Direktoratet for e-helse

Nasjonal e-helsemonitor

Informasjonssikkerhet i helse- og omsorgssektoren 2019

Kunnskapsgrunnlag

20.12.2019

IE-1054

Publikasjonens tittel:
Informasjonssikkerhet i helse- og omsorgssektoren 2019

Rapportnummer
IE-1054, versjon 1.1

Utgitt:
20.11.2019

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:
www.ehelse.no

Forord

Direktoratet for e-helse skal følge med på IKT-utviklingen i helse- og omsorgssektoren i Norge og etablere et kunnskapsgrunnlag. Direktoratet startet i 2018 et arbeid for å etablere indikatorer for informasjonssikkerhet i helse- og omsorgssektoren. En arbeidsgruppe fra fagområdet har derfor utarbeidet en spørreundersøkelse om informasjonssikkerhet.

Spørsmålene ble hentet fra en undersøkelse av Direktoratet for forvaltning og IKT (Difi) om arbeidet med informasjonssikkerhet i statsforvaltningen (2018) og spørsmålene ble stilt likt til de regionale helseforetakene, helseforetak, regionale felles IKT-tjenesteleverandører (Sykehuspartner, Helse Vest IKT, Hemit og Helse Nord IKT) samt Norsk helsenett (NHN). Alle svarene er basert på selv-evaluering fra deltakerne. Kommunehelsetjenesten og fastleger ble ikke dekket i denne omgang.

Arbeidsgruppen har bestått av ledere og fagpersoner innen informasjonssikkerhet i helsesektoren. Direktoratet ønsker å takke deltakerne fra:

- Helse Nord RHF
- Helse Midt-Norge RHF
- Helse Sør-Øst RHF
- Oslo Universitetssykehus HF
- Helse Nord IKT
- Helse Vest IKT
- HEMIT
- Sykehuspartner
- Helseforetakenes driftsorganisasjon for nødnett HF
- Norsk helsenett (NHN)
- Nasjonal IKT
- Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Innhold

1 Innledning 9

1.1 Oppdrag og mandat 9

1.2 Formål og avgrensing 9

2 Metode og gjennomføring 10

2.1 Overordnet metodebeskrivelse 10

2.1.1 Forbehold til metodene 10

2.2 Evalueringskriterier og spørsmål 11

2.2.1 Styring og kontroll 11

2.2.2 Risikostyring 11

2.2.3 Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten 11

2.2.4 Beredskap og hendelseshåndtering 11

2.2.5 Sikkerhetskultur og kompetanse 12

2.2.6 Modenhetsundersøkelse IKT-tjenesteleverandører 12

2.3 Empirisk grunnlag 12

3 Analyse av de enkelte vurderingstemaene 14

3.1 Styring og kontroll 14

3.1.1 Observasjoner om føringer fra RHF 14

3.1.2 Observasjoner om føringer internt i HF og IKT-tjenesteleverandør 16

3.1.3 Vurdering for styring og kontroll 17

3.1.4 Anbefaling for styring og kontroll 17

3.2 Risikostyring 18

3.2.1 Observasjoner om roller ved risikostyring 18

3.2.2 Vurdering om roller ved risikovurdering 20

3.2.3 Anbefaling for risikovurdering 20

3.3 Normen 21

3.3.1 Observasjoner om Normen for utforming av krav 21

3.3.2 Vurdering om bruk av Normen for utforming av krav 22

3.3.3 Anbefaling for bruk av Normen for utforming av krav 22

3.4 Beredskap og hendelseshåndtering 22

3.4.1 Observasjoner på øvelser på informasjonssikkerhet 22

3.4.2 Observasjoner på IKT-beredskapsplan 23

3.4.3 Observasjoner på evaluering og læring av hendelser 24

3.4.4 Observasjoner på kostnader ved hendelser 24
3.4.5 Vurdering på beredskap og hendelseshåndtering 25
3.4.6 Anbefaling for beredskap og hendelseshåndtering 26
3.5 Sikkerhetskultur 26
3.5.1 Observasjoner på måling av sikkerhetskultur 26
3.5.2 Vurdering av måling av sikkerhetskultur 27
3.5.3 Anbefaling på måling av sikkerhetskultur 27
4 Modenhetsundersøkelse IKT-tjenesteleverandører 29
4.1 Kort om modenhetsmodeller 29
4.1.1 Observasjoner på modenhetsundersøkelse IKT-tjenesteleverandør 29
4.1.2 Observasjoner av modenhet på prosesser / fagområder 30
4.1.3 Analyse av modenhet på prosesser / fagområder 31
4.1.4 Forbedringsforslag for økt modenhet på prosesser / fagområder 32
5 Oppfølging og tilbakemelding 33
5.1 Forbedringsforslag til undersøkelsen 33

Sammendrag

Direktoratet for e-helse skal følge med på IKT-utviklingen i helse- og omsorgssektoren i Norge og etablere et kunnskapsgrunnlag. I 2018 startet Direktoratet et arbeid med å etablere indikatorer for informasjonssikkerhet i samarbeid med aktører fra helse- og omsorgssektoren med høy informasjonssikkerhetskompetanse og -erfaring. Denne undersøkelsen er et resultat av det arbeidet.

Undersøkelsen kartlegger status på informasjonssikkerhet i helsesektoren ved å etablere sammenlignbare indikatorer, og som kan relateres til internasjonale forhold. Undersøkelsen danner også et viktig utgangspunkt for å kunne følge med på utviklingen av informasjonssikkerhet i helsesektoren.

Utvikling av undersøkelsen

Utviklingen av en indikator for informasjonssikkerhet ble gjort gjennom en prosess der arbeidsgruppen ble presentert for flere alternativer for å måle og monitorere informasjonssikkerhet. Basert på gjennomgangen ble arbeidsgruppen enig om å bruke en nedskalert utgave av den informasjonssikkerhetskartleggingen Difi gjorde mot virksomheter i statsforvaltningen i 2018[1].

I tillegg ble de regionale IKT-tjenesteleverandørene og Norsk helsenett (NHN) enige om å benytte en internasjonal modenhetskartlegging med sammenliknbare data fra helsesektoren globalt. Det ble lagt til mulighet for å svare i fritekst, samt en tilpassing av spørsmålene til helsesektoren for å ivareta viktige prinsipp om at de regionale helseforetakene (RHF) har et "sørge for"-ansvar for informasjonssikkerhet i sine helseforetak (HF), mens HF-ene selv har ansvar for å vurdere risiko. Svarene er, som i Difi-undersøkelsen, anonymisert.

Slik har vi gjennomført undersøkelsen

Det ble sendt ut spørreskjema til ledelsen i RHF, utvalgte HF, de regionale IKT-tjenesteleverandørene og NHN. Svarene ble samlet inn og aggregert opp av Direktoratet for e-helse. Besvarelsene var delvis fra virksomhetsledelse og delvis fra fagansvarlige innenfor informasjonssikkerhet. Basert på innsendte svar og kommentarer ble det utarbeidet analyser, og på noen områder er det laget anbefalinger for videre arbeid innen informasjonssikkerhet.

Resultat og rapport ble diskutert i møter med arbeidsgruppen for å få frem nyanser og felles forståelse. Særlig på anbefalingene var det viktig å få konsensus.

Rapporten sier noe om *hvordan virksomhetene arbeider med informasjonssikkerhet*. Den kartlegger ikke selve sikkerhetstilstanden, som antall hendelser, avvik eller lignende.

Våre hovedfunn

Generelt skårer respondentene høyere enn statlige virksomheter som ble undersøkt av Difi i 2018. I tillegg skårer samtlige av de regionale felles IKT-tjenesteleverandørene i gjennomsnitt høyere enn sammenliknbare IKT-leverandører i helsesektoren globalt.

[1] Difi (Direktoratet for forvaltning og IKT), 2018, "Arbeidet med informasjonssikkerhet i statsforvaltningen" https://www.Difi.no/sites/Difino/files/Difi-rapport_2018_4_arbeidet_med_informasjonssikkerhet_i_statsforvaltningen_kunnskapsgrunnlag.pdf

- Alle RHF oppgir at de gir føringer for informasjonssikkerhetsarbeidet til regionens felles IKT-tjenesteleverandører og HF, og disse bekrefter også at slike føringer gis. Informasjonssikkerhet oppfattes derfor som forankret og plassert på det nivået det bør.
- Oppfølgning fra RHF skjer ved formell eierstyring. HF og IKT-tjenesteleverandør er derfor mer involvert i operativ risikovurdering og -håndtering enn RHF. De to sistnevnte oppfatter dette som riktig, og at regionsnivået primært har et sørge-for-ansvar.

  Når det er sagt, peker noen av HFenes fagansvarlige for informasjonssikkerhet på at det kan være dialog på ledelsesnivå mellom region og helseforetak de ikke deltar i.
- I HFene er det fagansvarlige for informasjonssikkerhet som i stor grad har et tydelig definert og delegert ansvar for risikovurdering (80 prosent), men mange HF-ledere (27 prosent) svarer at de også i stor grad er med i vurderinger.
- Alle nivåene, og regionsnivået i høyest grad, svarer at de benytter Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten som utgangspunkt for utforming av krav. Undersøkelsen bekrefter dermed at Normen er et godt innarbeidet felles kravsett for sektoren.
- Alle respondentene, med unntak av ett RHF, oppgir at de har en IKT-beredskapsplan som er godkjent av ledelsen, mens bare 72 prosent av statlige virksomheter har det samme. Likevel oppgir majoriteten av respondentene at de kun i moderat grad arbeider systematisk med øvelser på informasjonssikkerhetsområdet. Antallet HF som i stor grad har systematiske øvelser er lavere (9 prosent) enn statlige virksomheter (18 prosent).
- Dersom en sikkerhetshendelse har forekommet, bør man sørge for at man evaluerer og lærer av hendelsen. Alle respondentene svarer at ledelsen i stor eller moderat grad er involvert slike evalueringer, med unntak av to av elleve HF hvor ledelsen kun i liten grad er involvert.
- Respondentene vet lite om kostnadene som følge av en eventuell informasjonssikkerhetshendelse. Blant HF svarer nesten alle at de i ingen eller liten grad har oversikt, bare en av elleve HF har her svart i moderat grad.
- Måling av sikkerhetskultur er lavest i RHF (25 prosent) etterfulgt av gjennomsnittet for staten (41 prosent), HF (45 prosent) og de regionale felles IKT-tjenesteleverandørene (75 prosent).
- De regionale felles IKT-tjenesteleverandørene i Norge skårer høyere (3,6) i modenhet innen informasjonssikkerhet enn helsesektoren globalt (3) (skala går fra 0-5).

Videre arbeid

Direktoratet for e-helse har i 2019 arbeidet systematisk med informasjonssikkerhet som tema:

- Innbyggerundersøkelsen 2019 viste at kun 55 prosent av innbyggerne har tillit til at helseopplysningene deres er lagret slik at utenforstående ikke har tilgang til dem.
- En tilsvarende klinikerundersøkelse 2019 er under arbeid og vil belyse klinikernes oppfatning av informasjonssikkerhet.

Resultatene fra disse undersøkelsene samt denne rapporten bidrar til økt transparens og et faktagrunnlag om arbeidet med informasjonssikkerhet i sektoren.

Nyere forskning viser at nettopp pasienters opplevelse av transparens i informasjonssikkerhetstiltak, prosedyrer for informasjonsdeling og personvernvilkår bidrar til økt tillit[2]. Økt tillit bidrar også til at pasientene i større grad velger å gi fra seg helseinformasjon. Her har Direktoratet for e-helse et viktig formidlingsansvar.

Anbefalinger

Direktoratet fremmer anbefalinger og forbedringsforslag basert på funnene i rapporten. Anbefalingene til virksomhetene i spesialisthelsetjenesten gjelder informasjonssikkerhet og beskrives her:

Anbefalinger på informasjonssikkerhet for virksomheter i spesialisthelsetjenesten.

