for akseptabel risiko» - policy i styringssystemet til Helse Vest RHF. Tilnærmet lik for alle føretaka.
[83] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – Kap.3.1 Forholdsmessighet ved valg av tiltak
[84] NSMs Grunnprinsipper for IKT-sikkerhet v2.1.pdf Anbefalt tiltak ID 1.1.3

Riksrevisjonen skreiv i rapporten som blei offentleggjort i 2020 at det er mange gjennomarbeida risikoanalysar, kor ein ser både risikonivå, sannsyn og konsekvens, tiltak, kven som har ansvar for tiltaka og tidsfrist for når tiltaka skal bli gjennomført. Men, dei fant og at fleire av analysane mangla nærare omtale om nokre av tiltaka, kven som er ansvarleg for gjennomføring og/eller frist.[8] I vår gjennomgang ser vi det same. I risikolista ligg det både risikonivå, sannsyn og konsekvens, tiltak, kven som har ansvar for tiltaka og tidsfrist, men vi ser at ein del av analysane manglar tiltaksansvarleg og frist. Dette gjelder òg analysar som er gjennomført etter at rapporten til Riksrevisjonen blei offentleggjort.

I SharePoint, kor all informasjon om risikoanalysane skal bli lagra, er det ei liste som heiter tiltaksliste. Denne har blitt nytta i få tilfelle, og i fleire av tilfella der den har blitt nytta er ikkje tiltaka dokumentert fylgt opp/ferdig utført, ref. kapittel 3.6.6 under. Internrevisjonen har ingen dokumentasjon på at tiltakslister er forankra hos leiinga, nokre av føretaka har tiltakslister i leiinga sin gjennomgang, sjå kapittel 3.7.

3.6.6 Oppfølging og evaluering

ROS-teamet har ikkje ansvar for å følgje opp risikovurderinga, og når tiltak er implementert skal risiko- eller tiltaksansvarleg sjølv oppdatere status på risikoen. Ein del av risikostyringa er å følgje opp og verifisere at risikoreduserande tiltak fungerer som planlagt[84]. I Helse Vest er det risikoansvarleg som har ansvar for oppfølging av tiltak, men gjennomføring kan bli delegert til tiltaksansvarleg, sjå kapittel 3.6.1 for roller og ansvar.

I rapporten til Riksrevisjonen blei det påpeika at CISO-ane ikkje hadde oversikt over korleis tiltaka HF-a hadde ansvar for blei fylgt opp ute i klinikkar og avdelingar[8]. Oppfølging av tiltak er ei av svakheitene som kjem fram i intervjua internrevisjonen har gjennomført. Det blir sagt at ein har fokus på å lukke risikoar, men ikkje nødvendigvis å oppdatere og ha kontroll på kva som framleis er ein risiko.

I gjennomgangen av risikoanalysar ser vi at det manglar oppfølging av tiltaka, for nokre av tiltaka står det for eksempel at dei berre er 50% fullført, sjølv om risikoanalysen blei gjennomført for ei stund tilbake og rapporten for risikoanalysen er ferdig. Det er heller ikkje dokumentert at tiltaka blir evaluert. Helse Stavanger skriv følgjande i sitt svar på dokumentførespurnaden at «Ansvar for oppfølging av risiko og vurdering av tiltak er p.t. hovedsakelig lagt til systemeier, men er i praksis et resultat av konsensus mellom systemforvalter, systemeier, og systemansvarlig, samt evt. andre kyndige interesser (programstyre/digitaliseringsstyre, klinikkledelse, IKT leder, informasjonssikkerhetsleder mfl.). Dette varierer i stor grad fra vurdering til vurdering og vi håper at innføring av cybermodulen i Synergi vil hjelpe med automatisering av denne type oppfølging». Slik internrevisjonen ser det bør ein tydeleggjere kven som faktisk skal følgje opp og dokumentere.

