Digdir-rapport ISSN 2703-7061

2020:3

Digdir

Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner

Kunnskapsgrunnlag – En dokumentstudie

www.digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarvegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo

Forord

Digitaliseringsdirektoratet har på oppdrag fra Kommunal- og moderniseringsdepartementet (KMD) undersøkt hvordan fylkeskommuner og kommuner arbeider med informasjonssikkerhet. Arbeidet er utført i samarbeid med KS.

Vi vil takke våre samarbeidspartnere som har bidratt med kunnskap og innspill til videre arbeid.

Svanhild Gundersen har vært prosjektleder. Elisabeth Aspaas Runsjø og Zoya Shah har vært prosjektdeltakere. Seksjonssjef Kjetil Korslien har vært prosjektansvarlig.

Oslo, 30.11.2020

Grete Orderud

avdelingsdirektør

Innhold

Sammendrag

Kommunal- og moderniseringsdepartementet (KMD) har gitt Digitaliseringsdirektoratet i samarbeid med KS oppdrag i tildelingsbrevet for 2020 å få frem et kunnskapsgrunnlag om arbeidet med informasjonssikkerhet i kommunene.

Oppdraget må sees i lys av tiltak 5 i «*Tiltaksoversikt til Nasjonal strategi for digital sikkerhet*» om at Digitaliseringsdirektoratets «arbeid med styring og kontroll på informasjonssikkerhet skal utvides til å omfatte både statsforvaltningen og kommunene fordi utfordringene i statsforvaltningen gjelder også for kommunene». Både KS og Foreningen kommunal informasjonssikkerhet (KiNS) er sentrale veiledningsaktører mot kommunene på informasjonssikkerhetsområdet. Digitaliseringsdirektoratet har etablert samarbeid med begge disse aktørene da vi mener at effekten av veiledningsarbeidet mot kommunene blir mest effektivt dersom veiledningsaktørene på området er koordinert og samkjørt.

I fagdialog med KMD presiseres det at fylkeskommuner også omfattes av oppdraget i tildelingsbrevet. Formålet med kunnskapsgrunnlaget er å få en bedre forståelse av hvordan fylkeskommuner og kommuner arbeider med informasjonssikkerhet.

Kunnskapsgrunnlaget tar utgangspunkt i observasjoner fra utvalgte dokumenter og det gis faglige vurderinger av disse observasjonene. Observasjonene er direkte hentet fra datagrunnlaget. Vurderingene er Digitaliseringsdirektoratets faglige analyse av datagrunnlaget vurdert opp mot Digitaliseringsdirektoratets veileder «*Internkontroll i praksis – informasjonssikkerhet*» samt andre anbefalinger og veiledningsmateriell på informasjonssikkerhetsområdet.

Samlet sett viser kunnskapsgrunnlaget at fylkeskommuner og kommuner, og spesielt små og mellomstore kommuner, ikke har tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet.

Oppsummering av vurderingene

Vurderingene fra dette kunnskapsgrunnlaget er oppsummert nedenfor:

Styring og kontroll (internkontroll)

Kunnskapsgrunnlaget finner svakheter i fylkeskommuners og kommuners arbeid med å etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet. Spesielt gjelder dette små og mellomstore kommuner. Dette indikerer at kommunestørrelse kan ha betydning for hvordan det arbeides med informasjonssikkerhet.

Små og mellomstore kommuner har i mindre grad enn fylkeskommuner og store kommuner en skriftlig informasjonssikkerhetspolicy og en formelt utnevnt person som er fagansvarlig for informasjonssikkerheten.

Kommuner har i mindre grad enn fylkeskommuner evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet. Få fylkeskommuner og kommuner oppgir at de har rapportert erfaringer fra øvelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten.

Små kommuner gjennomfører i særlig liten grad risikovurderinger systematisk og periodisk.

Beredskap, øvelser og hendelseshåndtering
Få fylkeskommuner og kommuner gjennomfører øvelser knyttet til informasjonssikkerhet minst én gang årlig. Sett i lys av Digitaliseringsdirektoratets anbefalinger om å øve minst én gang pr år indikerer dette at fylkeskommuner og kommuner ikke i tilstrekkelig grad gjennomfører øvelser knyttet til informasjonssikkerhet.

Sikkerhetskultur og sikkerhetskompetanse
Under halvparten av små og mellomstore kommuner gjennomfører kompetansehevende aktiviteter minst én gang i året. Fylkeskommuner og store kommuner gjør dette i større grad enn små og mellomstore kommuner.

Manglende kompetanse og forståelse hos både medarbeidere og ledere, samt manglende kultur, utgjør hindringer i forbindelse med informasjonssikkerhet.

Dette indikerer at fylkeskommuner og kommuner ikke i tilstrekkelig grad arbeider med kompetanseutvikling og sikkerhetskultur.

Våre hovedanbefalinger

Digitaliseringsdirektoratet gir følgende hovedanbefalinger om innretningen av videre arbeid på informasjonssikkerhetsområdet mot fylkeskommuner og kommuner:

1. Veiledning knyttet til hvordan virksomhetene kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet bør spesielt rettes mot små og mellomstore kommuner.

2. Veiledning i øvelser knyttet til informasjonssikkerhet bør rettes mot både fylkeskommuner og kommuner.

3. Veiledning i hvordan man identifiserer behov for kompetanse- og kulturutvikling bør rettes mot både fylkeskommuner og kommuner, spesielt mot små og mellomstore kommuner.

Det vil være mulig å basere mye av veiledningen på eksisterende og pågående arbeid, og det må legges til rette for samarbeid mellom veiledningsaktører på informasjonssikkerhetsområdet slik at videre arbeid fremstår helhetlig.

Kunnskapsgrunnlaget viser til eksisterende og planlagte tiltak i KS, Foreningen kommunal informasjonssikkerhet (KiNS), Direktoratet for samfunnssikkerhet og beredskap (DSB) og Digitaliseringsdirektoratet, som vil være egnet til å følge opp anbefalingene.

1 Innledning

1.1 Oppdrag og mandat

I oppdrag 9 i tildelingsbrev for 2020 fra KMD fikk Digitaliseringsdirektoratet følgende oppdrag: «Digitaliseringsdirektoratet skal i samarbeid med KS få frem et kunnskapsgrunnlag om arbeidet med informasjonssikkerhet i kommunene». I fagdialog med KMD presiseres det at fylkeskommuner også omfattes av dette oppdraget. Oppdraget har frist 1. september 2020.

Oppdraget må sees i lys av tiltak 5 i tiltaksoversikten til Nasjonal strategi for digital sikkerhet og Digitaliseringsstrategien for offentlig sektor. Tiltak 5 sier blant annet at Digitaliseringsdirektoratets «arbeid med styring og kontroll på informasjonssikkerhet skal utvides til å omfatte både statsforvaltningen og kommunene fordi utfordringene i statsforvaltningen gjelder også for kommunene». Videre følger det av digitaliseringsstrategien «*Én digital offentlig sektor – Digitaliseringsstrategi for offentlig sektor 2019-2025*» fra 2019 at «sikkerhetsmessige hensyn som må ivaretas av kommunal sektor som eget forvaltningsnivå, får den nødvendige plass i det nasjonale arbeidet og at kommunal sektor sikres medinnflytelse på gjennomføring av tiltak».

Formålet med kunnskapsgrunnlaget er å få en bedre forståelse av hvordan fylkeskommuner og kommuner arbeider med informasjonssikkerhet.

I dette kunnskapsgrunnlaget gir Digitaliseringsdirektoratet anbefalinger om innretningen av videre arbeid på informasjonssikkerhetsområdet mot fylkeskommuner og kommuner.

Samarbeidet med KS
Kunnskapsgrunnlaget er utarbeidet av Digitaliseringsdirektoratet. Som en del av samarbeidet med KS, har Digitaliseringsdirektoratet og KS hatt flere samtaler om oppdraget der det har blitt utvekslet relevant informasjon. KS har kommet med innspill til datagrunnlaget, lest igjennom og kommet med tilbakemeldinger på vurderingene og anbefalingene underveis i arbeidet. KS foreslår at vurderingene og anbefalingene bringes inn i samtaler med kommunene, for eksempel gjennom KommIT-rådet[1].

1.2 Presisering og begrensning av oppdraget

Kunnskapsgrunnlaget belyser hvordan fylkeskommuner og kommuner arbeider med informasjonssikkerhet. Kunnskapsgrunnlaget er ikke en kartlegging av selve sikkerhetstilstanden. Kunnskapsgrunnlaget omhandler det systematiske arbeidet med internkontroll på informasjonssikkerhetsområdet som utføres internt i fylkeskommuner og kommuner.

Risikostyring i en virksomhet omfatter all informasjonsbehandling, også behandling av personopplysninger. Kunnskapsgrunnlaget omfatter derfor i noen grad informasjonssikkerhet for personopplysninger, men vil ikke omtale personvernområdet som sådan.