- **Anbefaling 1:** Ledelsen må ha tilstrekkelig kompetanse og oppmerksomhet for å utøve reell styring og kontroll på informasjonssikkerhetsområdet.
- **Anbefaling 2**: Det bør iverksettes tettere kommunikasjon fra RHF og mer involvering av HF i informasjonssikkerhetsarbeidet i regionene.
- **Anbefaling 3:** Den enkelte virksomhet (RHF, HF og IKT-tjenesteleverandør) må sikre nødvendig kompetanse på fagfeltet risikostyring.
- **Anbefaling 4**: Helseforetakene, i samarbeid med de regionale helseforetakene og IKT-tjenesteleverandør, bør gjennomføre minst én årlig øvelse i informasjonssikkerhet.
- **Anbefaling 5:** Regionene bør søke å samarbeide om et felles rullerende øvelsesopplegg for informasjonssikkerhet, for å trekke ut felles lærdommer, beste praksis og løfte de som ligger etter i beredskapsplanlegging og -øvelser.
- **Anbefaling 6**: Virksomheter kartlegger sin sikkerhetskultur. På bakgrunn av kartleggingen utformer virksomheten eventuelle tiltak til forbedring.

Når det gjelder forbedringsforslag så er de myntet på de felles regionale IKT-tjenesteleverandørene og mer knyttet til beste-praksis for å øke grad av modenhet innen informasjonssikkerhet i IKT-leveranseorganisasjoner.

Arbeidsgruppen og direktoratet vil samarbeide videre med materialet knyttet til denne modenhetsundersøkelsen. De konkrete forbedringsforslagene beskrives avslutningsvis i rapporten.

[2]Esmaeilzadeh P. (2019). "The Impacts of the Perceived Transparency of Privacy Policies and Trust in Providers for Building Trust in Health Information Exchange: Empirical Study". JMIR Med Inform 2019;7(4). URL: https://medinform.jmir.org/2019/4/e14050/

1 Innledning

Med IKT-sikkerhet forstås beskyttelse av informasjon, tjenester og systemer som er sårbare fordi de er koplet til, eller på annen måte er avhengig av IKT. Sikkerhetsmål for IKT-sikkerhet omfatter tilgjengelighet, integritet og konfidensialitet[3].

Med informasjonssikkerhet forstås å sikre at informasjonen[4]:

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

1.1 Oppdrag og mandat

Direktoratet for e-helse utarbeider Nasjonal e-helsemonitor som skal følge digitaliseringen i norsk helse- og omsorgssektor. Dette gjelder også innenfor tverrgående prosesser og for eksempel løsninger for informasjonssikkerhet. Mandatet for dette oppdraget ble definert som:

"Utrede og anbefale indikator som gir kunnskap om informasjonssikkerhet knyttet til utviklingen av digitalisering i helse- og omsorgssektoren. Indikatoren bør gi grunnlag for å identifisere effekter av informasjonssikkerhet og skal om mulig kunne sammenliknes internasjonalt".

1.2 Formål og avgrensing

Informasjonssikkerhet er et bredt fagområde under løpende utvikling. Formålet med denne undersøkelsen har vært å få en overordnet tilstandsbeskrivelse av kultur, ledelse og struktur på informasjonssikkerhetsarbeidet i helsesektoren. Følgende avgrensinger ble gjort:

- Undersøkelsen dekker kun regionale helseforetak (RHF) og noen helseforetak (HF)
- Undersøkelsen dekker de regionale helseforetakenes IKT-tjenesteleverandører (dvs. Sykehuspartner, Helse Vest IKT, Hemit, Helse Nord IKT samt Norsk helsenett)
- Kommunehelsetjenesten er ikke dekket i denne rapporten
- Fastleger er ikke dekket i denne rapporten

[3] Difi (Direktoratet for forvaltning og IKT), 2018, "Arbeidet med informasjonssikkerhet i statsforvaltningen" https://www.Difi.no/sites/Difino/files/Difi-rapport_2018_4_arbeidet_med_informasjonssikkerhet_i_statsforvaltningen_kunnskapsgrunnlag.pdf

[4] Difi (Direktoratet for forvaltning og IKT) 2019, Henter fra: https://www.Difi.no/fagomrader-og-tjenester/informasjonssikkerhet

2 Metode og gjennomføring

Arbeidet er gjennomført av Direktoratet for e-helse med forankring i en arbeidsgruppe sammensatt av følgende deltakere fra helsesektoren:

- Regionale helseforetak: Helse Nord, Helse Midt-Norge, Helse Sør-Øst
- Regionale IKT-tjenesteleverandører: Helse Nord IKT, HEMIT, Helse Vest IKT, Sykehuspartner
- Norsk helsenett
- Direktoratet for e-helse*

*Fra direktoratet deltok personer fra sekretariatet for Normen[5].

2.1 Overordnet metodebeskrivelse

Flere typer data ble vurdert for å beskrive tilstanden på informasjonssikkerheten i helse-Norge. Hendelseslogger, strategier og planverk ble vurdert, i tillegg til søk mot andre nordiske land for å se hva de har gjort. Det var ønskelig at tilstandsbeskrivelsen kunne måles på sammenlignbare indikatorer mot land, bransjer eller liknende grupper.

Et forslag til arbeidsgruppen om å ta utgangspunkt i Difis materiale fra rapporten Arbeidet med informasjonssikkerhet i statsforvaltningen[6] ble akseptert; på denne måten kunne man sammenlikne seg mot situasjonen i offentlig sektor-virksomheter i Norge.

Det var i tillegg enighet om å benytte en internasjonal modenhetsmodell for Informasjonssikkerhet[7] mot de regionale IKT-tjenesteleverandørene for å sammenlikne mot IKT-tjenesteleverandører innenfor helsesektoren globalt.

2.1.1 Forbehold til metodene

I denne undersøkelsen var det ønskelig å se helsesektoren som helhet. Spørsmålene fra Difi ble derfor endret noe slik at de skulle passe de ulike nivåene (RHF, HF). Det ble benyttet kontrollspørsmål for å sjekke pålitelighet, for eksempel:

a) *Til RHF: I hvilken grad har ledelsen i RHF gitt HF føringer for XY?*
b) *Til HF: I hvilken grad har ledelsen i RHF gitt HF føringer for XY?*

De fleste spørsmålene ble utstyrt med fritekstfelt for å sikre at utdypende kontekst og forklaringer kunne tas med. Svarene fra virksomhetene er basert på selv-evaluering, ikke intervju eller vurdering fra nøytral annen part.

Den internasjonale modenhetsmodellen benyttet mot IKT-tjenesteleverandørene er basert på selv-evaluering fra liknende virksomheter i helsesektoren, ikke benchmarking-tall fra nøytral annen part.

[5] Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

[6] Difi (Direktoratet for forvaltning og IKT), 2018

[7] Gartner ITScore for Information Security er tilgjengelig for brukere av Gartner Research tjenester

2.2 Evalueringskriterier og spørsmål

Hovedtema i undersøkelsen har vært kultur, ledelse og struktur for informasjonssikkerhet. Dette er dekket inn gjennom å benytte elleve nesten likelydende spørsmål til RHF, HF og IKT-tjenesteleverandørene. IKT-tjenesteleverandørene måtte i tillegg svare på 30 spørsmål fra den internasjonale modenhetsmodellen. Under beskrives spørsmålene kort, samt formålet med å stille akkurat disse spørsmålene.

2.2.1 Styring og kontroll

Kortversjon av spørsmål (stilt både til RHF, HF og IKT-tjenesteleverandør):

- *I hvilken grad har RHF ledelse gitt tydelige føringer for roller og ansvar for informasjonssikkerhetsarbeidet?*

2.2.1.1 Formål med spørsmålet

Lederforankring eller «tonen på toppen» omfatter hvilke føringer som er gitt fra ledelsen og hvilke roller er definert. Målet er å se om RHF mener at de gir styringssignaler og om HF oppfatter at de får signaler. Spørsmålet er relevant med tanke på RHFenes "sørge for"-ansvar, HFenes databehandleransvar - og om disse er tydelig oppfattet i sektor.

2.2.2 Risikostyring

Kortversjon av spørsmål (stilt både til RHF, HF og IKT-tjenesteleverandør):

- *I hvilken grad er RHF med på å vurdere og håndtere risiko?*

2.2.2.1 Formål med spørsmålet

Spørsmålet om risikostyring omfatter to faktorer (vurdering og håndtering), i denne rapporten legges det mest vekt på risikovurdering. Målet er å se hvor "høyt opp" denne type risikovurderinger går.

2.2.3 Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Kortversjon av spørsmål (stilt både til RHF, HF og IKT-tjenesteleverandør):

- *I hvilken grad benyttes Normen for utforming av krav?*

2.2.3.1 Formål med spørsmålet

Normen inneholder flere veiledere med krav som kan benyttes mot leverandører av IKT løsninger og -tjenester. Målet med spørsmålet er få en oppfatning av hvor godt kjent Normen er i sektor.

2.2.4 Beredskap og hendelseshåndtering

Kortversjon av spørsmål (stilt både til RHF, HF og IKT-tjenesteleverandør):

- *Gjennomfører RHF systematisk øvelser på informasjonssikkerhetsområdet?*
- *Har RHF en IKT-beredskapsplan for foretaksgruppen?*
- *Er RHF involvert i evaluering og læring av hendelser innen informasjonssikkerhet?*

- *Har RHF oversikt over kostnadene som følge av hendelser?*

2.2.4.1 Formål med spørsmålene

God beredskapsplanlegging, øvelser og læringsprosess sikrer at man håndterer uønskede hendelser på en bedre måte. Målet med disse spørsmålene er å forstå om dette foregår i særlig grad hos RHF, HF og IKT-tjenesteleverandør. Graden av hva som gjøres uttrykker også et modenhetsnivå.

2.2.5 Sikkerhetskultur og kompetanse

Kortversjon av spørsmål (stilt både til RHF, HF og IKT-tjenesteleverandør):

- *Har ledelsen ved RHF kartlagt eller målt sikkerhetskultur i eget foretak?*

2.2.5.1 Formål med spørsmålet

Sikkerhetskulturen regnes som en del av organisasjonskulturen og gir et innblikk i felles verdier og normer. Spørsmålet er stilt for å få en oppfatning av hvilket forhold ledelsen har til sikkerhetskulturen i virksomheten.

2.2.6 Modenhetsundersøkelse IKT-tjenesteleverandører

ITScore-modellen som er benyttet stiller graderte spørsmål innenfor 10 områder:

- Sikkerhetsledelse
- Planlegging / budsjett
- Organisasjon
- Rammeverk for kontroll
- Arkitektur
- Prosess og drift
- Kommunikasjon og bevissthet
- Hendelseshåndtering
- Trussel og sårbarhetsstyring
- Risiko og kontroll vurdering

Modell og resultat er beskrevet mer utfyllende i kapittel 4.

2.3 Empirisk grunnlag

Helseforetakene ble valgt ut av deltakende RHF. Ikke alle helseforetak svarte på oppfordring om å delta. Til sammen fikk 22 helseforetak forespørsel om å delta, hvor 19 helseforetak svarte.

Virksomhetene som svarte på undersøkelsen og hva de har besvart:

Virksomhet:	**Spørreskjema**	**Modenhets undersøkelse (ITScore)**
Helse Nord RHF	X	
Nordlandssykehuset HF	X	
Helgelandssykehuset HF	X	

Helse Nord IKT	X	X
Helse Midt Norge RHF	X	
Helse Nord-Trøndelag HF	X	
Hemit	X	X
Helse Vest RHF	X	
Helse Stavanger HF	X	
Helse Fonna HF	X	
Helse Førde HF	X	
Helse Vest IKT	X	X
Helse Sør Øst RHF	X	
Ahus	X	
Sykehuset Østfold HF	X	
Sykehuset Innlandet HF	X	
Sørlandet Sykehus HF	X	
Sykehuspartner	X	X
Norsk helsenett	X	X
SUM:	**19**	**5**

Antallet respondenter er lavt, og svar i en retning fra ett av de fire RHF-ene vil for eksempel gi et utslag på 25 prosent. Fokuset i rapporten er derfor hovedtendensene i besvarelsene og mindre fokus på avvik.

3 Analyse av de enkelte vurderingstemaene

Evalueringen er delt inn i fem områder som er sentrale i arbeidet med informasjonssikkerhet. Hvert område er delt inn i beskrivelse av vurderingstema, observasjoner, vurderinger og anbefalinger. Vurderingene er basert på observasjoner om hvorvidt virksomhetene arbeider systematisk med disse områdene for å oppnå god informasjonssikkerhet.