I Helse Bergen har dei tatt initiativ til å følgje opp raude risikoar. Dei har trekt ut alle raude risikoar frå SharePoint. I Intervju med representant frå ROS-teamet blei det saget at dette er noko Helse Vest IKT og ROS-teamet ønskjer å få til for heile Helse Vest. Helse Bergen ser på alle desse risikoane og følgjer opp om desse har tilhøyrande risikoreduserande tiltak som er gjennomført. Dei har involvert dei andre føretaka der det har vore relevant. CISO i Helse Fonna opplyser om at dei har oppretta ei gruppe som skal sjå til at tiltak er passande og at dei blir fylgt opp. I Normen er det i tillegg at krav om at plan for oppfølging av tiltak skal bli kommunisert på rett detaljnivå til leiinga i verksemda og eventuelt styret der det er relevant[76]. Internrevisjonen kan ikkje bekrefte eller avkrefte at dette er tilfelle.

3.6.7 Oppdatering av risikoanalysar

I samsvar med Normen skal risikovurderingane bli oppdatert når det er endring i trusselbilete[76]. Alle CISO-ane er kjend med og arbeidar med ein årleg rapport om det digitale trusselbilete mot spesialisthelsetenesta[5]. Det blir i intervju påpeika at oppdatering av risikoanalysar er ei svakheit. Internrevisjonen ser at Helse Bergen, Helse Fonna, Helse Førde, Sjukehusapoteka Vest og Helse Vest IKT omtalar trusselbilete i leiinga sin gjennomgang for informasjonssikkerheit og personvern, og at ein er bevisst på kva som skjer utanfor verksemda sin kontroll. Den årlege rapporten om det digitale trusselbilete har blitt presentert for leiinga og/eller styret i enkelte føretak. Eit av tiltaka i den regionale handlingsplanen for informasjonssikkerheit[43] er å bruke trusselvurderinga for spesialisthelsetenesta[4,5] i eigen verksemd, og å leggje denne til grunn for arbeidet med sikkerheit og risikostyring. Internrevisjonen merkar seg at ein av ROS-analysane i utvalet hadde kommentar om at ein måtte revidere analysen ved endring i trusselbilete, men ein ser likevel ikkje dokumentasjon eller teikn på dette.

3.6.8 Aggregert risikobilete

I Riksrevisjonen sin rapport om «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-*system» (kapittel 6.7.3)*[8] *var eit av funna at føretaka har ein del informasjon knytt til risiko, men at dette ikkje blir* samanstilt i ein overordna risikoanalyse på verksemdsnivå. I Riksrevisjonens rapport om Helseplattforma[85] peikar dei også på alvorlege svakheiter i styring og risikohandtering. Eit av hovudpunkta dei trekker fram, er at risikovurderingar og -handtering var desentralisert. Dette innebar at ulike avdelingar og einingar gjennomførte sine eigne vurderingar utan ein sentral eller overordna oversikt. Resultatet blei ei fragmentert risikostyring utan eit heilskapleg risikobilde som kunne rettleie strategiske avgjerder eller varsle om overordna risikoområde. Konsekvensen av denne strukturen var at kritiske risikoar, særleg dei med potensiell innverknad på heile implementeringa, heldt fram med å vere uadressert eller blei handtert på ein måte som ikkje fanga opp kompleksiteten i prosjektet. Riksrevisjonen framhevar at dette bidrog til at problema fekk utvikle seg og eskalere trass i fleire åtvaringar. Utan ei konsolidert risikovurdering blei det umogleg for leiinga og styret å ha tilstrekkeleg innsikt i korleis samla risiko påverka framdrifta og resultata av prosjektet. Riksrevisjonen påpeikar også at styret dermed ikkje hadde eit fullstendig avgjerdsgrunnlag, noko som gjorde det utfordrande for dei å gripe inn eller sette inn nødvendige korrigerande tiltak.