[1] https://www.ks.no/kommit [hentet 28.08.2020]

Norsk senter for informasjonssikring (NorSIS) utredet i 2017 de felles behovene for støtte til håndtering av IKT-sikkerhetshendelser i kommunene.[2] På bakgrunn av denne utredningen og Direktoratet for samfunnssikkerhet og beredskap (DSB) sin kartlegging «*IKT-sikkerhet på lokalt og regionalt nivå*» fra 2018 (intern rapport), ble Kommune-CSIRT opprettet.[3] I dette kunnskapsgrunnlaget ville det vært positivt å kunne uttale seg om kommunenes behov for støtte og håndtering av IKT-sikkerhetshendelser, ved å for eksempel gi en anbefaling vedrørende Kommune-CSIRT som løsning på utfordringene i kommunal sektor. Da vi ikke har hatt muligheten til å gjennomføre egne spørreundersøkelser, har vi heller ikke grunnlag for å komme med vurderinger utover det som følger av utredningene beskrevet over. Vi vil derfor i dette kunnskapsgrunnlaget ikke komme med konkrete anbefalinger knyttet til Kommune-CSIRT.

1.3 Metode og datagrunnlag

Metoden vi har benyttet er dokumentstudier. Det har vært ønskelig å gjennomføre undersøkelser rettet mot fylkeskommuner og kommuner. I dialog med KS ble det besluttet at det i denne omgang ikke var forsvarlig å belaste kommunene med spørreundersøkelser på grunn av den pågående Covid-19-pandemien.

Datagrunnlaget består dermed av følgende dokumenter fra perioden 2015-2020:

- Tabeller fra SSBs statistikk «*Bruk av IKT i offentlig sektor*»[4] (oppdatert mai 2020):
  - Tabell 12041: *«Tiltak/rutiner ved administrasjon av IKT-sikkerheten, etter antall innbyggere (Fylkeskommuner, kommuner) 2018»*. Antall respondenter er omtalt i vedlegg B.
  - Tabell 12042: *«Tiltak som del av internkontroll for informasjonssikkerhet (Statlige virksomheter, fylkeskommuner, kommuner) 2018-2020»*. Antall respondenter er omtalt i vedlegg B.
- DSB. «*IKT-sikkerhet på lokalt og regionalt nivå*» (intern rapport), 2018. Vi har i tillegg mottatt utvalgte grunnlagsdata fra DSB for rapporten, se vedlegg C.
- NorSIS. «*Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)*», 2017.
- KS. «*Oppdatert kunnskapsgrunnlag på digitaliseringsområdet, Kartlegging av digital modenhet i kommunesektoren*», 2018.
- NOU 2015:13 «*Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*» (Lysneutvalget), 2015.
- NOU 2018:14 «*IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.*» (Holteutvalget), 2018.
- Utvalgte vedtak fra Datatilsynet (2019):
  - *Vedtak om pålegg og overtredelsesgebyr – Bergen kommune, 18.03.2019.*

[2] Norsk senter for informasjonssikring (2017). *Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)*. [https://norsis.no/wp-content/uploads/2018/05/Utredning-Kommune-CSIRT.pdf]
[3] se https://kommunecsirt.no/ [hentet 19.06.2020]
[4] For detaljer om denne statistikken se «Om statistikken» på [https://www.ssb.no/teknologi-og-innovasjon/statistikker/iktbruks]. Se spesielt «Nøyaktighet og pålitelighet».

- *Varsel om overtredelsesgebyr – Melding om avvik i Oslo kommune Sykehjemsetaten - Oslo kommune Sykehjemsetaten, 11.10.2019.*
- *Vedtak om pålegg – Arendal kommune – Behandling av personopplysninger i kartleggingsverktøyet Spekter,* 23.10.2019.

SSBs tabell 12041 er inndelt både etter forvaltningsnivå (fylkeskommuner og kommuner) og antall innbyggere. Tabellen deler i utgangspunktet kommuner inn i syv størrelsesgrupperinger. SSB har også i flere andre sammenhenger delt inn kommuner i tre størrelsesgrupperinger.[5] For dette kunnskapsgrunnlaget har vi valgt å bruke den tredelte størrelsesgrupperingen, se punktliste under. SSB har regnet ut prosenttall for tabell 12041 i henhold til denne inndelingen (se vedlegg A).

- Små kommuner: Kommuner med 0-4999 innbyggere
- Mellomstore kommuner: Kommuner med 5000-19999 innbyggere
- Store kommuner: Kommuner med minst 20000 innbyggere

Kunnskapsgrunnlaget tar utgangspunkt i observasjoner fra dokumentene beskrevet over og gir faglige vurderinger av disse observasjonene.

1.4 Leseveiledning

Hoveddelen av dette kunnskapsgrunnlaget har følgende inndeling:

Kapittel 2 beskriver føringer for arbeidet med informasjonssikkerhet, herunder fylkeskommuners og kommuners organisering samt føringer for styring og kontroll på informasjonssikkerhetsområdet.

Kapittel 3 beskriver observasjoner og vurderinger på sentrale områder i arbeidet med informasjonssikkerhet.

Kapittel 4 beskriver anbefalinger knyttet til oppfølgingen av observasjonene og vurderingene.

Kapittel 5 beskriver forslag til videre innretning av arbeidet med informasjonssikkerhet mot fylkeskommuner og kommuner.

Vedlegg:

Vedlegg A inneholder prosenttall regnet ut av SSB for tabell 12041 i henhold til inndelingen i små, mellomstore og store kommuner.

Vedlegg B gir antall respondenter i SSBs tabell 12041 og tabell 12042.

Vedlegg C viser utvalgte grunnlagsdata for DSBs rapport «*IKT-sikkerhet på lokalt og regionalt nivå*».

Vedlegg D beskriver pågående og planlagte tiltak i regi av DSB.

Vedlegg E beskriver pågående og planlagte tiltak i regi av KiNS.

Vedlegg F beskriver pågående og planlagte tiltak i regi av KS.

[5] Se for eksempel rapporten «Gruppering av kommuner etter folkemengde og økonomiske rammebetingelser 2000» s. 10 [https://www.ssb.no/a/publikasjoner/pdf/rapp_201108/rapp_201108.pdf]

2 Føringer for arbeidet med informasjonssikkerhet

2.1 Fylkeskommuners og kommuners organisering

Fylkeskommuner og kommuner er selvstendige forvaltningsnivåer i Norge og har gjennom det fylkeskommunale og kommunale selvstyret rett til å styre seg selv.[6] Begrensninger i denne retten må ha hjemmel i lov.[7]

Lov om kommuner og fylkeskommuner (kommuneloven) gir nærmere regler om fylkeskommuners og kommuners organisering. Etter kommuneloven § 5-3 er all utøving av fylkeskommunal eller kommunal kompetanse lagt til fylkestinget og kommunestyret som øverste organ. Det er med andre ord disse politisk valgte organene som innehar den reelle avgjørelsesmyndigheten om hvordan det administrative apparatet i fylkeskommunen og kommunen skal organiseres, også når det gjelder organiseringen av informasjonssikkerhetsarbeidet.

Kommunelovens regler om organisering åpner i utgangspunktet opp for store variasjoner i hvordan fylkeskommuner og kommuner organiserer seg. Tradisjonelt har den administrative strukturen fulgt en hierarkisk organisasjonsmodell basert på en inndeling i etater eller sektorer, ofte kalt etatsmodellen eller sektormodellen. Flere fylkeskommuner og kommuner har også innført administrative modeller med flatere struktur og resultatenheter, ofte kalt to-nivåmodellen. Denne modellen bygger derimot på ideen om at drift og resultat må ses mer i sammenheng samt at myndighet delegeres lengre ned i organisasjonen.[8]

2.2 Føringer for styring og kontroll på informasjonssikkerhetsområdet

Offentlige virksomheter[9] er gjennom ulike regelverk pålagt visse krav til å ha et systematisk arbeid med informasjonssikkerhet.