Det sjette området er en skåring basert på en internasjonal modenhetsmodell som sammenstiller egen vurdering opp mot besvarelser fra liknende virksomheter i helsesektoren globalt.

3.1 Styring og kontroll

Ledere på alle nivå skal sikre at virksomheten når sine samlede mål. Sikkerhetsmål for informasjonssikkerhet omfatter tilgjengelighet, integritet og konfidensialitet[89]. I offentlig sektor er styringssystem for informasjonssikkerhet ledelsens verktøy for å ha tilstrekkelig styring og kontroll på området, og kan ikke være forankret eller ledet fra noe annet sted i virksomheten.

Føringer fra ledelsen er viktig og dersom ledelsen ikke tar informasjonssikkerhet på alvor, blir dette fort synlig for de ansatte. En konsekvens er da ofte at virksomhetene får problemer med å lykkes med etablering og gjennomføring av systematiske aktiviteter.

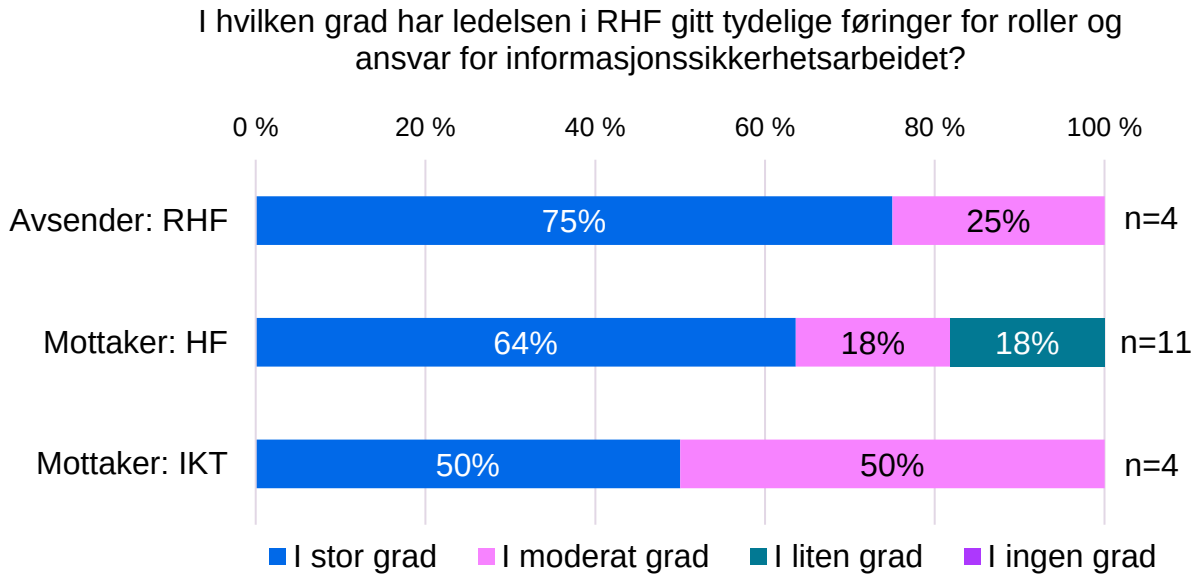
De regionale helseforetakene (RHF) har et "sørge for"-ansvar for informasjonssikkerhet i sine helseforetak (HF), mens ledelsen i HF-ene har ansvar for styring og kontroll i sine egne foretak. IKT-tjenesteleverandørene har HF som kunder, men eies som regel av RHF. Denne organiseringen gjør at det må stilles kontrollspørsmål som går "begge veier".

3.1.1 Observasjoner om føringer fra RHF

Det første spørsmålet undersøker hos RHF og HF, om ledelsen i RHF har gitt tydelige føringer for roller og ansvar for informasjonssikkerhetsarbeidet. Dette viser i hvilken grad RHF selv mener at de gir føringer, og om HF og IKT-tjenesteleverandørene opplever det samme.

[8] eForvaltningsforskriften §15

[9] Normen, Kapittel 2, Ledelse og ansvar



Ulike spørsmålstillinger(forkortet):
RHF: I hvilken grad har ledelsen for RHF gitt helseforetakene tydelige føringer for roller og ansvar for informasjonssikkerhetsarbeidet?
HF: I hvilken grad har ledelsen i RHF gitt helseforetaket tydelige føringer for roller og ansvar for informasjonssikkerhetsarbeidet?
IKT: I hvilken grad har ledelsen i RHF gitt ditt foretak tydelige føringer for roller og ansvar for informasjonssikkerhetsarbeidet?

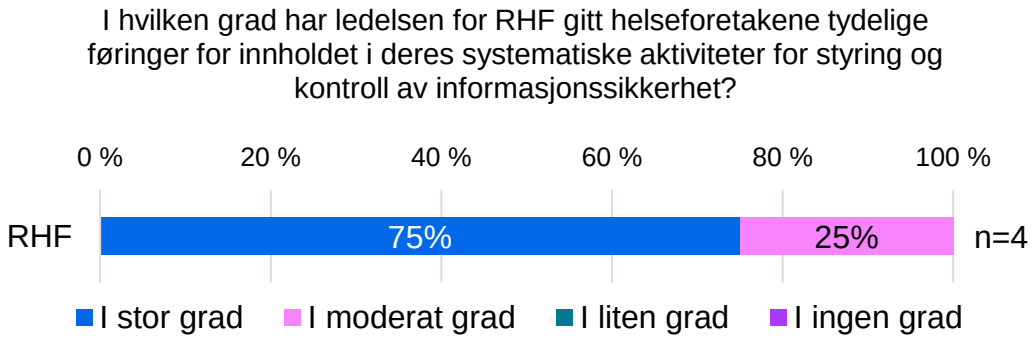
RHF mener de i stor eller moderat grad gir føringer om roller og ansvar for informasjonssikkerhetsarbeidet. De fleste HF (ni av elleve) bekrefter at ledelsen i RHF gir slike føringer i større eller moderat grad. Alle IKT-tjenesteleverandørene mener også at RHF i stor eller moderat grad gir føringer.

> "RHF har videre stilt krav om at HF skal sørge for god og reell ledelsesforankring og styring av informasjonssikkerhet" (RHF).

Respondentenes tilleggskommentarer i fritekstfeltene kan tyde på at i HF som svarer "i liten grad", er det delegert myndighet fra RHF til et regionalt sikkerhetsutvalg som håndterer metode og styringssystem for informasjonssikkerhet.

Samlet sett kan det sies at føringer gitt fra RHF blir mottatt av HF og IKT-tjenesteleverandør.

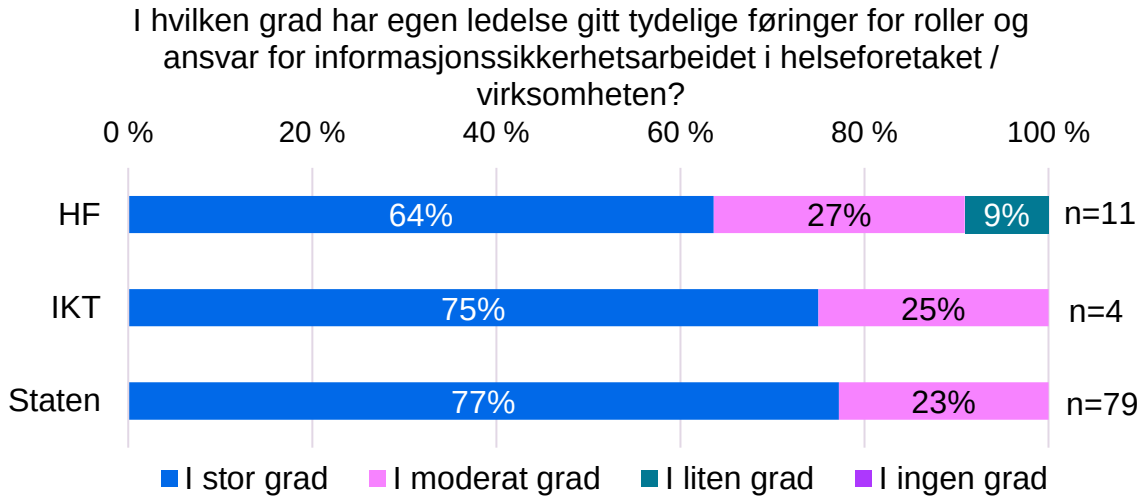
Et mer konkret spørsmål er stilt for å vurdere om RHF også gir føringer for innholdet i informasjonssikkerhetsaktiviteter:



Her bekrefter RHF at de gir føringer for aktiviteter. Andelen som i stor grad gir slike føringer er likt som for føringer for roller og ansvar.

3.1.2 Observasjoner om føringer internt i HF og IKT-tjenesteleverandør

Den andre dimensjonen av styring og kontroll er i hvilken grad egen ledelse i HF og hos IKT-tjenesteleverandørene gir føringer internt i sine virksomheter.

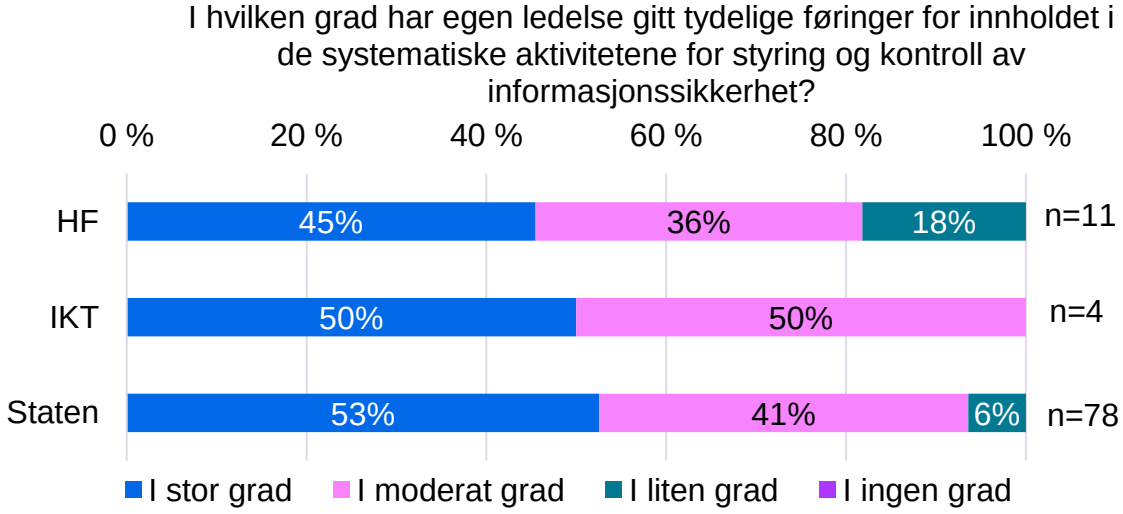


Ulike spørsmålstillinger (forkortet):
HF: I hvilken grad har foretaksledelsen i ditt HF gitt tydelige føringer for roller og ansvar for informasjonssikkerhetsarbeidet i helseforetaket?
IKT: I hvilken grad har ledelsen i din virksomhet gitt tydelige føringer for roller og ansvar for informasjonssikkerhetsarbeidet i virksomheten?
Staten: I hvilken grad har virksomhetsleder gitt tydelige føringer for roller og ansvar i informasjonssikkerhetsarbeidet i virksomheten?

I diagrammet over bekrefter flertallet i HF og hos IKT-tjenesteleverandørene at ledelsen i stor eller moderat grad gir føringer for roller og ansvar for informasjonssikkerhetsarbeidet. Resultatene er sammenstilt med tall fra Difis rapport om Arbeidet med informasjonssikkerhet i statsforvaltningen (2018).

Samlet sett ligger helsesektoren omtrent på nivå med statlige virksomheter.

Det andre spørsmålet, føringer for innholdet i de systematiske aktivitetene for styring og kontroll av informasjonssikkerhet, viser at føringer fra egen ledelse blir gitt i noe mindre grad enn for roller og ansvar.