[85] Riksrevisor: Sterk kritikk mot Helseplattformen

Styret har ansvar for å sikre god styring og kontroll, men desentralisert risikohandtering reduserte deira evne til å ta informerte avgjerder og sjå til at Helseplattforma blei implementert på ein sikker og effektiv måte. Internrevisjonen har gått gjennom leiinga sin gjennomgang for informasjonssikkerheit (og personvern) for alle føretaka over fleire år, ref. kapittel 3.7, og vi ser at det er vanskeleg å gi eit aggregert risikobilete, dette blir òg framheva i intervju. Helse Bergen er det einaste føretaket som skriv om samla risikonivå for enkelte områder, eksempelvis IKT-systema.

Eit krav i Normen er «I tillegg skal virksomhetens ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten»[76]. Dette kan vere vanskeleg om ein ikkje har eit aggregert risikobilete. Det blir likevel sagt i intervju av administrerande direktørar og fagdirektørar at leiinga sin gjennomgang for informasjonssikkerheit og personvern vil vere kvalifisert for å dekke dette kravet. Internrevisjonen stiller spørsmål ved om årleg gjennomgang er jamleg og detaljert nok, og leiinga bør gjere ei dokumentert vurdering av om dei sjølv meiner dette er godt nok. Eit av tiltaka i den regionale handlingsplanen for informasjonssikkerheit[43] er at alle verksemdene skal rapportere om risiko knytt til informasjonssikkerheit i den ordinære verksemdsrapporteringa anten kvartalsvis eller tertialsvis[43]. Internrevisjonen meiner dette er eit godt tiltak.

3.6.9 Verktøystøtte

Som nemnt tidlegare i kapittelet så nyttar føretaka seg av SharePoint til dokumentasjon av alt som har med ROS-analysar å gjere. I leiinga sin gjennomgang for informasjonssikkerheit i 2023 skreiv Helse Vest IKT at det er utfordringar knytt til funksjonaliteten ved oppretting av ROS-områder og rapportutforming med mykje manuelt arbeid og mange operasjonstrinn. I den samanheng kan det oppstå mange feil, i tillegg er det lite effektiv bruk av arbeidskapasitet. Dei har heller ikkje moglegheit til å hente ut eit overordna risikobilde. Internrevisjonen har som nemnt vore gjennom fleire ROS-analysar på SharePoint og opplevde blant anna at funksjonane i verktøyet ikkje var nytta fullt ut, jf. tiltaksliste i delkapittel 3.6.5.

I den regionale handlingsplanen for informasjonssikkerheit[43] har dei eit tiltak om «Synergi for risikostyring, sammen med modulen Cyber Risk i Synergi». Dette tiltaket handlar om å innføre Synergi som støttesystem for risikostyring, og at ein da skal bruke det til aktiv risikostyring av verksemda, og ikkje berre til dokumentasjon av utførte ROS for informasjonssikkerheit og personvern. Her blir det nemnt at verksemdene har behov for å ha oversikt over totalt aggregert risikobilete, ref. kapittel 3.6.8, og gjerne brote ned på einingar og ansvarlege. Fleire av intervjuobjekta løftar den kommande funksjonen i Synergi, og at denne skal gi ein meir systematisk tilnærming til risikostyringsprosessen. Representanten internrevisjonen har intervjua frå ROS-teamet seier at det ikkje nødvendigvis vil gjere jobben til ROS-teamet enklare, i tillegg seier andre intervjuobjekt at ein kan stille spørsmål om eit verktøy vil gjere det betre og at ein er usikker på om aggregering er mogleg.

Direktoratet for økonomistyring har ein rettleiar i internkontroll[86] kor eit av kapitla er «Hvordan utføre internkontroll?». Eit av momenta her er implementering, som ein eksempelvis kan overføre til det å implementere verktøystøtte. Det er fleire faktorar som er av betyding for ei vellykka implementering. Tonen frå toppen er viktig, saman med informasjon, kommunikasjon, kompetanse, ferdigheiter og kapasitet. Internrevisjonen meiner det er viktig å gjere implementeringa av verktøyet på ein grundig måte, kor ein sørgjer for tydelege rollemodellar og klar kommunikasjon om iverksetting, ansvar og krav til utføring.