For fylkeskommuner og kommuner er det i utgangspunktet nærliggende å se til kommunelovens bestemmelser om internkontroll, se for eksempel kommuneloven § 25-1 første ledd som stiller krav om at «kommuner og fylkeskommuner skal ha internkontroll med administrasjonens ledelse». Bestemmelsen regulerer det generelle arbeidet med systematisk kontroll med administrasjonens virksomhet.[10]

For å utdype hvordan fylkeskommuner og kommuner kan gjennomføre internkontroll etter kommuneloven § 25-1 i praksis, har KS den 4. juni 2020 lansert veilederen «*Orden i eget hus – Kommunedirektørens internkontroll*», samt en egen temaside om internkontroll.[11] Veilederen fra KS har til hensikt å gi oversikt og praktisk støtte til

[6] Kongeriket Noregs Grunnlov (Grunnloven) § 49 og Lov om kommuner og fylkeskommuner (Kommuneloven) § 2-1 annet ledd
[7] Lov om kommuner og fylkeskommuner (Kommuneloven) § 2-1 tredje ledd
[8] Engelsrud, Gerd, Gunnar Jahren og Ingun Sletnes (2014). *Kommunalrett – Oppgaver, organisering og kontroll* s. 117-118
[9] Som definert i lov om behandlingen i forvaltningssaker (forvaltningsloven) § 1
[10] NOU 2016:4 *Ny kommunelov.* «Til § 25-1 Internkontroll i kommunen og fylkeskommunen»
[11] KS. *Internkontroll i kommunene.* [nettsted: https://www.ks.no/fagomrader/demokrati-og-styring/stat---kommune/internkontroll/ [hentet 21.08.2020]

fylkeskommuner og kommuner som ønsker å styrke den administrative internkontrollen.[12]

For offentlige virksomheter stilles det imidlertid også spesifikke krav til styring og kontroll (internkontroll) på informasjonssikkerhetsområdet, se Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15 som stiller krav om internkontroll på informasjonssikkerhetsområdet i all informasjonsbehandling som offentlige virksomheter har ansvaret for.

I henhold til eForvaltningsforskriften § 15 første ledd skal alle offentlige virksomheter etablere «mål og strategi for informasjonssikkerhet i virksomheten». Mål og strategi for informasjonssikkerhet inngår som grunnlaget for internkontrollen og er ledelsens viktigste redskap i styringen av informasjonssikkerheten innenfor forvaltningsorganets ansvarsområde.[13] KMD har i brev datert 12. mars 2014 utpekt Direktoratet for forvaltning og IKT (Difi), nå Digitaliseringsdirektoratet, til det organ som iht. eForvaltningsforskriften § 15 skal gi anbefalinger på området.[14] At Digitaliseringsdirektoratet skal gi anbefalinger på dette området er også gjentatt i «*Digitaliseringsrundskrivet*» for 2020.[15]

Internkontrollen på informasjonssikkerhetsområdet skal i henhold til eForvaltningsforskriften § 15 annet ledd være basert på anerkjente standarder for styringssystem for informasjonssikkerhet.

Referansekatalogen for IT-standarder i offentlig sektor er en oversikt over IT-standarder som er obligatoriske eller anbefalte for offentlig sektor.[16] En anbefalt standard skal benyttes med mindre man har gode grunner til å la være. Det er anbefalt å basere seg på den anerkjente standarden ISO/IEC 27001:2013 ved etablering av internkontroll på informasjonssikkerhetsområdet. Videre er det anbefalt å benytte Digitaliseringsdirektoratets veiledningsmateriell for internkontroll på informasjonssikkerhetsområdet, «*Internkontroll i praksis – Informasjonssikkerhet*» ved etablering og forbedring av internkontroll på informasjonssikkerhetsområdet.

Dette veiledningsmateriellet, heretter kalt Digitaliseringsdirektoratets interkontrollveileder, konkretiserer de mest sentrale delene av standarden ISO/IEC 27001:2013 og beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet. Veilederen understøtter også virksomhetsledelsens arbeid med helhetlig internkontroll, blant annet ved å hjelpe virksomheten til også å identifisere plikter etter annet regelverk (som for

---

[12] KS. *Orden i eget hus Kommunedirektørens internkontroll.* S. 9 https://www.ks.no/globalassets/fagomrader/lokaldemokrati/internkontroll/Kommunedirektorens-internkontroll-veileder-F41-web.pdf [hentet 21.08.2020]

[13] Kommunal- og moderniseringsdepartementet (2015). Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). S. [fotnote 89] https://www.regjeringen.no/contentassets/be9697d7e68041e29ffca576c331b4b0/efvf_del3.pdf

[14] Kommunal- og moderniseringsdepartementet (2014). *Styring og kontroll med informasjonssikkerhet.* Dokument saksnr: 2014/2232. Dokumentdato: 12.03.2014
«Departementet utpeker med dette Direktoratet for forvaltning og IKT til det organ som skal gi anbefalinger på området, jf. eForvaltningsforskriften § 15 annet ledd siste punktum».

[15] Kommunal- og moderniseringsdepartementet. *Digitaliseringsrundskrivet.* Nr: Rundskriv H-5/19. Referanse:
19/3313.[https://www.regjeringen.no/Kono/dokumenter/digitaliseringsrundskrivet/id2683652/]

[16] Se https://www.digdir.no/digitalisering-og-samordning/referansekatalogen-it-standarder/1480

eksempel personvernforordningen). Veilederen fungerer som beste praksis som alle kan tilpasse til egen virksomhet og benytte seg av.

For å vurdere arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, har Digitaliseringsdirektoratet i dette kunnskapsgrunnlaget vurdert observasjoner i datagrunnlaget opp mot anbefalingene i Digitaliseringsdirektoratets internkontrollveileder.

3 Observasjoner og vurderinger

I dette kunnskapsgrunnlaget har vi tatt utgangspunkt de sentrale aktivitetene som er beskrevet i Digitaliseringsdirektoratets internkontrollveileder. Disse sentrale aktivitetene er videre begrenset til det materialet som var tilgjengelig i datagrunnlaget for kunnskapsgrunnlaget. Aktivitetene er omtalt som hovedområder med undertemaer.

Hovedområder og undertemaer:

- Styring og kontroll (internkontroll)
    - Styrende dokumenter og lederforankring
    - Organisering
    - Rapportering til ledelsen
    - Oppfølging og kontinuerlig forbedring
    - Risikostyring
- Beredskap, øvelser og hendelseshåndtering
- Sikkerhetskultur og sikkerhetskompetanse

For hvert hovedområde beskriver vi observasjoner og vurderinger. Innledningen til hovedområdene henviser til Digitaliseringsdirektoratets internkontrollveileder og viser hvordan hvert hovedområde belyser arbeidet med informasjonssikkerhet i en virksomhet.

Observasjonene er direkte hentet fra datagrunnlaget. Vurderingene er Digitaliseringsdirektoratets faglige analyse av datagrunnlaget og er foretatt opp mot Digitaliseringsdirektoratets internkontrollveileder.

3.1 Styring og kontroll (internkontroll)

Internkontroll på informasjonssikkerhetsområdet i en virksomhet handler om å ha en systematisk tilnærming til arbeidet med informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. For å etablere en tilfredsstillende internkontroll på informasjonssikkerhetsområdet, bør man gjennomføre flere aktiviteter nærmere beskrevet i Digitaliseringsdirektoratets internkontrollveileder.[17]

Alle virksomheter bør ha en egeninteresse i et systematisk arbeid med informasjonssikkerhet.[18]

Lysneutvalget fant i 2015 at mange kommuner manglet et styringssystem på informasjonssikkerhetsområdet.[19] Utvalget fant også at «kommunene har i dag bare unntaksvis en tydelig sikkerhetsorganisasjon, og etterspør derfor i liten grad relevant

[17] https://internkontroll-infosikkerhet.difi.no/ledelsens-gjennomgang/hvorfor-internkontroll-pa-informasjonssikkerhetsomradet
[18] https://internkontroll-infosikkerhet.difi.no/regelverkskrav
[19] NOU 2015: 13. *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden* s. 246. [https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf]

kompetanse innen IKT-sikkerhet. Kommunene har stort sett små IKT-miljøer, der IKT-sikkerhetsarbeidet bare er én av mange oppgaver for IKT-personalet (…) Mange ledere har også for lav bevissthet om at de er ansvarlige for IKT-sikkerheten, og har verken vilje eller evne til å ivareta denne rollen.»[20]

NorSIS finner i sin rapport fra 2017 at det er store forskjeller i hvordan kommunene har organisert IKT-området, og at modenheten for informasjonssikkerhet i kommunal sektor er varierende.[21]