Ulike spørsmålsstillinger:
HF: I hvilken grad har HFs leder gitt tydelige føringer for innholdet i de systematiske aktivitetene for styring og kontroll av informasjonssikkerhet?
IKT: I hvilken grad har ledelsen i din virksomhet gitt tydelige føringer for innholdet i de systematiske aktivitetene for styring og kontroll av informasjonssikkerhet?
Staten: I hvilken grad har virksomhetsleder gitt tydelige føringer for innholdet i de systematiske aktivitetene for styring og kontroll av informasjonssikkerhet?

Andelen HF som oppgir at egen ledelse i stor grad gir slike føringer er under 50 prosent (fem av elleve). I tillegg svarer 18 prosent (to av elleve) at ledelsen kun i liten grad gir slike føringer. For IKT-tjenesteleverandørene er andelen på 50 prosent (to av fire), mens resten svarer i moderat grad.

Sammenlignet med statlige virksomheter, hvor 53 prosent svarer "i stor grad", er det tydelig at ledelsen i HF og IKT-tjenesteleverandørene ikke i like stor grad gir tydelige føringer for innholdet i de systematiske aktivitetene for styring og kontroll.

> "Det er tydelig kommunisert at helseforetaket har dataansvaret – ikke det regionale helseforetaket […] understreket gjennom forelegget fra Datatilsynet i HF-ene i 2018" (HF).

Samlet sett er det en utbredt tendens til å gi føringer også på dette området, selv om praksisen ser ut til å være noe mindre utbredt blant HF. Helsesektoren ligger også her på et noe lavere nivå enn andelen i statsforvaltningen når det gjelder føringer fra ledelsen.

3.1.3 Vurdering for styring og kontroll

Modenheten innenfor området styring og kontroll oppfattes å være god, selv om den er noe lavere enn nivået i statsforvaltningen for øvrig. At også IKT-tjenesteleverandørene opplever å motta føringer fra RHF tyder på at samarbeid og ansvar for at styringssystem for informasjonssikkerhet er forankret og plassert på det nivået det bør høre hjemme.

Det legges derimot merke til at 18 prosent av HF oppgir at ledelsen i liten grad gir føringer for innholdet i aktivitetene knyttet til styring og kontroll. I tillegg vil det påpekes at andelen som oppgir at ledelsen i stor grad gir føringer er under 50 prosent, noe som anses å være for lavt.

3.1.4 Anbefaling for styring og kontroll

Kommentarer fra respondentene tyder på at det er god dialog om informasjonssikkerhet mellom ledelsen i HF og deres felles IKT-tjenesteleverandør. Fagansvarlig for informasjonssikkerhet i HF gir derimot uttrykk for at de opplever noe avstand til denne dialogen som skjer "regionalt" mellom ledelsen i HF og IKT-tjenesteleverandør.

Dette er i og for seg ikke så kritisk, men siden regionene ikke tilnærmer seg eller organiserer seg likt bør informasjon deles slik at det over tid blir mer oversiktlig for alle deltakere. Direktoratet for e-helse foreslår å styrke kompetansen, som også er et av tiltakene i rapporten om Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten[10]. Forslaget innebærer at informasjonssikkerhetsansvarlig i HF, som bestiller, har tettere rutiner og kommunikasjon overfor IKT-tjenesteleverandørene.

Direktoratet for e-helse vil komme med følgende anbefaling:

[10] Direktoratet for e-helse, 2017, "Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten"

Anbefaling 1: Ledelsen i HF må ha tilstrekkelig kompetanse og oppmerksomhet for å utøve reell styring og kontroll på informasjonssikkerhetsområdet.

Anbefaling 2: Det bør iverksettes tettere kommunikasjon og mer involvering av HF i informasjonssikkerhetsarbeidet i regionene.

3.2 Risikostyring

Risikostyring vil si å identifisere, vurdere, håndtere og følge opp hendelser som kan påvirke måloppnåelsen negativt[11]. Risikostyring henviser til de systematiske aktivitetene for å vurdere og håndtere risiko som en del av styring og kontroll av informasjonssikkerhet. Som en vurdering av målgruppens risikostyring ble HF og IKT-tjenesteleverandørene spurt om i hvilken grad ulike roller (ledere eller fagansvarlige) er med på å vurdere og håndtere risiko innen informasjonssikkerhet.

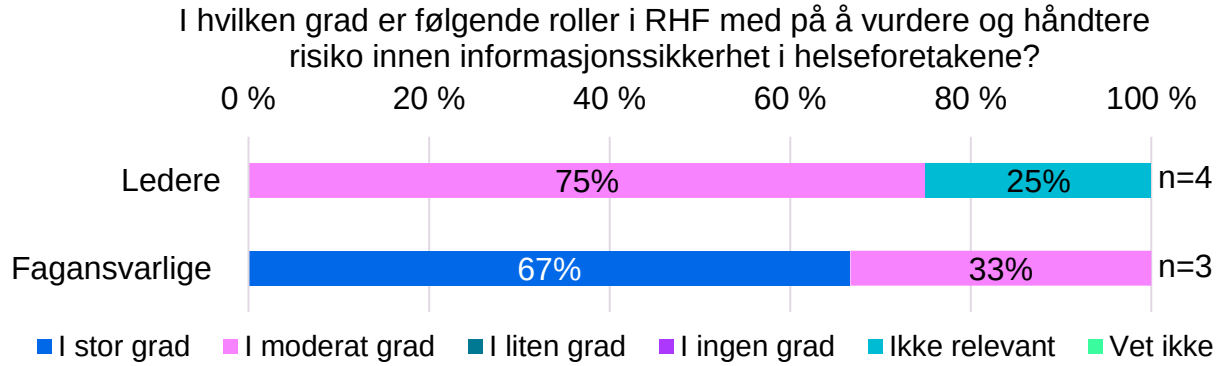
3.2.1 Observasjoner om roller ved risikostyring

Alle respondentene hadde mulighet til å svare på hvorvidt ledere eller fagansvarlige er med på å vurdere og håndtere risiko, og i hvor stor grad disse rollene er involvert. Svarene indikerer at det er noe ulikt for HFene og IKT-tjenesteleverandørene hvordan rollene som har en relevans i risikohåndtering og -vurdering. For enkelte er både leder og fagansvarlig med, mens for andre er det kun én av disse rollene som deltar i risikovurderingen.

Det ble stilt ulike spørsmål til RHF, HF og IKT-tjenesteleverandørene. RHF ble spurt i hvilken grad deres ledere, fagansvarlige, egen gruppe for informasjonssikkerhet, eller lignende i RHF er "hands-on", og med på å vurdere og håndtere risiko i HF. IKT-tjenesteleverandørene på sin side ble spurt om i hvilken grad ledere, eller fagansvarlige for informasjonssikkerhet fra RHF, er involvert i risikovurdering i deres virksomhet. HF ble spurt om i hvilken grad egne ledere, eller fagansvarlige, er med på å vurdere og håndtere risiko internt.

3.2.1.1 RHF sin risikostyring mot HF

Spørsmålet om i hvilken grad ledere eller fagansvarlige i RHF deltar i risikostyring har ett manglende svar (missing) for alternativet "fagansvarlige". Dette medfører at antall svar fra fagansvarlige blir noe lavt. Respondentene fra RHF oppgir at tre av fire ledere tar del i risikostyringen i HF i moderat grad, mens én respondent svarer "ikke relevant". For fagansvarlige eller faggrupper for informasjonssikkerhet i fra RHF svarer to av tre (67 prosent) at disse deltar i stor grad, mens én (33 prosent) svarer i moderat grad.



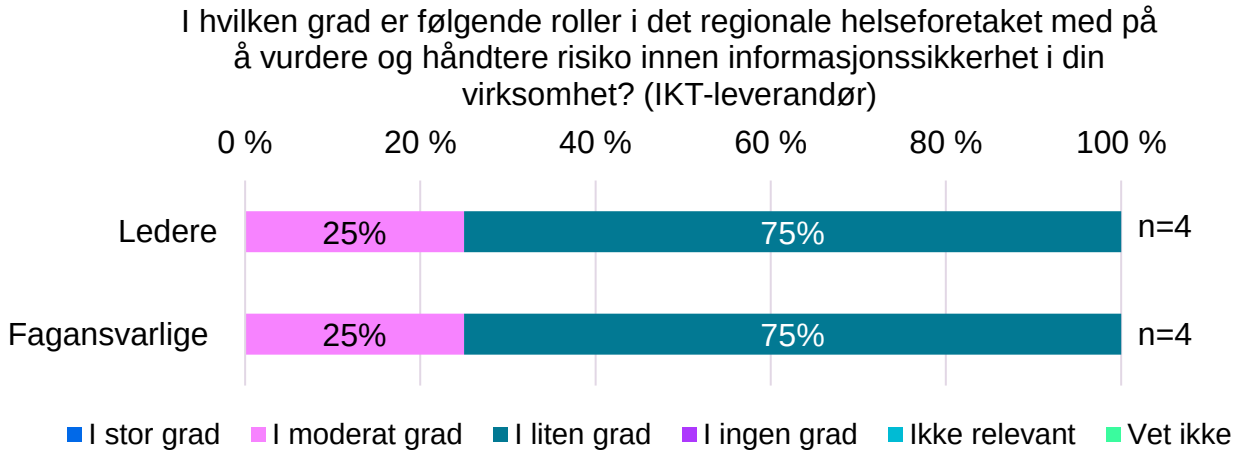
[11] Direktoratet for økonomistyring

Det synes som RHF-koordinerte fagansvarlige, eller faggrupper, i større grad deltar i risikostyringen mot HF, enn ledere i RHF.

3.2.1.2 RHF sin risikostyring mot IKT-tjenesteleverandørene

IKT-tjenesteleverandørene ble spurt om i hvilken grad ledere, fagansvarlige, egen gruppe for informasjonssikkerhet eller lignende i RHF, deltar i risikovurdering i deres virksomhet.

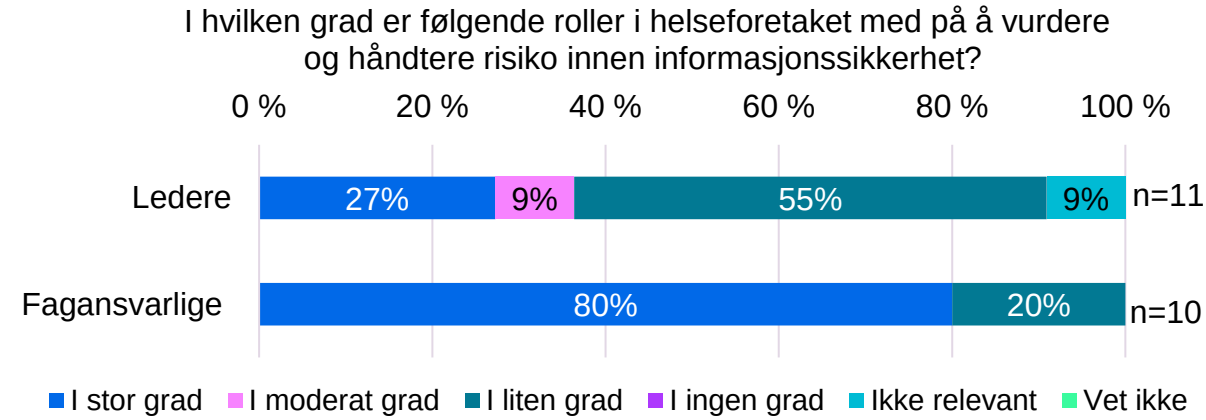
Respondentene fra IKT-tjenesteleverandørene svarer at ledere og fagansvarlige fra RHF i like stor grad tar del i risikovurderingen i deres virksomheter. Dette er derimot hovedsakelig i liten grad, noe tre av fire svarer.



Samlet sett indikerer dette at RHFenes ledere og fagansvarlige i liten grad tar del i risikovurdering blant sine IKT-tjenesteleverandører. Roller fra RHF deltar også i mindre grad i risikostyring mot IKT-tjenesteleverandører, sammenlignet med deltakelse mot HF. Dette er også i tråd med uttalte rutiner.

3.2.1.3 Roller i risikostyring i HF

På dette spørsmålet er det ett manglende svar (missing), for svaralternativet "fagansvarlige". For HFene er det også stilt spørsmål om i hvilken grad egne ledere eller fagansvarlige for informasjonssikkerhet internt i HFet tar del i risikovurderingen.