Det er òg avgjerande at alle relevante partar har nødvendig kompetanse, ferdigheiter og kapasitet til å implementere verktøystøtta fullt ut. Dersom den kommande modulen i Synergi ikkje har moglegheit for aggregering, bør føretaka undersøkje om det er andre verktøy og moglegheiter for å få ein systematisk oversikt over risikoar knytt til informasjonssikkerheit på føretaksnivå.

3.6.10 Oppsummering av funn knytt til risikostyring

Risikovurderingar blir fasilitert av ROS-teamet med god kompetanse. Desse er i tråd med Normen, men likevel ressurskrevjande. Internrevisjonen meiner ein bør følgje tiltaket i den regionale handlingsplanen om ein forbetra metodikk, og sørgje for at det er tilhøyrande skriftlege krav til ROS-teamet. Internrevisjonen stiller spørsmål til om ein gjer risikovurderingar ved alle tilfelle og endringar som Normen listar opp. Det er tydeleg kva som er akseptabel risiko i styringssystem og i intervjua, men likevel set ein i gang system med raude risikoar, dei raude risikoane er redusert til gult utan dokumentasjon og liknande.

Internrevisjonen kan ikkje bekrefte at føretaka har planar med risikoreduserande tiltak (inkludert fristar og kven som er ansvarleg) som er forankra hos leiinga, at ein har evalueringar av tiltak eller oppfølging av analysane, og at tiltaka er inkludert i plan for oppfølging av tiltak som er kommunisert på rett detaljnivå til leiinga. Internrevisjonen vil likevel løfte fram at det er positivt med initiativet frå Helse Bergen om å følgje opp dei raude risikoane. Risikovurderingane skal bli oppdatert når det er endring i trusselbilete, noko internrevisjonen ikkje kan bekrefte er gjort.

Gjennom kapittel 3.6 er det nemnt fleire tiltak som ligger i den regionale handlingsplanen for informasjonssikkerheit[43], og internrevisjonen meiner desse er viktige. Eit av desse tiltaka er blant anna knytt til aggregert risikobilete, som er ein svakheit i dag. Dette gjer det meir utfordrande å integrere informasjonssikkerheit i den ordinære verksemdstyringa. Det kjem klart og tydeleg fram at føretaksgruppa gjer mange risiko*vurderingar*, men at det ikkje er risiko*styring.* Internrevisjonen meiner vidare, basert på fleire av funna, at det er uklart kva ansvar dei ulike rollene knytt til risikostyring har, og om systemeigarane er bevisst sitt ansvar for informasjonssikkerheit.

[86] 4.4 Implementering - DFØ (dfo.no)

Dette er noko som òg kan bli gjort tydelegare ved hjelp av dei tiltaksplanane Normen stiller krav om[76]. I handlingsplanen blir det løfta fram at ein skal få nytt verktøy for å betre risikostyringa, og internrevisjonen meiner det er vesentleg å få til god implementering av dette verktøyet.

3.7 Leiinga sin gjennomgang

Leiinga i føretaka skal gå gjennom aktivitetar innan informasjonssikkerheit og personvern minst ein gong i året[87]. I Normen står det:

«Gjennomgangen kan være nødvendig ved

- endringer i behandlinger av helse- og personopplysninger (protokoll)
- endringer i organiseringen av arbeidet
- resultat fra risikovurderinger og personvernkonsekvensvurderinger
- resultat av avviksbehandling
- oppfølging av leverandører og databehandleravtaler
- endring i akseptabel risiko mv.»[87]

Helse Bergen, Helse Fonna, Helse Førde, Sjukehusapoteka Vest og Helse Vest IKT har same prosedyre for leiinga sin gjennomgang i sitt styringssystem. Dette er ein gjennomgang som er dedikert til informasjonssikkerheit og personvern. Alle krava som kan tolkast ut frå Normen er inkludert i prosedyren for leiinga sin gjennomgang for desse føretaka. Det er likevel varierande om denne blir oppfylt for dei gjeldande føretaka. I Riksrevisjonen sin rapport «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-system» peika dei på at dei fleste HF-a hadde ein felles gjennomgang for mange verksemdsområde[8], men slik det har utvikla seg til no er det heller unntaket.