Styrende dokumenter og lederforankring

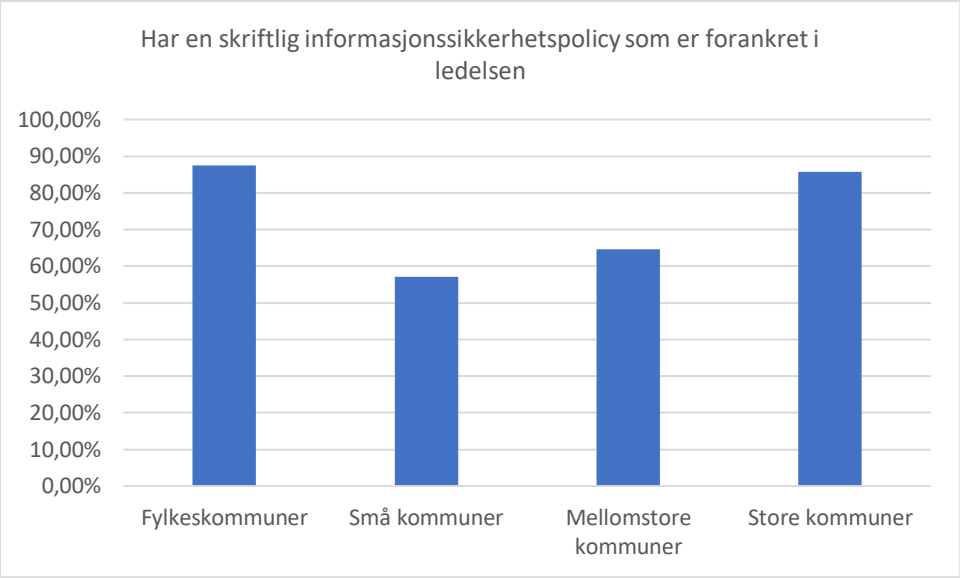
For å etablere en tilfredsstillende internkontroll på informasjonssikkerhetsområdet er det nødvendig å utarbeide styrende dokumenter. Styrende dokumenter bør gi føringer for arbeidet og klargjøre hvem som gjør hva i virksomheten. De styrende dokumentene bør videre gi en beskrivelse av blant annet ansvar, plikter og krav knyttet til informasjonssikkerhet og være overordnet i sin form. I henhold til Digitaliseringsdirektoratets internkontrollveileder er innholdet i de styrende dokumentene fundamentet i internkontrollen.[22]

I Digitaliseringsdirektoratets internkontrollveileder er det anbefalt at det blant annet utarbeides en policy for informasjonssikkerhet som en del av de overordnede styrende dokumentene. En slik policy bør inneholde mål og strategier for arbeidet med informasjonssikkerhet. Ledelsen må engasjere seg aktivt både ved utforming og godkjenning av policyen, det er også avgjørende at policyen følges opp og etterleves i praksis.[23]

Observasjoner
I SSBs tabell om «*Tiltak/rutiner ved administrasjon av IKT-sikkerheten»* for 2018, oppga

- **87,5 %** av fylkeskommunene at de hadde «*en skriftlig informasjonssikkerhetspolicy forankret i ledelse*n».
- Når det gjelder kommunene oppga **57,1 %** av de små kommunene, **64,6 %** av de mellomstore kommunene og **85,7 %** av de store kommunene det samme.

[20] Ibid. s. 224
[21] Norsk senter for informasjonssikring (2017). *Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)* s. 25 [https://norsis.no/wp-content/uploads/2018/05/Utredning-Kommune-CSIRT.pdf]
[22] https://internkontroll-infosikkerhet.difi.no/etableringsaktiviteter
[23] Ibid.



Figur 1: Tiltak/rutiner ved administrasjon av IKT-sikkerheten (prosent), etter forvaltningsnivå og størrelsesgruppering. Har en skriftlig informasjonssikkerhetspolicy som er forankret i ledelsen, 2018.[24]

I KS' kartlegging av digital modenhet i kommunesektoren fra 2018,[25] oppga

- **68 %** av fylkeskommunene og kommunene at «*samtlige av fylkeskommunens/kommunens virksomheter*» er «*omfattet av en strategi eller har en veileder for håndtering av informasjonssikkerhet*.» [26]

Vurderinger

Mange fylkeskommuner og kommuner oppgir at de har styrende dokumenter i en eller annen form. I undersøkelsene ble det ikke stilt spørsmål om dokumentene etterleves i praksis.

Observasjonene viser at 87,5 % av fylkeskommunene og 85,7 % av de store kommunene har en skriftlig informasjonssikkerhetspolicy forankret i ledelsen. Bare 57,1 % av de små kommunene og 64,6 % av de mellomstore kommunene har det samme.

Basert på observasjonene bør veiledning rettes mot små og mellomstore kommuner når det gjelder å dokumentere og forankre føringer knyttet til informasjonssikkerhetsarbeidet.

Organisering

Det overordnede ansvaret for å etablere tilstrekkelig internkontroll på informasjonssikkerhetsområdet ligger hos virksomhetsledelsen.[27] For å understøtte ledere på ulike nivåer bør det etableres støttefunksjoner i virksomheten.[28] Det er virksomhetsledelsens ansvar å etablere disse. Informasjonssikkerhetsarbeidet kan

[24] *Tabell 12041 fra SSB, prosenttall for små, mellomstore og store kommuner, se vedlegg A*
[25] KS (2018). *Oppdatert kunnskapsgrunnlag på digitaliseringsområdet. Kartlegging av digital modenhet i kommunesektoren*. [https://www.ks.no/contentassets/3f544fbe44c1404a8b81f7f98737509f/digital-modenhet.pdf]
[26] Ibid. s. 52
[27] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/ledelsens-styring-og-oppfolging
[28] https://internkontroll-infosikkerhet.difi.no/etableringsaktiviteter#Nokkelpersoner_sikkerhetsorganisasjonen

være organisert på mange ulike måter, som tidligere omtalt i kapittel 2.1. Hva som utgjør virksomhet og virksomhetsledelse må derfor tilpasses organiseringen i hver enkelt fylkeskommune og kommune.

En støttefunksjon kan for eksempel være en fagansvarlig informasjonssikkerhet, med hovedansvar å være pådriver og støtte til ledelsen og organisasjonen i informasjonssikkerhetsarbeidet. Fagansvarlig informasjonssikkerhet er en nøkkelressurs i virksomhetens kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet, blant annet ved å bistå i arbeidet med risikovurdering og -håndtering, og måling, evaluering og revisjon. Fagansvarlig informasjonssikkerhet har også ofte ansvaret for å planlegge og gjennomføre opplæring og bevisstgjøringsaktiviteter innen informasjonssikkerhet i virksomheten.[29]

Observasjoner
I SSBs tabell om «*Tiltak/rutiner ved administrasjon av IKT-sikkerheten»* for 2018, oppga

- **87,5 %** av fylkeskommunene at «*en formelt utnevnt person er fagansvarlig for informasjonssikkerheten*»
- Når det gjelder kommunene, oppga **57,6 %** av de små kommunene, **64,6 %** av de mellomstore kommunene og **80,4 %** av de store kommunene det samme.

KS' kartlegging av digital modenhet i kommunesektoren fra 2018,[30] viser at:

- **86%** av fylkeskommunene og kommunene at de organisert arbeidet med informasjonssikkerhet gjennom en form for rolle/sikkerhetsfunksjon med ansvar for informasjonssikkerhet.[31] Disse rollene varierer mellom å være en «*dedikert sikkerhetsfunksjon som rapporterer til rådmann*» (54 %), «*informasjonssikkerhetsfunksjon som rapporterer til IKT-ansvarlige*» (13 %), «*sikkerhetsfunksjon i hver enkelt virksomhet*» (10 %) og en «*tilfeldig utvalgt ressurs*» (9 %).

Vurderinger
Observasjonene fra SSB viser at 87,5 % av fylkeskommunene og 80,4 % av de store kommunene har formelt utnevnt en fagansvarlig for informasjonssikkerhet. Dette kan tyde på at både fylkeskommuner og store kommuner har organisert sitt informasjonssikkerhetsarbeid og ser betydningen av å etablere en form for fagansvarlig rolle innenfor informasjonssikkerhet.

Observasjonene fra SSB viser at bare 57,6 % og 64,6 % av henholdsvis de små og mellomstore kommunene har utnevnt en fagansvarlig for informasjonssikkerhet.

KS' kartlegging av digital modenhet viser at en stor andel av både fylkeskommuner og kommuner kan ha utpekt en form for rolle/sikkerhetsfunksjon med ansvar for informasjonssikkerhet.

---

[29] Direktoratet for forvaltning og IKT (2019) *Kompetansebeskrivelser – Ansvar, oppgaver og ønsket kompetanse for roller knyttet til styring og kontroll av informasjonssikkerhet Fagansvarlig informasjonssikkerhet* s. 5 [https://www.difi.no/sites/difino/files/kompetansebeskrivelser_0.pdf]
[30] KS (2018). *Oppdatert kunnskapsgrunnlag på digitaliseringsområdet. Kartlegging av digital modenhet i kommunesektoren*. [https://www.ks.no/contentassets/3f544fbe44c1404a8b81f7f98737509f/digital-modenhet.pdf]
[31] Ibid. S. 53 «Hvordan organiserer kommunen/fylkeskommunen arbeidet med informasjonssikkerhet?».

De lave prosenttallene for små og mellomstore kommuner kan bety at de organiserer informasjonssikkerhetsarbeidet på annen måte. I datagrunnlaget er det ikke stilt spørsmål om den nærmere organiseringen i fylkeskommuner og kommuner.

Observasjonene kan indikere at spesielt små og mellomstore kommuner trenger veiledning for å beskrive roller og ansvar for støttefunksjoner på informasjonssikkerhetsområdet.