Seks av elleve (55 prosent) av respondentene fra HF svarer at egen ledelse i liten grad er med på risikostyringen i sitt helseforetak. Kun tre av ti (27 prosent) respondenter svarer at ledelsen i stor grad tar del i helseforetakets risikostyring.

For fagansvarlige er bildet et annet. Der er det hele åtte av ti (80 prosent) som svarer at fagansvarlige for informasjonssikkerhet i stor grad tar del i risikostyring. De resterende to av ti (20 prosent) svarer at dette skjer i liten grad. Dette indikerer at det for det meste er fagansvarlige for informasjonssikkerhet i HF som har en aktiv rolle i HFenes egne risikostyring, mens ledelsen har en mer tilbaketrukken rolle.

Undersøkelsen som Difi har gjennomført blant statlige virksomheter kan ikke direkte sammenliknes her. Difi spør: "Hvem har det formelle ansvaret for å vurdere og håndtere risiko innen informasjonssikkerhet?", hvorav 84 prosent svarer at det er virksomhetslederne som har det ansvaret.

3.2.2 Vurdering om roller ved risikovurdering

Regelverket på informasjonssikkerhetsområdet er i hovedsak risikobasert. Det overlater til virksomheten å velge et passende nivå for usikkerhet (risikoappetitt), samt å velge egnede sikkerhetstiltak. Det gir rom for tilpasning til en virksomhets størrelse, egenart og risikobilde.

Slik fleksibilitet kan være positivt. Det muliggjør tilpasning av styring og sikkerhetstiltak til lokale behov, sørger for at sikkerhetsarbeidet er kostnadseffektivt og understøtter virksomhetens måloppnåelse. Uansett kreves god kunnskap, kompetanse og evne for å utnytte denne fleksibiliteten og gjøre kloke vurderinger og valg.

Det foreligger ingen ordinær linjeledelse mellom RHFet og de enkelte HF. Oppfølgning av HF skjer ved formell eierstyring. I trekantsamarbeidet som foregår mellom RHF, HF og IKT-tjenesteleverandør er det tydelig at det er HFene selv som er mest involvert i sin egen risikovurdering og -håndtering. De oppfatter også at det er slik det skal være. Også RHF og IKT-tjenesteleverandørene er involvert i dette arbeidet. Fra et HF kommenteres det:

> "[…] hovedvekten av vurderingene og beslutninger rundt informasjonssikkerhet oppleves å være tatt av IKT-tjenesteleverandøren […]" (HF).

Men også her er det ulikheter i hvordan aktivitetene er gjennomført.

3.2.3 Anbefaling for risikovurdering

Fra HFene generelt tyder kommentarene og svarene på at de forholder seg til linjen i sin egen virksomhet. Det kommenteres videre at det foregår kommunikasjon om risiko "på toppen" mellom HF-ledelse og RHF-ledelse. De fagansvarlige trekkes ikke alltid med i vurderinger.

Som fagansvarlig for informasjonssikkerhet i et HF (og enhver virksomhet for øvrig) er det viktig å fornye og holde vedlike kompetanse innen risikovurderinger på tvers av foretaksgruppen, og i samarbeid med IKT-tjenesteleverandør. Dette kan for eksempel skje gjennom aktiv deltakelse i ulike fora, eller at man trekkes med i beslutningsprosessen ved vurderinger.

Direktoratet for e-helse vil komme med følgende anbefaling:

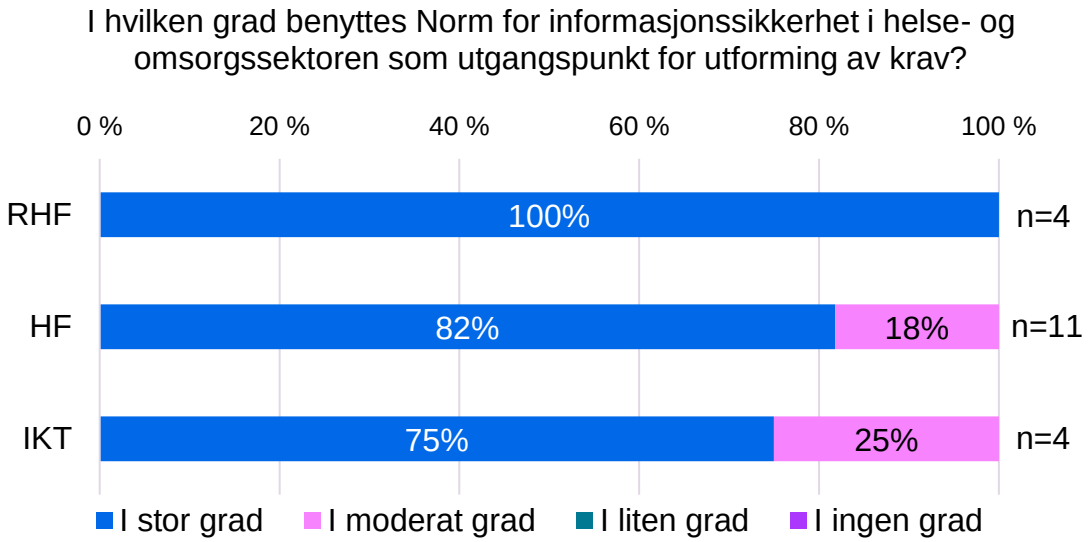
Anbefaling 3: Den enkelte virksomhet (RHF, HF og IKT-tjenesteleverandør) må sikre nødvendig kompetanse på fagfeltet risikostyring.

3.3 Normen

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten er et viktig utgangspunkt for virksomhetenes arbeid med informasjonssikkerhet.

3.3.1 Observasjoner om Normen for utforming av krav

RHF og HF har fått tilnærmet samme spørsmål om i hvilken grad Normen benyttes som utgangspunkt for utforming av krav, men tolkningen er litt ulik. For RHF gjelder dette i stor grad deres styringssystem for informasjonssikkerhet i sin region, mens for HF gjelder det også deres rutiner og aktiviteter i informasjonssikkerhetsarbeidet internt, samt krav overfor leverandører i innkjøpsprosesser eller lignende. IKT-tjenesteleverandørene har fått en mer spesifikk spørsmålsstilling om de benytter Normen som utgangspunkt for utforming av krav mot foretakene eller andre leverandører.



Ulike spørsmålsstillinger (forkortet her):
RHF/HF: I hvilken grad benyttes Normen som utgangspunkt for utforming av krav?
IKT: I hvilken grad benyttes Normen som utgangspunkt for utforming av krav mot foretak, leverandører og andre?

Normen utgjør en tydelig del av RHFs krav og styringssystem for informasjonssikkerhet for sine regioner, hvor alle regioner svarer at de benytter Normen i stor grad.

> "I virksomhetene i [regionen] benyttes Normen og dens vedlegg ved utarbeidelse og forvaltning av felles regionalt styringssystem for informasjonssikkerhet" (RHF).

Normen benyttes også i stor grad av HF, med unntak av to av elleve som svarer "i moderat grad". Enkelte HF utdyper i sine svar at Normen inngår i regionens styringssystem for informasjonssikkerhet, og utgjør en kilde til deres informasjonssikkerhetsarbeid og rutiner, både internt og overfor eksterne.

> "Rutinene våre rundt informasjonssikkerhet er basert på kravene i Normen, og disse kravene skal også være implementert i innkjøpsprosessene" (HF).

IKT-tjenesteleverandørene på sin side er blitt spurt om de benytter Normen som utgangspunkt for å stille krav mot foretak, leverandører og andre. Tre av fire svarer her at de i stor grad legger Normen til grunn for slike krav.

3.3.2 Vurdering om bruk av Normen for utforming av krav

Alt i alt tyder funnene på at Normen er godt kjent, utbredt og i stor grad implementert i aktuelle prosesser i helsesektoren. Hvis man slår sammen at Normen benyttes "I stor grad" og "I moderat grad" svarer alle RHF, HF og IKT-tjenesteleverandørene at de benytter Normen for utforming av krav.

3.3.3 Anbefaling for bruk av Normen for utforming av krav

Observasjoner fra spørreskjema og kommentarer tyder på at Normen som felles kravsett for sektoren er godt forankret og aktivt i bruk i helsesektoren, også hos IKT-tjenesteleverandørene. Dette er betryggende og i stedet for en anbefaling gis en kommentar på at fortsatt forankring og bevisstgjøring rundt Normen bør foregå med samme styrke som tidligere.

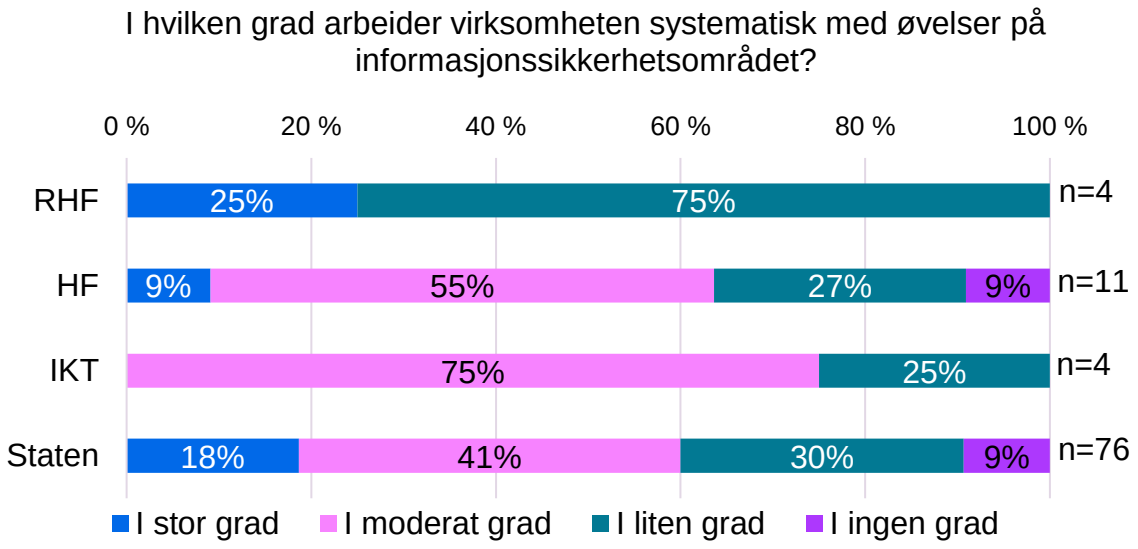
3.4 Beredskap og hendelseshåndtering

Virksomheter må være forberedt på at sikkerhetshendelser vil inntreffe. God beredskapsplanlegging bidrar til at man håndterer uønskede hendelser på en bedre måte. Uten beredskapsplaner som beskriver hvem som har ansvar for hva, vil det bli vanskeligere å håndtere hendelser på en god måte. Det å øve alene eller sammen med andre bidrar til at virksomheter gjør de rette handlingsvalgene. Ved krisehåndtering er tid kritisk for å redusere konsekvensene av en hendelse.

3.4.1 Observasjoner på øvelser på informasjonssikkerhet

For å måle beredskap og hendelseshåndtering har vi stilt spørsmål om øvelser, beredskapsplaner, evaluering av hendelser og hva man vet om kostnadene av en eventuell sikkerhetshendelse.

Diagrammet under viser om respondentene arbeider systematisk med øvelser på informasjonssikkerhetsområdet. Funnene viser at RHFer, HFer og IKT-tjenesteleverandører i moderat eller liten grad arbeider systematisk med slike øvelser.



Ulike spørsmålsstillinger(forkortet):
RHF: I hvilken grad gjennomfører RHF systematisk øvelser på informasjonssikkerhetsområdet i foretaksgruppen?
HF: I hvilken grad arbeider foretaket systematisk med øvelser på informasjonssikkerhetsområdet?

IKT: I hvilken grad arbeider virksomheten systematisk med øvelser på informasjonssikkerhetsområdet?
Staten: I hvilken grad arbeider virksomheten systematisk med øvelser på informasjonssikkerhetsområdet?

Samlet sett arbeider RHFene i liten grad systematisk med øvelser i foretaksgruppen, med unntak av en region som oppgir at de gjør det i stor grad. Dette er ikke unaturlig da de sitter som eiere, nokså langt unna den operative hverdagen. Ett RHF svarer at de "gjør jevnlige øvelser" i samarbeid med lokal beredskapsledelse.