RHF-et og Helse Stavanger er dei føretaka i Helse Vest som ikkje har ein dedikert gjennomgang for informasjonssikkerheit og personvern, og informasjonssikkerheit blir inkludert i den ordinære gjennomgangen til verksemda. Det blir opplyst i intervju med Helse Bergen at dei vurderte denne løysinga sjølv, men administrerande direktør og føretakssekretariatet ville fortsette med ein eigen gjennomgang for å ha fokus på temaet. CISO i Helse Stavanger seier at informasjonssikkerheit er eit av mange tema i leiinga sin gjennomgang og at ein da forstår at pasienttryggleik blir prioritert. CISO i RHF-et opplyser om at dei skal innføre leiinga sin gjennomgang for informasjonssikkerheit og personvern frå 2025.

[87] Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse – 2.5. Ledelsens gjennomgang

I mandatet til SU[46] er ein av oppgåvene deira å sette saman ein regional rapport for leiinga sin gjennomgang av informasjonssikkerheit, og på den måten ha oversikt over tilstanden på sikkerheita og dei største risikoane knytt til informasjonssikkerheit i regionen. I den regionale handlingsplanen for informasjonssikkerheit er dette eit av tiltaka for å oppnå målet om å ha styring av informasjonssikkerheit som ein integrert del av ordinær verksemdsstyring. Det står at tiltaket skal bli gjennomført frå og med 2025, og er altså ikkje gjennomført per no.

Eit anna tiltak er at føretaka og Helse Vest IKT skal sende leiinga sin gjennomgang for informasjonssikkerheit til Helse Vest RHF etter at den er behandla i verksemda[43], da vil RHF-et vere orientert om arbeidet og risikobilde knytt til informasjonssikkerheit i resten av føretaksgruppa. Dette er òg eit argument for å samkøyre kva tid på året ein har leiinga sin gjennomgang for informasjonssikkerheit og personvern, jf. kapittel 3.2.3.

Internrevisjonen oppfattar leiinga sin gjennomgang å vere den formelle forma for rapportering til styret via leiinga. Vidare har CISO gjerne andre møtepunkt med leiinga i verksemda si, ref. kapittel 3.2.4. Internrevisjonen meiner ein bør sjå leiinga sin gjennomgang saman med det å ha tilgang til eit systematisk, aggregert risikobilete. Dette er noko som manglar, kvaliteten på den overordna gjennomgangen av informasjonssikkerheit ville ha blitt styrka om ein hadde det aggregerte risikobilete basert på systematiske data. Aggregert risikobilete er omtalt nærare under risikostyring i delkapittel 3.6.8. Internrevisjonen meiner alle føretaka bør ha eigen leiinga sin gjennomgang for informasjonssikkerheit.

4 KONKLUSJON OG TILRÅDINGAR

I denne revisjonen har internrevisjonen undersøkt om det er klare roller og ansvar for informasjonssikkerheit i Helse Vest, med særleg fokus på risikovurderingar og -styring. Vi har i hovudsak gjort vurderingar med bakgrunn i krav frå Normen som byggjer på ulike lovkrav.

Føretaka har dei siste åra hatt eit **aukande fokus på arbeidet med informasjonssikkerheit**, spesielt etter Riksrevisjonen sin rapport «Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer» som blei offentleggjort i 2020. Dette har blant anna resultert i ein **regional handlingsplan for informasjonssikkerhei**t, i tillegg til at informasjonssikkerheit var eit av **topp 5 risikoområde** i ein periode fram til april 2024. Det viser ei god tone frå toppen. **Det regionale informasjonssikkerheitsutvalet** (SU) blir løfta fram som eit godt fora for CISO-ane. Alle dei administrerande direktørane er klare på at det er dei som har det øvste ansvaret for informasjonssikkerheit, og at det er nødvendig for å sikre god pasienttryggleik. Internrevisjonen ser at forankring hos leiinga er vesentleg for å kunne gjennomføre arbeidsoppgåvene som CISO, og at dette varierer frå føretak til føretak. Det er òg ulikt kva møtepunkt CISO har med administrerande direktør og andre i leiinga.