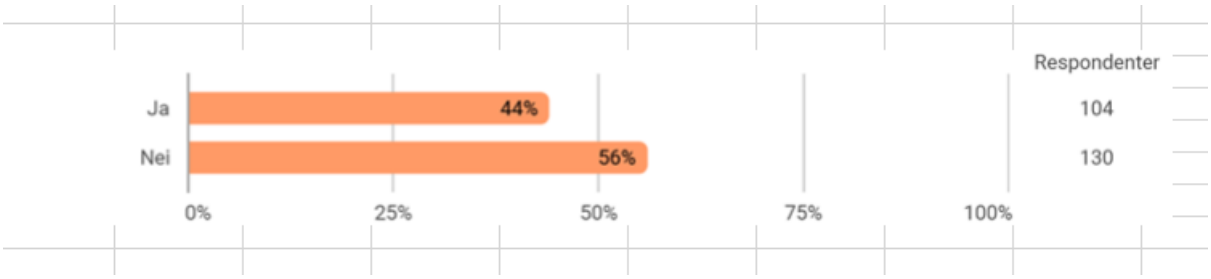
Rapportering til ledelsen

For å kunne nå virksomhetens mål er ledelsen avhengig av god internkontroll på informasjonssikkerhetsområdet. Ledelsen er derfor avhengig av en god oppfølging av aktiviteter knyttet til informasjonssikkerhet. Denne oppfølgingen bør skje jevnlig og ved behov. Hvordan og hvor ofte dette foregår er avhengig av hvordan informasjonssikkerhetsarbeidet er organisert.[32]

Observasjoner

Datagrunnlag for DSBs rapport «*IKT-sikkerhet på lokalt og regionalt nivå*» fra 2018, se vedlegg C, viser at:

- **44 %** av kommunene har «*informasjonssikkerhet som et fast punkt i kommuneledelsens styringsdialog i egen organisasjon*». Det finnes ikke tilsvarende tall for fylkeskommunene.



Figur 2: «Er informasjonssikkerhet et fast punkt i kommuneledelsens styringsdialog i egen organisasjon?», se vedlegg C.

Vurderinger

Observasjonene viser at 44 % av kommunene har informasjonssikkerhet som et fast punkt i styringsdialogen i egen organisasjon. At under halvparten av kommunene har dette kan tyde på at informasjonssikkerhet ikke har tilstrekkelig plass i styringsdialogen hos kommunene.

Viktigheten av at informasjonssikkerhet inngår som et fast punkt i styringsdialogen i egen organisasjon hos kommunene bør tydeliggjøres.

Oppfølging og kontinuerlig forbedring

Et viktig aspekt ved internkontrollarbeidet på informasjonssikkerhetsområdet er å følge opp arbeidet, legge til rette for forbedringer og gjøre endringer der det er nødvendig. Hendelseshåndtering og øvelser er viktige kilder til forbedringer, for eksempel til bruk i risikovurderinger. Formålet med hendelseshåndtering er å håndtere uønskede hendelser så effektivt som mulig, slik at man lettere kan unngå

[32] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/ledelsens-styring-og-oppfolging

informasjonssikkerhetsbrudd, redusere konsekvensene når slike brudd skjer og lære av tidligere erfaringer.[33]

Observasjoner
I SSBs tabell om «*Tiltak som del av internkontroll for informasjonssikkerhet*» for 2018-2020, oppga

- **87,5 % og 75 %** av fylkeskommunene i henholdsvis 2018 og 2019 at de hadde «*evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet*». Tall for fylkeskommunene fra 2020 finnes ikke.
- Når det gjelder kommunene, oppga **52,3 %**, **64,4 %**, og **61,2 %** at de har gjort tilsvarende i henholdsvis 2018, 2019 og 2020.

I samme tabell oppga også

- **68,8 % og 75 %** av fylkeskommunene i henholdsvis 2018 og 2019 at de hadde «*rapportert erfaringer fra håndtering av uønskede hendelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten*». Tall for fylkeskommunene fra 2020 finnes ikke.
- Når det gjelder kommunene, oppga **49,6 %**, **53,6 %** og **54,8 %** at de har gjort tilsvarende i henholdsvis 2018, 2019 og 2020.

I samme tabell oppga også

- **37,5 % og 31,3 %** av fylkeskommunene i henholdsvis 2018 og 2019 at de hadde «*rapportert erfaringer fra øvelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten*». Tall for fylkeskommunene fra 2020 finnes ikke.
- Når det gjelder kommunene, oppga **22,5 %**, **26,8 %** og **25,8 %** at de har gjort tilsvarende i henholdsvis 2018, 2019 og 2020.

Vurderinger
Observasjonene viser at over 75 % av fylkeskommunene i tidsperioden 2018-2019 svarte at de har evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet. Under 65 % av kommunene svarer tilsvarende i tidsperioden 2018-2020. Dette kan tyde på at fylkeskommuner har bedre rutiner for dette enn kommuner. Det er likevel viktig å påpeke at tallene viser variasjon fra år til år, noe som kan tyde på manglende systematikk knyttet til dette.

Observasjonene viser videre at under 75 % av fylkeskommune i tidsperioden 2018-2019 svarte at de rapporterte erfaringer fra håndtering av uønskede hendelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten. Under 55 % av kommunene har gjort tilsvarende i tidsperioden 2018-2020. Dette kan tyde på at fylkeskommuner har bedre rutiner enn kommuner også på dette området.

Observasjonene viser videre at under 40 % av fylkeskommunene svarte at de rapporterte erfaringer fra øvelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten i tidsperioden 2018 - 2019. Under 30 % av kommunene har gjort tilsvarende i tidsperioden 2018-2020. Dette kan indikere at fylkeskommuner og kommuner i liten grad rapporterer erfaringer fra øvelser til bruk i risikovurderinger

[33] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/overvaking-og-hendelseshandtering#Rapportere%20hendelser%20avvik%20og%20informasjonssikkerhetsbrudd

og/eller forbedring av informasjonssikkerheten. Observasjonene knyttet til hovedområdet «Beredskap, øvelser og hendelseshåndtering» viser også at fylkeskommuner og kommuner i liten grad gjennomfører øvelser på informasjonssikkerhetsområdet.

Viktigheten av oppfølging og kontinuerlig forbedring av informasjonssikkerhetsarbeidet bør tydeliggjøres for fylkeskommuner og kommuner.

Risikostyring

Systematiske aktiviteter for å vurdere og håndtere risiko er sentralt i internkontrollarbeidet på informasjonssikkerhetsområdet.[34] Dagens regelverk blir stadig mer risikobasert slik at systematiske risikovurderinger og risikohåndtering blir viktigere.

Ledere på alle nivå skal sikre at virksomheten når sine samlede mål.[35] Dette forutsetter at ledere har tilstrekkelig kontroll på risikoene knyttet til mål og arbeidsoppgaver – inkludert informasjonssikkerhetsrisiko.

Virksomheten må ha tilstrekkelig oversikt og kunne jevnlig vurdere og prioritere hvor det er behov for grundig vurdering av risiko. De ansvarlige bør periodisk foreta en gjennomgang for å se om de vurderingene som er gjort tidligere og sikkerhetstiltakene som er innført fortsatt er hensiktsmessige.[36]

Som følge av risikovurderingen må det bestemmes hvilke risikoer som kan aksepteres, og hvilke som krever håndtering. Eventuell aksept av risiko må tas på riktig nivå i virksomheten. Risikohåndtering innebærer vurdering av ulike sikkerhetstiltak. Dette kan medføre at nye tiltak etableres, noen forbedres og noen eventuelt fjernes.[37]

Observasjoner

I SSBs tabell om «*Tiltak/rutiner ved administrasjon av IKT-sikkerheten»* fra 2018, oppga

- **68,8 %** av fylkeskommunene at «*risikovurderinger gjennomføres systematisk og periodisk*».
- Når det gjelder kommunene oppga **33 %** av de små kommunene, **47,7 %** av de mellomstore kommunene og **58,9 %** av de store kommunene det samme.

I samme tabell oppga også

- **87,5 %** av fylkeskommunene at «*ved nye risikovurderinger iverksettes nødvendig risikohåndtering*».
- Når det gjelder kommunene, oppga **58,6 %** av de små kommunene, **73,1 %** av de mellomstore kommunene og **85,7 %** av de store kommunene det samme.

DSB-rapporten «*IKT-sikkerhet på lokalt og regionalt nivå»* fra 2018 viser at:

[34] Direktoratet for forvaltning og IKT (2018). *Arbeidet med informasjonssikkerhet i statsforvaltningen – Kunnskapsgrunnlag* s. 22 [https://www.difi.no/sites/difino/files/difi-rapport_2018_4_arbeidet_med_informasjonssikkerhet_i_statsforvaltningen_kunnskapsgrunnlag.pdf]
[35] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/ledelsens-styring-og-oppfolging
[36] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/risikovurdering
[37] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/risikohandtering

- **62** % av kommunene sa at de gjennomfører «*rutinemessig risiko- og sårbarhetsanalyser av sine IKT-systemer*». Imidlertid var det flere av kommunene som rapporterte at de ikke hadde gjennomført analyser siste året.[38] Rapporten har ikke tilsvarende tall for fylkeskommuner.