HF og IKT-tjenesteleverandører arbeider stort sett systematisk med slike øvelser, men de fleste oppgir at dette skjer i moderat grad. Det er også verdt å merke at ett HF oppgir at de i ingen grad arbeider systematisk med slike øvelser.

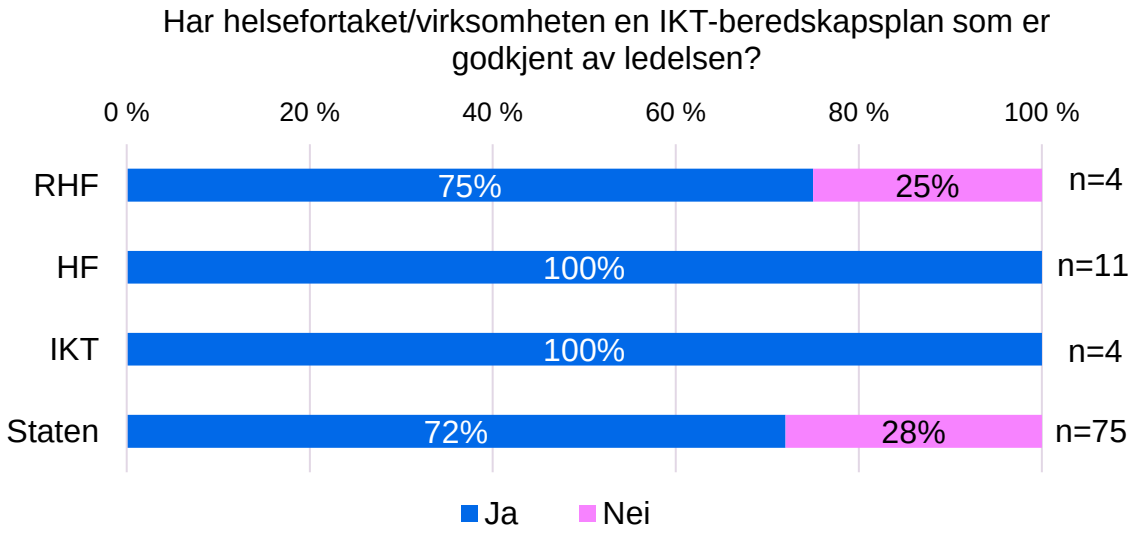
"Vi øver gjennom reelle hendelser …" (HF).

En kommentar er at øving på informasjonssikkerhet kan gå ut over tilgjengeligheten der og da, og at man i tillegg til bortfall (tilgjengelighet) av infrastruktur eller tjenester som journalsystemer også bør øve på integritet og konfidensialitet. Her kan omdømmeøvelser også vurderes.

I statsforvaltningen oppgir 18 prosent av statlige virksomheter at de i stor grad jobber systematisk med øvelser, altså noe flere enn i helsesektoren slik den er definert her. Ellers ligger sektoren omtrent likt med staten.

3.4.2 Observasjoner på IKT-beredskapsplan

Nesten alle har respondentene oppgir at de har IKT-beredskapsplaner, og at de er godkjent av ledelsen i sine respektive virksomheter.



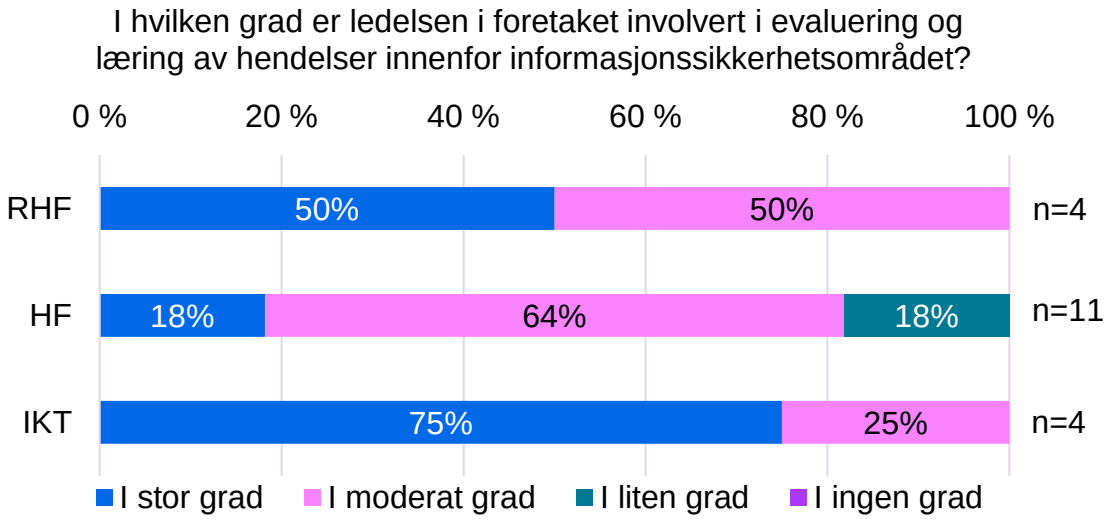
Ulike spørsmålsstillinger(forkortet):
RHF: Har RHF en IKT-beredskapsplan for foretaksgruppen som er godkjent av ledelsen ved det regionale helseforetaket?
HF: Har foretaket en IKT-beredskapsplan som er godkjent av ledelsen for helseforetaket?
IKT: Har virksomheten en IKT-beredskapsplan som er godkjent av virksomhetsledelsen?
Staten: Har virksomheten en IKT-beredskapsplan som er godkjent av virksomhetslederen?

I RHF har tre av fire en godkjent IKT-beredskapsplan. Dette er på nivå med statsforvaltningen, som oppgir at 72 prosent av undersøkte virksomheter hadde en IKT-beredskapsplan. Dette oppfattes her som meget bra.

Ser man på HF og IKT-tjenesteleverandørene har alle respondentene godkjente IKT-beredskapsplaner. Dette er som forventet.

3.4.3 Observasjoner på evaluering og læring av hendelser

Evaluering og læring av sikkerhetshendelser er en viktig del av beredskapen til en virksomhet. I undersøkelsen svarer tilnærmet alle at ledelsen i moderat eller stor grad er involvert i evaluering og læring av hendelser innenfor informasjonssikkerhetsområdet.



Ulike spørsmålsstillinger(forkortet):
RHF: I hvilken grad er ledelsen ved RHF involvert i evaluering og læring av hendelser innenfor informasjonssikkerhetsområdet i foretaksgruppen?
HF: I hvilken grad er ledelsen i foretaket involvert i evaluering og læring av hendelser innenfor informasjonssikkerhetsområdet?
IKT: I hvilken grad er ledelsen i virksomheten involvert i evaluering og læring av hendelser innenfor informasjonssikkerhetsområdet?

Halvparten av RHF og tre av fire IKT-tjenesteleverandører oppgir at egen ledelse i stor grad er involvert i evaluering og læring av hendelser. Her skiller HF seg ut negativt. Kun to av elleve (18 prosent) av HF svarer tilsvarende at ledelsen i stor grad er involvert. I tillegg er det to av elleve (18 prosent) som svarer at ledelsen i liten grad er involvert.

HFene kommenterer at det er noe forskjell mellom det de opplever som generelle virksomhetsøvelser og øvelser innenfor informasjonssikkerhet eller IKT. Virksomhetsøvelser (feilbehandling, konfidensialitetsbrudd) er i større grad gjenstand for evaluering og læring.

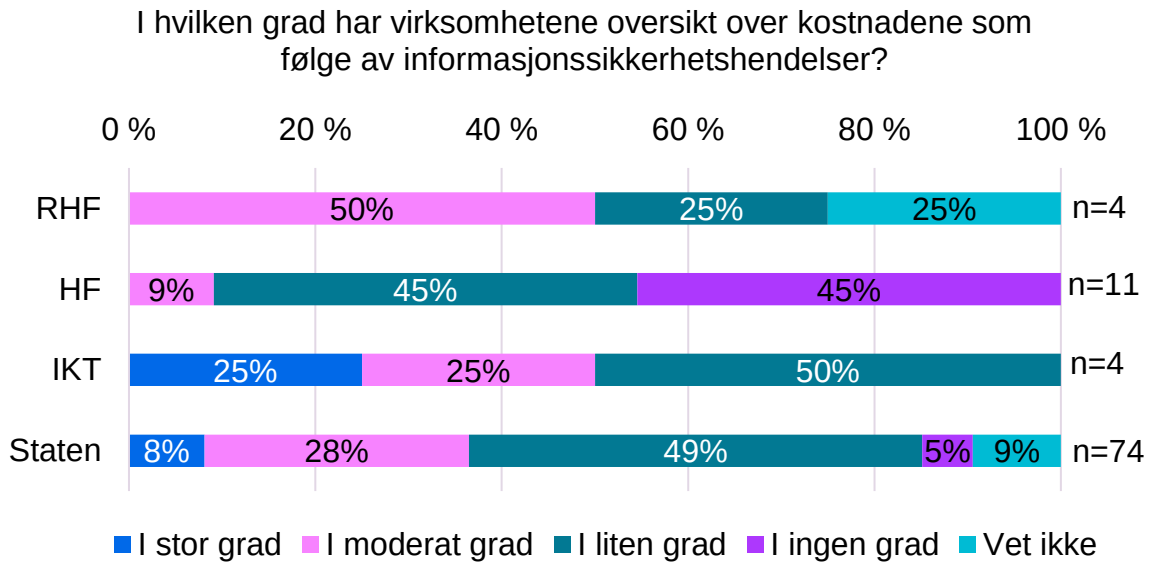
3.4.4 Observasjoner på kostnader ved hendelser

Mørketallsundersøkelsen 2018[12] peker på en gjennomsnittskostnad på 54 000 kroner per hendelse og 2 millioner kroner for den mest alvorlige hendelsen rapportert inn fra virksomheter. Undersøkelsen viser at virksomhetene generelt har liten oversikt over kostnadene knyttet til sikkerhetshendelser.

Funnene i denne undersøkelsen tyder på at det også i helsesektoren er lite kunnskap om kostnadene som følge av informasjonssikkerhetshendelser.

HF skiller seg her spesielt ut der hele 90 prosent (ti av elleve) har svart at de i liten eller ingen grad har oversikt over disse kostnadene. Kun ett HF har svart at de i moderat grad har oversikt over kostnadene ved hendelser. Dette er naturlig siden de fleste kostnadene nok føles mest hos IKT-tjenesteleverandørene. På den annen side bør man også ha et forhold til konsekvensene av hendelser ute hos klinikere og virksomhetene.

[12] Næringslivets Sikkerhetsråd, Mørketallsundersøkelsen 2018 (20.09.2018)



Ulike spørsmålsstillinger(forkortet):
RHF: I hvilken grad har RHF oversikt over kostnadene som følge av informasjonssikkerhetshendelser i foretaksgruppen?
HF: I hvilken grad har foretaket oversikt over kostnadene som følge av informasjonssikkerhetshendelser?
IKT: I hvilken grad har virksomheten oversikt over kostnadene som følge av informasjonssikkerhetshendelser?
Staten: I hvilken grad har virksomheten oversikt over kostnadene som følge av informasjonssikkerhetshendelser?

Kun én respondent fra helsesektoren, en IKT-tjenesteleverandør, svarer at de i stor grad har oversikt og kontroll over kostnaden som følge av informasjonssikkerhetshendelser. For leverandører i markedet er det vanlig å operere med tjenestenivåavtaler som inneholder bøter eller annen kreditering ved reduksjon eller frafall av tilgjengelige tjenester eller, som regel, infrastruktur. For tjenesteleverandører som er eid av RHFene er det ikke naturlig å opprette liknende avtaler, men prinsippene og prosessene for måling av dette kan allikevel adopteres.

Blant statlige virksomheter ser man at 36 prosent svarer i stor, eller moderat grad og 49 prosent i liten grad. Med andre ord skårer verken helsesektor eller statlige virksomheter høyt på denne indikatoren.

IKT-tjenesteleverandørene er de som skårer høyest av respondentgruppene, mens det blant HF framkommer tydelig at det er få som har oversikt og kontroll over kostnadene som følge av informasjonssikkerhetshendelser.