Internrevisjonen merkar seg at sjølv om ein har avklart kva det inneber å vere **dataansvarleg og databehandlar** på øvste nivå, er det **indikasjonar på at dette ikkje er klart for alle relevante parter**. Føretaksgruppa bør jobbe med å tydeleggjere kva rolla som dataansvarleg inneber, og alle krav dette fører til, eksempelvis det å ha ei dokumentert oversikt over lokal IKT.

Helseføretaka har eigne **lokale IKT-løysingar som i all hovudsak ikkje er del av Helse Vest IKT si forvalting**. Dette omfattar for eksempel utstyr og system innanfor forsking, medisinsk utstyr (MU) og teknisk utstyr (TU). Det er variasjonar mellom føretaka i kor stor grad de har systematisert oversikt over system under eiga forvaltning.

Eit stort **forbetringsområde knytt til informasjonssikkerheit er risikovurderingar, og spesielt risikostyring**. Det blir gjort mange gode risikovurderingar, sjølv om dei kan vere ressurskrevjande, men det manglar styring og oppfølging. Inntrykket vi siter igjen med er at føretaka er gode på risiko*vurdering*, men har manglar innanfor risiko*styring*. Internrevisjonen kan ikkje bekrefte at det blir gjennomført risikovurderingar ved alle tilfelle som Normen stiller krav om, eller at desse blir fylgt opp. Det er eldre system som ikkje har blitt risikovurdert. Det manglar tiltaksplanar og planar for oppfølging av tiltak, samt at desse, på rett detaljnivå, er forankra hos leiinga. Det er **ikkje tydeleg kva ein skal gjere med raude og gule risikoar**, sjølv om dei fleste uttrykker at raude risikoar ikkje er akseptabelt. Det er **mangel på oppfølging av risikovurderingar**, og ein har heller ikkje evaluering av risikoreduserande tiltak. Føretaksgruppa **manglar moglegheita til å kunne sjå eit aggregert risikobilete** som, blant anna, ville gjort leiinga sin gjennomgang betre.

Det er ikkje alle som har ei eigen leiinga sin gjennomgang for informasjonssikkerheit, og ulike føretak har desse på ulike tider. I den regionale handlingsplanen for informasjonssikkerheit har RHF-et plan om å samanstille alle gjennomgangane.

Dei fleste CISO-ane vi har intervjua trekker fram at dei skulle hatt fleire ressursar i arbeidet med informasjonssikkerheit, da det blir fleire og fleire krav. Det er tydeleg at ein må gjere prioriteringar i spesialisthelsetenesta, og at dette òg omfattar arbeidet som ikkje er direkte pasientretta. Internrevisjonen vil ikkje gje anbefalingar om ressursar eller bemanning, men ser at fleire krav til CISO og andre som jobbar med informasjonssikkerheit gir behov for meir arbeidskraft.

Tilrådingane er gruppert etter tema, og vi ser at nokre av føretaka allereie følgjer desse tilrådingane, og at ein da kan lese desse som tilrådingar om å fortset med arbeidet. Tilrådingane kan vere retta mot RHF-et aleine, HF-a (Helse Bergen, Helse Fonna, Helse Førde, Helse Stavanger, Sjukehusapoteka Vest) og føretaka (heile føretaksgruppa, det vil seie RHF-et, Helse Bergen, Helse Fonna, Helse Førde, Helse Stavanger, Sjukehusapoteka Vest og Helse Vest IKT), ev. spesifikt til Helse Vest IKT åleine.