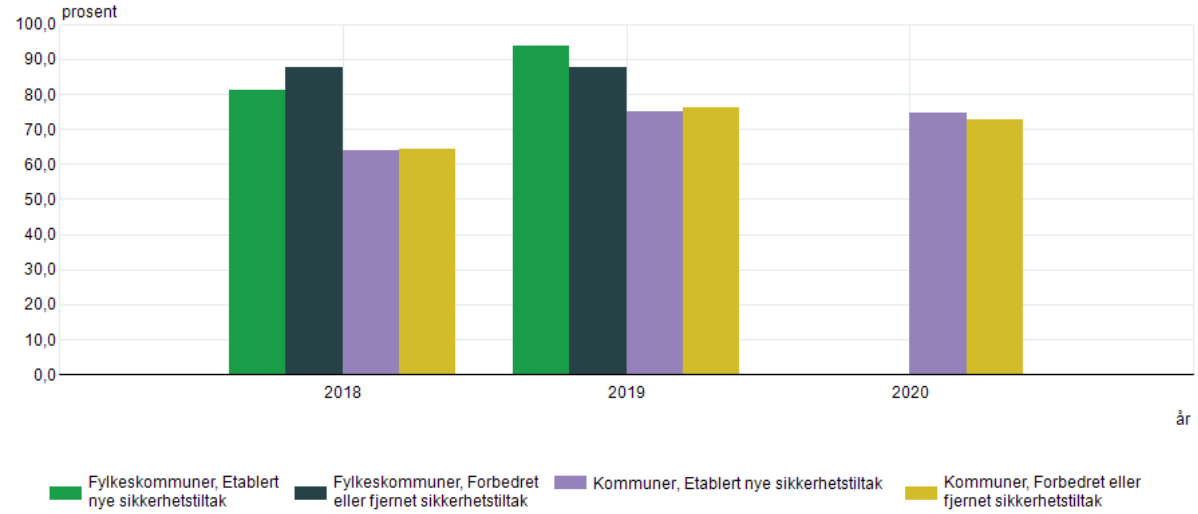
I SSBs tabell om «*Tiltak som del av internkontroll for informasjonssikkerhet*» for 2018-2020, oppga

- **81,3 %** og **93,8 %** av fylkeskommunene i henholdsvis 2018 og 2019 at de hadde «*etablert nye sikkerhetstiltak*». Tall for fylkeskommunene fra 2020 finnes ikke.
- Når det gjelder kommunene oppga **63,9 %**, **75,2 %** og **74,5 %** at de har gjort tilsvarende i henholdsvis 2018, 2019 og 2020.

I samme tabell oppga også

- **87,5 %** og **87,5 %** av fylkeskommunene i henholdsvis 2018 og 2019at de hadde «*forbedret eller fjernet sikkerhetstiltak*». Tall for fylkeskommunene fra 2020 finnes ikke.
- Når det gjelder kommunene oppga **64,2 %**, **76,2 %** og **72,9 %** at de har gjort tilsvarende i henholdsvis 2018, 2019 og 2020.

12042: Tiltak som del av internkontroll for informasjonssikkerhet (prosent), etter forvaltningsnivå, statistikkvariabel og år.



Kilde: Statistisk sentralbyrå

Figur 3: SSB tabell 12042: Tiltak som del av internkontroll for informasjonssikkerhet (prosent), etter forvaltningsnivå, statistikkvariabel «etablert nye sikkerhetstiltak» og «forbedret eller fjernet sikkerhetstiltak» og år (2018, 2019 og 2020).

Når det gjelder risikostyring knyttet til behandling av personopplysninger, har også Datatilsynet i flere saker fra 2019 vedtatt overtredelsesgebyr for brudd på

[38] Direktoratet for samfunnssikkerhet og beredskap (2018). *IKT-sikkerhet på lokalt og regionalt nivå* s. 4 [Intern rapport]

personvernforordningens krav til behandlingssikkerhet i artikkel 32. I to av vedtakene sanksjonerte Datatilsynet for brudd på ikke å ha gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.[39] I et annet vedtak ble kommunen klaget inn for brudd på sentrale plikter for informasjonssikkerhet knyttet til personopplysninger, herunder manglende risikovurderinger og vurdering av personvernkonsekvenser.[40]

Vurderinger

Observasjonene viser at 68,8 % av fylkeskommunene gjennomfører risikovurderinger systematisk og periodisk. Tall for kommunene viser at 58,9 % av de store kommunene, 47,7 % av de mellomstore kommunene og 33 % av de små kommunene gjør det samme. Dette indikerer at det er de mellomstore og spesielt de små kommunene som i særlig liten grad gjennomfører risikovurderinger systematisk og periodisk.

Observasjonene viser videre at 87,5 % av fylkeskommunene iverksetter nødvendig risikohåndtering ved nye risikovurderinger. Tall for kommunene viser at 85,7 % av de store kommunene, 73,1 % av de mellomstore kommunene og 58,6 % av de små kommunene iverksetter nødvendig risikohåndtering ved nye risikovurderinger. Dette indikerer at de store kommunene er på høyde med fylkeskommunene på dette området.

Fylkeskommunene er bedre enn kommunene på etablering, forbedring eller fjerning av sikkerhetstiltak. Tall for fylkeskommunene finnes imidlertid ikke for 2020. For både fylkeskommuner og kommuner er tallene over 70 % ved måling i 2019. Det bør trekkes fram at for kommunene viser tallene en forbedring fra 2018 til 2019, men en liten nedgang fra 2019 til 2020.

Vurderinger Datatilsynet har gjort viser at noen større kommuner ikke har tilstrekkelige tekniske og organisatoriske tiltak som sørger for tilfredsstillende informasjonssikkerhet om personopplysninger. I enkelttilfeller har kommunen heller ikke hatt nok kompetanse rundt gjennomføringen av risikovurderinger. Dette indikerer at også blant store kommuner kan det i enkelttilfeller være utfordringer med risikostyring.

Veiledning knyttet til kompetanseheving på risikovurdering og risikohåndtering bør spesielt rettes mot små og mellomstore kommuner.

3.2 Beredskap, øvelser og hendelseshåndtering

Norske virksomheter har blitt mer sikkerhetsbevisst, de identifiserer mange tiltak og iverksetter dem raskere enn før.[41] Til tross for dette må virksomheter være forberedt på at sikkerhetshendelser og sikkerhetsbrudd vil inntreffe. God planlegging og

---

[39] *Vedtak om pålegg og overtredelsesgebyr – Bergen kommune, 18.03.2019* og *Varsel om overtredelsesgebyr – Melding om avvik i Oslo kommune Sykehjemsetaten - Oslo kommune Sykehjemsetaten, 11.10.2019.*

[40] *Vedtak om pålegg – Arendal kommune – Behandling av personopplysninger i kartleggingsverktøyet Spekter,* 23.10.2019

[41] Nasjonal Sikkerhetsmyndighet (2019). *Helhetlig digitalt risikobilde 2019* s. 5 [https://nsm.no/getfile.php/133669-1592830841/Demo/Dokumenter/Rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf]

regelmessig gjennomføring av øvelser bidrar til at uønskede hendelser kan håndteres på en bedre måte.

Digitaliseringsdirektoratet anbefaler at virksomheter gjennomfører minst en årlig øvelse innen informasjonssikkerhet.[42]

NorSIS utredet i 2017 de felles behovene for støtte til håndtering av IKT-sikkerhetshendelser i kommunene. Rapporten oppsummerer at «kommunal sektor har behov for støtte til håndtering av hendelser, etablering av et felles situasjonsbilde, støtte til analyser av digitale elementer, støtte til opplæring og kompetanseheving og støtte til veiledning, rådgiving og revisjon.»[43]

Observasjoner
I SSBs «*Tabell om tiltak/rutiner ved administrasjon av IKT-sikkerheten»* fra 2018, oppga

- **25 %** av fylkeskommunene at «*beredskapsøvelse gjennomføres minst en gang per år*».
- Når det gjelder kommunene, oppga **12,6 %** av de små kommunene, **9,2 %** av de mellomstore kommunene og **21,4 %** av de store kommunene det samme.

DSB-rapporten «*IKT-sikkerhet på lokalt og regionalt nivå»* fra 2018 og datagrunnlag for denne, se vedlegg C, viser at:

- **84 %** av kommunene har svart at det finnes *«dedikerte personer eller grupper i kommunen eller dens samarbeidspartnere som har ansvaret for varsler om sårbarheter/trusler samt sikkerhetshendelser knyttet til IKT».* [44]
- **82 %** av kommunene har «*etablert et system/rutiner for håndtering av varsler om sårbarheter/trusler og sikkerhetshendelser mot sine IKT-systemer*». Rapporten sier at de færreste har kommentert undersøkelsen på en måte som viser at både systemer og rutiner er på plass.[45]

Vurderinger
Observasjonene viser at bare 25 % av fylkeskommune gjennomfører en beredskapsøvelse på IKT sikkerhetsområdet minst en gang per år. Bare 12,6 % av de små kommunene, 9,2 % av de mellomstore kommunene og 21,4 % av de store kommunene gjør det samme.