3.4.5 Vurdering på beredskap og hendelseshåndtering

Når en hendelse eller en krise skal håndteres må det fattes mange beslutninger raskt og under usikkerhet. Man har ikke all den informasjonen som man gjerne skulle ønske man hadde, og det er en stor grad av forventning om å gjøre de rette tingene til rett tid. Det stiller store krav til beslutningstakerne og de som jobber tett med håndtering av selve krisen.

Øvelser er et godt verktøy for å drille rutiner, beslutningsveier, og å finne forbedringspunkter. Her har både RHF, HF og til en viss grad IKT-tjenesteleverandørene potensiale for å øke frekvens, spisse øvelsene mot informasjonssikkerhetsområdet og knytte øvelsene opp mot områdene virksomhetene har mest fokus på (pasientsikkerhet, riktig behandling, rennommé, kostnader osv.).

En annen kilde til læring er evaluering av eventuelle sikkerhetshendelser. HF fremstår her som for svake på å involvere egen ledelse i læring og evaluering av slike hendelser. At 18

prosent av HF oppgir at ledelsen i liten grad er involvert i evalueringer av denne typen er for lavt.

Siden både gjennomføring og læring varierer på tvers av regionene bør det være mulig å gjennomføre en interregional øvelse som oppsummeres felles slik at man tar læring av det på tvers av regionene. En kommentar fra arbeidsgruppen er at myndighetene bør utøve mer nasjonal styring og gi føringer og krav i forbindelse med øvelser.

3.4.6 Anbefaling for beredskap og hendelseshåndtering

Alle HF og IKT-tjenesteleverandører rapporterer at beredskapsplaner er godkjent av ledelsen. De store variasjonene i de ulike virksomhetene knyttet til grad av systematisk tilnærming til øvelser, sår tvil om planene er oppdaterte og om det har foregått konkret læring rundt planverket i senere tid.

Direktoratet for e-helse vil komme med følgende anbefalinger:

Anbefaling 4: Helseforetakene, i samarbeid med de regionale helseforetakene og deres IKT-tjenesteleverandør, gjennomfører minst en årlig øvelse innen informasjonssikkerhet. Både planlegging og rapportering av erfaringer fra øvelsen må knyttes opp mot virksomhetenes styringssystem for informasjonssikkerhet, men kan også være en del av virksomhetenes ordinære øvelser.

Anbefaling 5: Regionene bør søke å samarbeide om et felles rullerende øvelsesopplegg innenfor informasjonssikkerhet. Dette for å trekke ut felles lærdommer, beste praksis og løfte de som ligger etter i beredskapsplanlegging og -øvelser. En slik øvelse kan foregå hvert annet år, og f.eks. ta for seg en nasjonal hendelse (feil i legemiddel, feil i nasjonal infrastruktur eller andre tverrsektorielle problemstillinger).

På sikt bør man på nasjonalt nivå vurdere deltakelse i internasjonale øvelser for å få erfaring med grenseoverskridende hendelser.

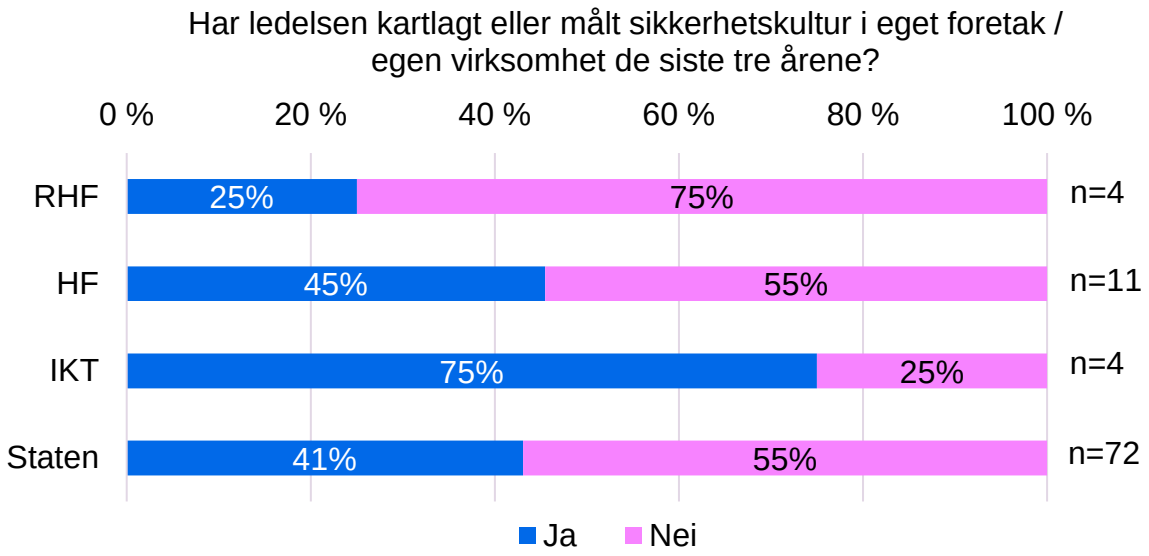
3.5 Sikkerhetskultur

Sikkerhetskultur regnes som en del av organisasjonskulturen, og handler om hvilke felles verdier og normer som ligger til grunn for risikoforståelse, den enkeltes valg for hvordan informasjon håndteres og hvordan man reagerer på avvik eller sikkerhetsbrudd.

3.5.1 Observasjoner på måling av sikkerhetskultur

Sikkerhetskulturen i en virksomhet kan ha positive eller negative konsekvenser for informasjonssikkerheten. Kartlegging av kultur er et godt utgangspunkt for å påvirke og endre sikkerhetskulturen. En god sikkerhetskultur kan gi bedre effekt av sikkerhetstiltak.

Ledelsen i RHF, HF og IKT-tjenesteleverandørene ble spurt om de har kartlagt eller målt sikkerhetskulturen i deres eget foretak, eller virksomhet, de siste tre årene. Funnene viser at respondentene i varierende grad har undersøkt og er bevisst sin organisasjons sikkerhetskultur.



Ulike spørsmålsstillinger(forkortet):
RHF: Har ledelsen ved RHF kartlagt eller målt sikkerhetskultur i eget foretak (her mener vi i RHF) i løpet av de siste tre årene?
HF: Har foretaksledelsen kartlagt eller målt sikkerhetskultur i eget foretak i løpet av de siste tre årene?
IKT: Har ledelsen kartlagt eller målt sikkerhetskultur i egen virksomhet i løpet av de siste tre årene?
Staten: Har ledelsen kartlagt eller målt sikkerhetskultur i egen virksomhet i løpet av de siste tre årene?

Blant RHFene oppgir kun 25 prosent (én av fire) at ledelsen har kartlagt eller målt sikkerhetskultur i eget foretak de siste tre årene. For HF har 45 prosent (fem av elleve) kartlagt eller målt sikkerhetskultur. Dette er på nivå med andelen for statlige virksomheter (41 prosent). Det er blant IKT-tjenesteleverandørene at ledelsen i størst grad har gjennomført slike kartlegginger, med tre av fire virksomheter. Respondentene fra HF og IKT-tjenesteleverandørene skårer samlet litt over nivået for statlige virksomheter, men med tanke på graden av konfidensiell og sensitiv informasjon som behandles i helsesektoren oppfattes dette som lavt.

3.5.2 Vurdering av måling av sikkerhetskultur

I Mørketallsundersøkelsen 2018 peker man på at sikkerhetskulturen er under press, de vanligste informasjonssikkerhetshendelsene er phishing og sosial manipulering, mens de vanligste årsakene er:

> "[…] tilfeldigheter og uflaks, menneskelige feil, mangel på sikkerhetsbevissthet hos de ansatte og at eksisterende prosesser ikke blir fulgt" (Næringslivets Sikkerhetsråd 2018).

Det pekes også på at phishing og sosial manipulering har doblet seg siden 2016.Det er rimelig å anta at disse tallene også gjelder for helsesektoren.

3.5.3 Anbefaling på måling av sikkerhetskultur

Selv om sikkerhetskulturen må vurderes ut fra den enkelte virksomhets oppgaver og egenart bør man også i RHF (eierorganisasjon) søke å løfte antallet som har kartlagt sikkerhetskultur noe (er i dag 25 prosent). Det vil bidra til å sende et signal om fokus til underliggende virksomheter. Anbefalingen her er derfor generell og til alle virksomhetsnivå.

Direktoratet for e-helse vil komme med følgende anbefalinger:

Anbefaling 6: Virksomheter kartlegger sin sikkerhetskultur. På bakgrunn av kartleggingen utformer virksomheten eventuelle tiltak til forbedring.

Det foreslås å ha en felles nasjonal tilnærming i kartleggingen, dette kan presenteres i et felles resultat som også bør kommuniseres eksternt og bidra til trygghet blant brukere[13].

[13] NorSIS (Norsk Senter for Informasjonssikring) kan være en samarbeidspartner her

4 Modenhetsundersøkelse IKT-tjenesteleverandører

Innenfor fagområdet informasjonssikkerhet er det ikke entydig hva som benyttes til å måle status eller tilstand; det benyttes stort sett ulike spørreundersøkelser for å etablere status og mål for fagområdet. Noen spørreundersøkelser er knyttet opp mot modenhetsmodeller, som er et sett med egenskaper, indikatorer eller mønstre som representerer kapabiliteter innenfor et fagområde eller en organisasjon.

4.1 Kort om modenhetsmodeller

Modenhetsmodellen inneholder vanligvis eksempler på beste praksis, standarder eller andre retningslinjer for fagområdet. Modellen gir dermed en referansemåling som en virksomhet kan evaluere sitt gjeldende kapabilitetsnivå mot, og deretter sette mål og prioriteringer for forbedring.

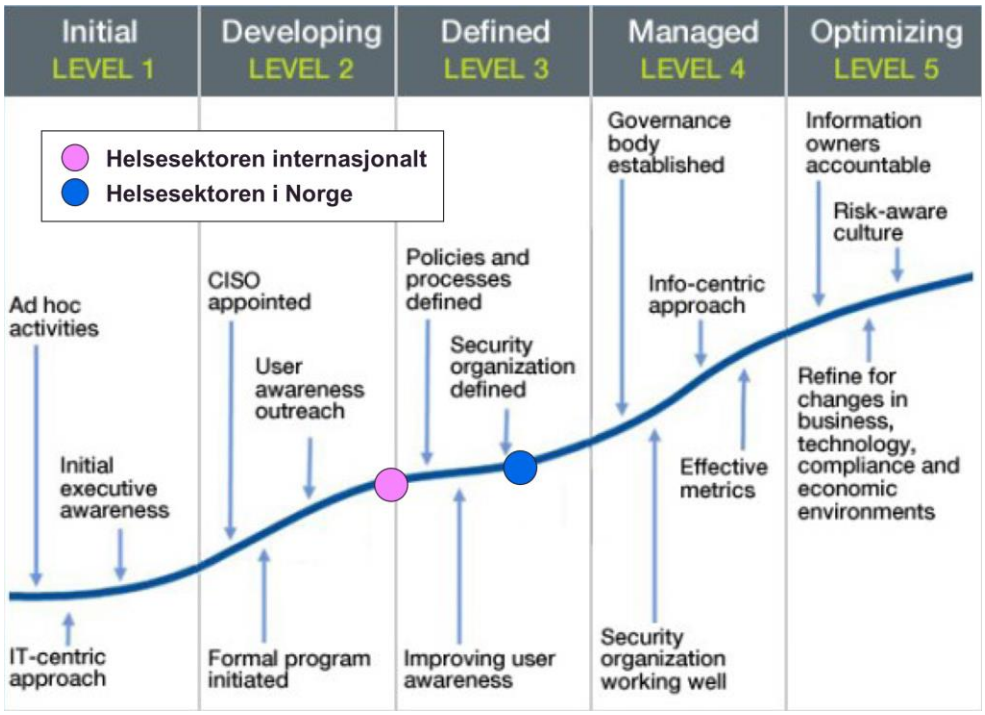
Når en modell er mye brukt i en bestemt bransje og vurderingsresultatene deles, kan organisasjoner også gjøre en referansemåling (benchmarking) av sine resultater mot andre organisasjoner. Internasjonalt benyttes ofte modenhetsstegene fra CMMI[14] i modellene.