Tilrådingar gjeldande øvste leiing og styre;

- RHF-et bør vurdere å nytte seg av moglegheita til å kome med eigne krav i styringsdokument, ev. andre styrande dokument, gjeldande informasjonssikkerheit
- RHF-et og HF-a bør ha ei felles tilnærming på kva styresaker ein bør ha knytt til informasjonssikkerheit
- føretaka bør ha ei eigen leiinga sin gjennomgang for informasjonssikkerheit, som bør vere styresak. Kva tid ein skal ha gjennomgangen, kor ofte og kva den skal innehalde, bør samkøyrast i føretaksgruppa – dette for å letta arbeidet med å setje saman gjennomgangen og nytte den til vidare arbeid, og for å sikre tiltaket i den regionale handlingsplanen for informasjonssikkerheit om å rapportere om risiko knytt til informasjonssikkerheit i den ordinære verksemdsrapporteringa anten kvartalsvis eller tertialsvis
- RHF-et og HF-a[88] bør undersøkje om dei kan nytte seg av styreplassen administrerande direktør har i Helse Vest IKT og at CISO kan bidra med innspel til dei opne styresakene
- føretaka bør oppretthalde/opprette faste møtepunkt mellom CISO og administrerande direktør og andre i leiinga
- RHF-et bør løfte diskusjonen og endeleg avgjere om ein bør synleggjere informasjonssikkerheit i den nye styringsstrukturen for digitalisering
- føretaka bør arbeide med å få fram kva det inneber å vere dataansvarleg verksemd, og kva krav som følgjer med dette
- RHF-et bør løfte ein diskusjon, og involvere relevante parter, om korleis helseføretaka skal vere involvert i arbeidet med informasjonssikkerheit som Helse Vest IKT gjer knytt til IKT-infrastruktur

[88] Internrevisjonen vil presisere at dette ikkje gjeld Sjukehusapoteka Vest HF, da deira administrerande direktør ikkje sit i styret til Helse Vest IKT AS

Tilrådingar gjeldande CISO sin rolle og ansvar;

- føretaka bør ha eigne systematiske oversikter over status på innføringa av NSM sine grunnprinsipp
- føretaka bør gjennomføre eigne, interne sikkerheitsrevisjonar
- føretaka bør aktivt jobbe med det å ha oversikt over lokal IKT, MU og TU, inkludert førebyggande tiltak som regionale fora for MU/TU og krav i anskaffingar

Tilrådingar knytt til risikovurderingar- og -styring;

- føretaka bør arbeide med å forbetre metodikken knytt til risikovurderingar og -styring, at ein gjennomfører risikovurderingar når det er krav om det og sørgje for at ROS-teamet har skriftlege krav
- føretaka bør vurdere om talet på deltakarar i ROS-analysane er riktig dimensjonert i forhold til oppgåva
- føretaka bør jobbe med korleis ein handterer raude og gule risikoar, inkludert det å følgje opp, evaluere tiltak og oppdatere ROS-analysar
- føretaka bør utarbeide planar over risikoreduserande tiltak og planar for oppfølging av tiltak, og at desse er kommunisert på rett detaljnivå til leiinga
- føretaka bør ha eit system for aggregert risikobilde på føretaksnivå
- Helse Vest IKT og ROS-teamet bør tydeleggjere og definere dei ulike rollene knytt til risikovurderingar og -styring

5 VEDLEGG

5.1 Om internrevisjon

Internrevisjonen skal på vegner av styret i Helse Vest RHF overvake og bidra til forbetringar i føretaksgruppa si verksemdstyring, risikostyring og internkontroll. Det gjer vi i samsvar med dei internasjonale standardane for profesjonell utøving av internrevisjon, slik dei er fastsett av IIA. Les meir på Helse Vest.

Internasjonal definisjon av internrevisjon: "Internrevisjon er en uavhengig, objektiv bekreftelses- og rådgivningsfunksjon som har til hensikt å tilføre merverdi og forbedre organisasjonens drift. Den bidrar til at organisasjonen oppnår sine målsettinger ved å benytte en systematisk og strukturert metode for å evaluere og forbedre effektiviteten og hensiktsmessigheten av organisasjonens prosesser for risikostyring, kontroll og governance."

5.2 Figurliste