At under 25 % av både fylkeskommuner og kommuner gjennomfører beredskapsøvelser knyttet til informasjonssikkerhet, indikerer at øvelser ikke gjennomføres i tilstrekkelig grad. Dette indikerer at både fylkeskommuner og kommuner i stor grad trenger hjelp til å komme i gang med å gjennomføre jevnlige øvelser knyttet til informasjonssikkerhet.

---

[42] Direktoratet for forvaltning og IKT (2018). *Arbeidet med informasjonssikkerhet i statsforvaltningen – Kunnskapsgrunnlag* s. 30 [https://www.difi.no/sites/difino/files/difi-rapport_2018_4_arbeidet_med_informasjonssikkerhet_i_statsforvaltningen_kunnskapsgrunnlag.pdf]
[43] Norsk senter for informasjonssikring (2017). *Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)* s. 6 [https://norsis.no/wp-content/uploads/2018/05/Utredning-Kommune-CSIRT.pdf]
[44] Direktoratet for samfunnssikkerhet og beredskap (2018). *IKT-sikkerhet på lokalt og regionalt nivå* (2018) s. 5 [intern rapport]
[45] Direktoratet for samfunnssikkerhet og beredskap (2018). *IKT-sikkerhet på lokalt og regionalt nivå* (2018) s.4 [intern rapport]

Grunnlagsdata fra DSB, se vedlegg C, viser videre at over 80 % av kommunene har etablert et system/rutiner for håndtering av varsler om sårbarheter/trusler og sikkerhetshendelser mot sine IKT-systemer. Rapporten sier imidlertid at «de færreste har kommentert på en måte som viser at både systemer og rutiner er på plass. De fleste svarene fokuserer på varsling etter hendelser og ikke på håndtering av varsler om sårbarheter og trusler».[46]

Veiledning i beredskapsøvelser knyttet til informasjonssikkerhet bør rettes mot både fylkeskommuner og kommuner.

3.3 Sikkerhetskultur og sikkerhetskompetanse

Sikkerhetskultur og sikkerhetskompetanse er en avgjørende del av internkontroll på informasjonssikkerhetsområdet. Kompetanse er de samlede kunnskaper, ferdigheter, evner og holdninger som gjør det mulig å utføre aktuelle oppgaver i henhold til definerte krav og mål.[47] Sikkerhetskulturen regnes som en del av organisasjonskulturen, og handler om hvilke felles verdier og normer som ligger til grunn i virksomheten, blant annet for risikoforståelse.[48]

Et viktig grunnlag for internkontrollen på informasjonssikkerhetsområdet er at de ansatte på alle nivåer har nødvendig kompetanse, er bevisst på hvorfor informasjonssikkerhet er viktig og har tilstrekkelige ferdigheter til å utføre arbeidet sitt i tråd med denne kompetansen. Justis- og beredskapsdepartementet (JD) har i samarbeid med Kunnskapsdepartementet (KD) utarbeidet «*Nasjonal strategi for digital sikkerhetskompetanse»* som grunnlag for å utvikle kompetanse i tråd med samfunnets, arbeidslivets og den enkeltes behov.[49]

Virksomheten bør ha en kontinuerlig prosess for å sikre tilstrekkelig kompetanse- og kulturutvikling. Identifisering av behovet for slik kompetanse- og kulturutvikling bør derfor gjøres løpende som en del av internkontrollen på informasjonssikkerhetsområdet.[50]

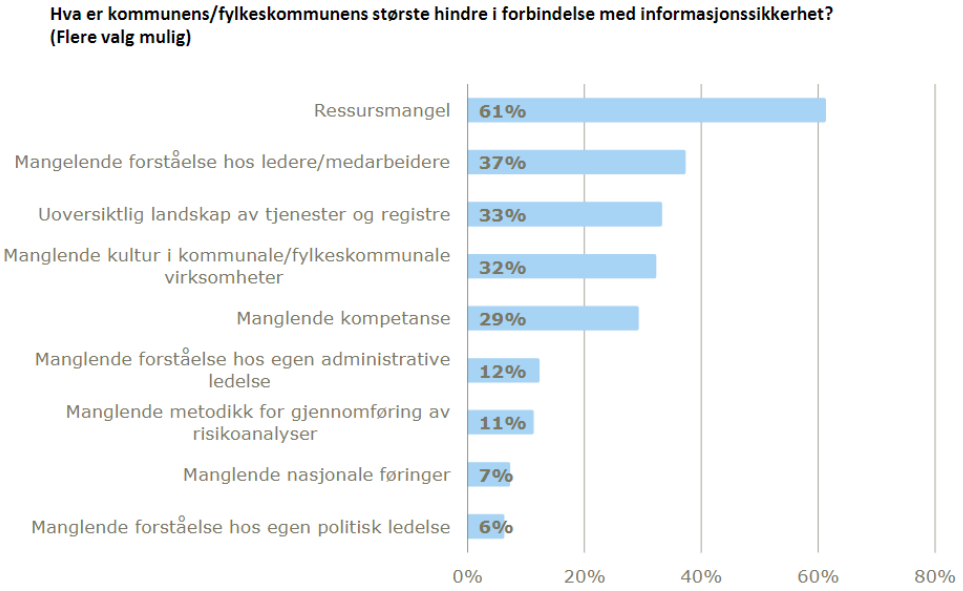
Observasjoner
I SSBs tabell om «*Tiltak/rutiner ved administrasjon av IKT-sikkerheten»* fra 2018, oppga

- **68,8 %** av fylkeskommunene i 2018 at de gjennomfører «*aktiviteter for opplæring og bevisstgjøring av ansatte og ledere minst én gang per år*».
- Når det gjelder kommunene, oppgir **34 %** av de små kommunene, **46,9 %** av de mellomstore kommunene og **64,3 %** av de store kommunene det samme.

I KS' kartlegging av digital modenhet fra 2018, på spørsmål om hva som er «*kommunens/fylkeskommunens største hindre i forbindelse med informasjonssikkerhet*», oppga

[46] Ibid. s. 4
[47] Lai, Linda. *Strategisk Kompetanseledelse* (3. utg), (2013). Oslo: Fagbokforlaget [ISBN: 9788245014471]
[48] Direktoratet for forvaltning og IKT (2018). *Arbeidet med informasjonssikkerhet i statsforvaltningen – Kunnskapsgrunnlag* s. 34 [https://www.difi.no/sites/difino/files/difi-rapport_2018_4_arbeidet_med_informasjonssikkerhet_i_statsforvaltningen_kunnskapsgrunnlag.pdf]
[49] https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/
[50] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/kompetanse-og-kulturutvikling

- **29 %** at dette er «*manglende kompetanse*», **37 %** at dette er «*manglende forståelse hos ledere/medarbeidere*», **12 %** at dette er «*manglende forståelse hos egen administrative ledelse*» og **32 %** at dette er «*manglende kultur i kommunale/fylkeskommunale virksomheter*».[51]



Figur 4: KS' kartlegging av digital modenhet. Hva er kommunens/fylkeskommunens største hindre i forbindelse med informasjonssikkerhet? 2018.

Vurderinger

68,8 % av fylkeskommuner og 64,3 % av store kommuner gjennomfører kompetansehevende aktiviteter minst én gang hvert år. Videre svarer 46,9 % av de mellomstore kommunene og 34 % av de små kommunene at de gjør det samme. Dette indikerer at spesielt små og mellomstore kommuner trenger hjelp til kompetansehevende aktiviteter.

Videre viser KS' kartlegging at blant annet manglende kompetanse og forståelse hos både medarbeidere og leder, samt manglende kultur utgjør hindringer i forbindelse med informasjonssikkerhet.

Dette indikerer at både fylkeskommuner og kommuner trenger hjelp til kompetanseutvikling og å arbeide med sikkerhetskultur. Dette støttes også opp av både Holteutvalget som refererer til manglende kompetanse på IKT-området generelt[52], og Lysneutvalget om manglende kompetanse på sikkerhetsområdet spesielt[53].

---

[51] KS (2018). *Oppdatert kunnskapsgrunnlag på digitaliseringsområdet. Kartlegging av digital modenhet i kommunesektoren*. s. 57 [https://www.ks.no/contentassets/3f544fbe44c1404a8b81f7f98737509f/digital-modenhet.pdf]

[52] NOU 2018:14. *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.* s. 47 [https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf.