4.1.1 Observasjoner på modenhetsundersøkelse IKT-tjenesteleverandør

I denne rapporten er det benyttet en selvevalueringsmodell som inneholder resultater fra virksomheter i helsesektoren globalt (ITScore fra Gartner[15]):

[14] CMMI- Capability Maturity Model Integration

[15] Gartner ITScore for Information Security er tilgjengelig for brukere av Gartner Research tjenester



Det er 6 modenhetsnivå, på en skala fra 0-5 (0 = kaos, ikke vist i figuren over). Det internasjonale gjennomsnittet er rundt 3, mens Norge ligger på 3,6. Beregningen av ITScore for informasjonssikkerhet i Norge er et gjennomsnitt for de regionale IKT-tjenesteleverandørene og Norsk helsenett.

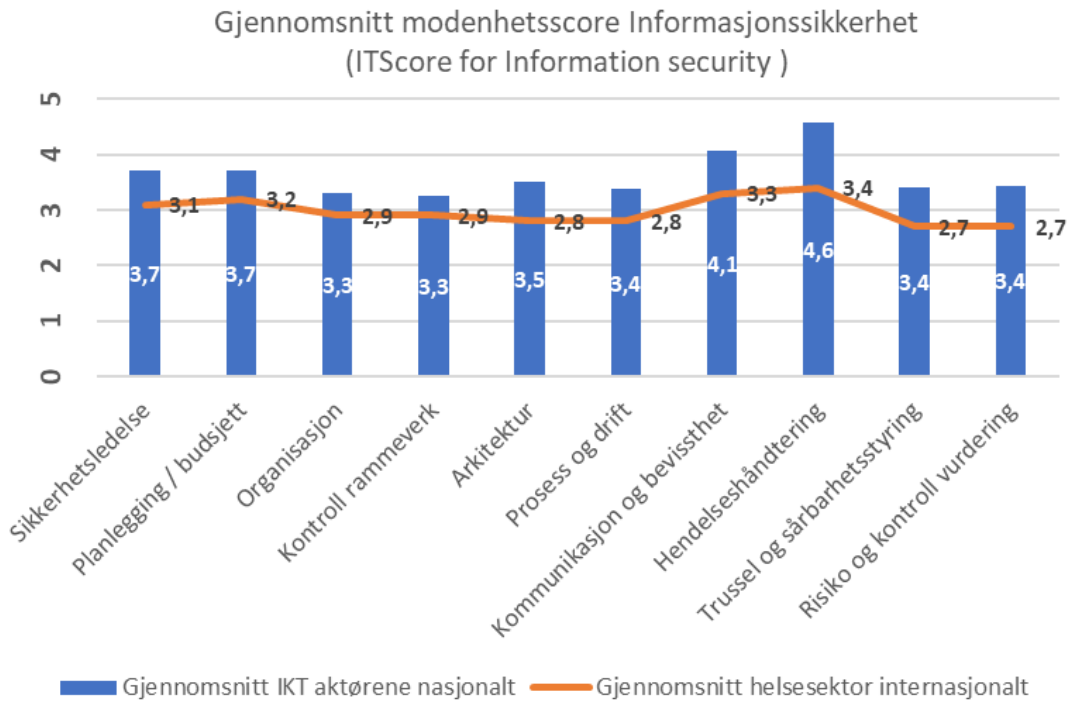
4.1.2 Observasjoner av modenhet på prosesser / fagområder

Litt dypere ned i modellen er det benyttet graderte spørsmål innenfor 10 fagområder, som har fått hver sin skåre:

- **Sikkerhetsledelse**: Evnen til å gi tydelig ansvar, beslutningsmyndighet og prioritere for å sikre at virksomhetens mål er oppfylt.
- **Planlegging / budsjett**: Umodne organisasjoner arbeider ad-hoc mens modne organisasjoner planlegger og gjennomfører virksomhetsdefinerte sikkerhetsstrategier.
- **Organisasjon**: Modne organisasjoner sikrer at de riktige personene forstår sine roller, har klare eskaleringsveier og samhandler effektivt om informasjonssikkerhet.
- **Rammeverk for kontroll**: Et modent styringssystem for informasjonssikkerhet henger sammen i sine aktiviteter og tekniske mekanismer.
- **Arkitektur**: Effektiv sikkerhet er en del av applikasjonsutviklingsprosessene, og teknologianskaffelser er i tråd med sikkerhetsteknologien som planlegges.
- **Prosess og drift**: Grundig og konsistent gjennomføring av dokumenterte aktiviteter og prosedyrer er et kjennetegn for et styringssystem for informasjonssikkerhet.
- **Kommunikasjon og bevissthet**: Mennesker er en del av sikkerhetsøkosystemet og riktig kultur og kommunikasjon styrer individene til å følge retningslinjene.
- **Hendelseshåndtering**: Modne styringssystem for informasjonssikkerhet blir raskt oppmerksomme på sikkerhetshendelser og mer effektiv i å hindre, undersøke og gjenopprette.
- **Trussel og sårbarhetsstyring**: Fordi IKT utsettes løpende for nye sårbarheter må prosesser etableres for oppdateringer og nye konfigurasjoner, og for effektiv utrulling.

- **Risiko og kontroll vurdering**: I hjertet av ethvert informasjonssikkerhetssystem er evnen til å estimere risiko og måle effekten av kontroller.

ITScore for hvert fagområde ser samlet slik ut for IKT-tjenesteleverandørene og Norsk helsenett:



4.1.3 Analyse av modenhet på prosesser / fagområder

Spredningen blant respondentene går fra 3,2 til 4,2 i gjennomsnittsskåre, altså er alle over det internasjonale gjennomsnittet. Dette gjelder også for hvert fagområde med unntak av én virksomhet som rapporterer å ligge under det internasjonale gjennomsnittet forområdet organisering. Det oppfattes at det er noe forskjell på risikoappetitt mellom regionene.

Dette viser at RHFenes IKT-tjenesteleverandører og NHN ligger på et modenhetsnivå mellom 3 og 4 i modenhetsmodellen. Det kan være nyttig å gjøre seg kjent med disse nivåene for å etablere en felles nullpunktsmåling som sier noe om hvor man står i dag.

På nivå 3 i modellen har den enkelte virksomhet etablert et "solid antall retningslinjer" for informasjonssikkerhet og er i "tidlig fase av å definere en tydelig ansvarsmatrise" som definerer individuelle informasjonssikkerhetsroller. Regler er på plass, men ansvarlighet for og håndhevelse av disse reglene er i de tidligste stadiene. Informasjonssikkerhetsaktiviteter er fremdeles sentrert rundt IKT i virksomheten.

På nivå 4 i modellen er ansvarsmatrise for informasjonssikkerhet godt etablert og noe formell ansvarlighet eksisterer, men virksomhetssiden tar kun delvis ansvar for risiko på siden av fagområdet. Det finnes et "formalisert tverrorganisatorisk utvalg" som ledes av en informasjonssikkerhetsleder (CISO[16]), som har "bilateral utveksling av informasjon og meninger mellom fagfolk innen informasjonssikkerhet og virksomhetssiden". Man er på vei

[16] CISO – Chief Information Security Officer (øverste informasjonssikkerhetsleder i en virksomhet)

bort fra en IKT-sentrisk modell og sikkerhetsansvaret overføres mer tydelig til en informasjonssikkerhetsleder for virksomheten. Alle risikoer som nå kan være rimelig forventet tas opp og rapporteres gjennom etablerte prosesser og definerte metrikker som igjen sikrer at definerte tjenestenivåer blir oppfylt. Håndhevelse av informasjonssikkerhet er strukturert og formalisert.

4.1.4 Forbedringsforslag for økt modenhet på prosesser / fagområder

Forslag til forbedring og økt modenhet hos de regionale IKT-tjenesteleverandørene samt NHN genereres basert på det nivået man ligger på i modenhetsmodellen. Siden det benyttes aggregerte tall er presisjonen ikke så god som den burde være og det er valgt å kun liste opp forslag til beste-praksis forbedringer som deltakerne kan vurdere:

- Etablere en formell tverrgående komité for å diskutere og samarbeide om informasjonssikkerhetsspørsmål. Komiteen skal være på beslutningsdyktig nivå og ha medlemmer fra virksomhetsledelsen i HF, IKT-tjenesteleverandør og HF IKT sikkerhetsledere
- Styringssystem for informasjonssikkerhet skal minimum revideres årlig
- Gjennomføre en gapanalyse for å identifisere og prioritere områder der forbedring er nødvendig
- Lage realistiske metrikker som kan gjøres noe med/påvirkes for å måle suksess og utfordringer i informasjonssikkerhetssystemet og formidle dem til toppledelsen
- Skille ut operasjonelle informasjonssikkerhetsfunksjoner fra strategiske risikostyringsfunksjoner
- Forsikre at det finnes en formalisert ansvarsmatrise på plass
- Forsikre at linjeledere og eiere av virksomhetsprosesser aksepterer eksplisitt ansvar for risikoen forbundet med deres bruk av informasjon og informasjonsteknologi
- Implementere et virksomhetssikkerhetsprogram som fokuserer på å sikre at ansatte har kultur, bevissthet, vilje og evne til å overholde fastlagte sikkerhetsregler
- La CISO rapportere til styret i virksomheten, minst halvårlig, om suksessene og utfordringene ved informasjonssikkerhetsprogrammet og restrisikoer som er relevante for viktige virksomhetsmål
- Arbeide for å utvikle en prosess med kontinuerlig forbedring, ved å bruke metrikker og beregninger for å styre og øke bidrag fra enkeltpersoner og virksomhet utover minstekrav.

5 Oppfølging og tilbakemelding

Dette er første gang det gjennomføres en nasjonal survey og modenhetsmåling av RHF, HF og IKT-tjenesteleverandørene i spesialisthelsetjenesten samlet. Rapporten vil vurderes videreført i samarbeid med deltakerne, i den forbindelse er det viktig å få med seg forbedringsforslag allerede nå, noen av disse er listet opp under.

5.1 Forbedringsforslag til undersøkelsen

I del 4 av spørreskjemaene kom det inn følgende forbedringsforslag fra RHF:

- *Spørsmål 3 og hvor begrepet «linjeledelse i foretaksgruppen» blir misvisende da hver virksomhet er selvstendige juridiske virksomheter med et selvstendig juridisk ansvar.*
- *Lettere om undersøkelsen var delt i 2 deler. En del for plan og utviklingsarbeid, og del til kontroll og oppfølging.*
- *Indikatorene/kategoriene som brukes (i noen grad, moderat osv.) bør defineres presist slik at de ikke kan vurderes ulikt hos respondentene.*
- *Spørsmålene må ikke være relatert til en bestemt organisasjonsmodell eller styringssystem for informasjonssikkerhet.*

Og følgende forbedringsforslag fra HF:

- *Være tydeligere på om man snakker om foretaksledelse i det regionale foretaket, det lokale helseforetaket eller IT foretaket i spørsmålsstillingene.*
- *Vurder om hensiktsmessig å dele spørsmål 3 i 2, så kan ta høyde for både/og-organisering.*
- *Der var vanskelig å dele eks. spørsmål 3 der vi blir bedt å dele mellom ledere og fagpersoner. Jeg ville ha besvart begge områdene, men på litt annet vis.*
- *Svarene må forstås ut fra min rolle og ståsted som IKT sikkerhetsleder. Toppledelsen får annen informasjon enn jeg får, og hadde trolig svart noen av spørsmålene annerledes enn meg.*
- *Gjennomfør dybdeintervju i tillegg, mer presise svar, blir litt kort her.*
- *Samkjøre med andre statlige myndigheter som f.eks. Datatilsynet og Riksrevisjonen? Dere spør om de samme tingene, men på hver deres måte.*
- *Gjøre undersøkelsen elektronisk.*

Fra Modenhetsundersøkelsen kom det inn kommentarer fra IKT-tjenesteleverandørene:

- *Oversettelsen i foreliggende form gjør det ikke enklere å besvare spørsmålene. Vurder å behold originalt språk med norsk hjelpetekst til å forstå kontekst.*
- *Spørsmålene får ikke fram arbeid som gjøres, men som ikke passer innenfor begreper brukt i standarder/rammeverk.*
- *Flere spørsmålsformuleringer er doble (f.eks «vi gjør X og Y") som egentlig burde vært separate spørsmål.*

---x---

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt
postmottak@ehelse.no