[53] NOU 2015: 13. *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* s. 224 og s 246 [https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

Veiledning i hvordan man identifiserer behov for kompetanse- og kulturutvikling bør rettes mot både fylkeskommuner og kommuner, spesielt små og mellomstore kommuner.

4 Anbefalinger

Observasjoner og vurderinger i kapittel 3 tyder på at fylkeskommuner og kommuner trenger mer veiledning på informasjonssikkerhetsområdet. Basert på dette har Digitaliseringsdirektoratet tre anbefalinger med underanbefalinger.

Anbefalinger: Styring og kontroll (internkontroll)

Anbefaling 1: Veiledning knyttet til hvordan virksomhetene kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet, bør spesielt rettes mot små og mellomstore kommuner.

Underanbefalinger:

1.1 Veiledning for å dokumentere og forankre føringer knyttet til informasjonssikkerhetsarbeidet bør rettes mot små og mellomstore kommuner.

1.2 Viktigheten av å beskrive roller og ansvar for informasjonssikkerhetsarbeidet bør tydeliggjøres for små og mellomstore kommuner.

1.3 Viktigheten av at Informasjonssikkerhet inngår som et fast punkt i styringsdialogen i egen organisasjon hos kommunene bør tydeliggjøres.

1.4 Viktigheten av oppfølging og kontinuerlig forbedring av informasjonssikkerhetsarbeidet bør tydeliggjøres for fylkeskommuner og kommuner.

1.5 Veiledning knyttet til kompetanseheving på risikovurdering og risikohåndtering bør spesielt rettes mot små og mellomstore kommuner.

Anbefalinger: Gjennomføring av beredskap, øvelser og hendelseshåndtering

Anbefaling 2: Veiledning i øvelser knyttet til informasjonssikkerhet bør rettes mot både fylkeskommuner og kommuner.

Anbefalinger: Sikkerhetskultur og sikkerhetskompetanse

Anbefaling 3: Veiledning i hvordan man identifiserer behov for kompetanse- og kulturutvikling bør rettes mot både fylkeskommuner og kommuner, spesielt mot små og mellomstore kommuner.

5 Videre arbeid

5.1 Tiltak

Videre arbeid bør basere seg på eksisterende veiledningsmateriell i så stor grad som mulig. Her vises det til flere eksisterende og planlagte tiltak i KS, KiNS, DSB og Digitaliseringsdirektoratet, som vil være egnet til å følge opp anbefalingene i dette kunnskapsgrunnlaget.

KS: «Verktøykasse» for toppledelsen (FOU1)[54]
KS er i gang med et arbeid (FOU1) som retter seg mot toppledelsen i fylkeskommuner og kommuner. Arbeidet skal bidra til at toppledelsen får en «verktøykasse» som de kan bruke for å oppnå tilstrekkelig kontroll på informasjonssikkerhet- og personvernområdet. Arbeidet er spesielt rettet mot små og mellomstore kommuner og er forventet ferdigstilt Q4 2020.

Imøtekommer anbefaling 1.

KS: Risikovurderinger og personvernkonsekvensvurderinger i skolesektoren (SkoleSEC)[55]
KS har også et pågående arbeid rettet mot skolesektoren spesielt, SkoleSEC, som blant annet skal støtte kommunene i å gjennomføre risikovurderinger og personvernkonsekvensutredninger for bruk av digitale tjenester.

Imøtekommer anbefaling 1.

KiNS: Implementering av ledelsessystem og personvern i kommunene[56]
KiNS arbeider med å lette arbeidet med implementering og gjennomføring av ledelsessystem for informasjonssikkerhet (LSIS) og personvern i kommunene. KiNS legger opp til god involvering av kommunene i arbeidet, herunder bruk av nettverksmøter.

Imøtekommer anbefaling 1.

DSB: Øvelser[57]
DSB utvikler øvingspakker til bruk i både offentlige og private virksomheter. Øvelsene utvikles som diskusjonsøvelser, og det gis en enkel veileder for evaluering av egne øvelser.

Imøtekommer anbefaling 2.

Digitaliseringsdirektoratet: Nettverk for veiledningsaktører
Effekten av veiledningsarbeidet mot kommunene blir mest effektivt om veiledningsaktørene på området er koordinert og samkjørt. Nettverk for veiledningsaktører innen styring og kontroll på informasjonssikkerhetsområdet ble reetablert av Digitaliseringsdirektoratet våren 2020. Nettverket skal bidra til et bedre

[54] Se detaljer i Vedlegg F
[55] Se detaljer i Vedlegg F
[56] Se detaljer i Vedlegg E
[57] Se detaljer i Vedlegg D

og mer helthetlig veiledningstilbud til offentlig sektor. DSB, KiNS, KS og NorSIS har takket ja til å bli med i nettverket.

Imøtekommer alle anbefalingene ved å sørge for koordinering mellom veiledningsaktørene.

Digitaliseringsdirektoratet: Veiledning i sikkerhetskultur og sikkerhetskompetanse
Digitaliseringsdirektoratets oppfølging av Difi-rapport 2018:4 «*Arbeidet med informasjonssikkerhet i statsforvaltningen – Kunnskapsgrunnlag*»[58] adresserer arbeidet med sikkerhetskultur på informasjonssikkerhetsområdet i statlige virksomheter. Det blir i denne anledning utarbeidet nytt veiledningsmateriell sammen med NorSIS. Dette veiledningsmateriellet henvender seg til offentlig forvaltning og vil kunne bidra til å bedre fylkeskommuners og kommuners arbeid med sikkerhetskultur.

Imøtekommer anbefaling 3.

5.2 Veien videre

Det anbefales at vurderingene og tiltakene tas med inn i samtaler med kommunene for å nyanseres og utfylles. Det er naturlig at vurderinger og tiltak diskuteres for eksempel i KommIT-rådet sammen med KS og kommunenes representanter der.

I tillegg til de tiltakene som er beskrevet over har Digitaliseringsdirektoratet en rekke veiledningstiltak gjennom sitt ordinære arbeid. Dette inkluderer blant annet «Nettverk for informasjonssikkerhet», veiledning i internkontroll, kurs for toppledelsen og annen kurs- og foredragsvirksomhet. Disse tiltakene vil også kunne rettes mot kommunesektoren der det er hensiktsmessig.

Formidling av Digitaliseringsdirektoratets veiledningsmateriell til fylkeskommuner og kommuner vil, sammen med tiltakene over, bidra til å bedre tilstanden på arbeidet med informasjonssikkerhet i kommunal sektor. Ved å opprettholde god kontakt med veiledningsaktørene og følge utviklingen av tiltakene vil Digitaliseringsdirektoratet få et godt grunnlag for å få innsikt i kommunesektorens behov og eventuelt utvikle og forbedre vårt eget veiledningsmateriell rettet mot kommunal sektor.

Etter gjennomføring av disse tiltakene bør det vurderes om anbefalingene er dekket opp i sin helhet eller om det er behov for ytterligere tiltak.

For å sikre god kontakt med veiledningsaktørene og harmoni mellom veiledningsmateriell er alle aktørene som er beskrevet over invitert inn i «Nettverk for veiledningsaktører».

[58] https://www.difi.no/sites/difino/files/difi-rapport_2018_4_arbeidet_med_informasjonssikkerhet_i_statsforvaltningen_kunnskapsgrunnlag.pdf

6 Vedlegg A: Tabell 12041 fra SSB, prosenttall for små, mellomstore og store kommuner

SSB har for dette kunnskapsgrunnlaget regnet ut prosenttall for en tredelt størrelsesgruppering fra tabell 12041.:

Tabell 12041: Tiltak/rutiner ved administrasjon av IKT-sikkerheten. 2018. Prosent

		Har en skriftlig informasjonssikkerhetspolicy som er forankret i ledelsen	En formelt utnevnt person er fagansvarlig for informasjonssikkerheten	Risikovurderinger gjennomføres systematisk og periodisk	Ved nye risikovurderinger iverksettes nødvendig risikovurdering	Beredskapsøvelse gjennomføres minst en gang per år	Aktiviteter for opplæring og bevisstgjøring av ansatte og ledere gjennomføres minst én gang per år
	ant	prst	prst	prst	prst	prst	prst
All	377	63,9	63,4	41,9	67,6	12,7	43
0-4999 innbyggere	191	57,1	57,6	33	58,6	12,6	34
5000-19999 innbyggere	130	64,6	64,6	47,7	73,1	9,2	46,9
Minst 20000 innbyggere	56	85,7	80,4	58,9	85,7	21,4	64,3

7 Vedlegg B: Tabell 12041 og 12042 fra SSB, antall respondenter

Antall respondenter for henholdsvis 2018, 2019 og 2020:

Antall innbyggere	2018 Kommuner	2018 Fylkes-kommuner	2019*) Kommuner	2019*) Fylkes-kommuner	2020*) Kommuner	2020*) Fylkes-kommuner
0-4999	191	-	206	-	160	-
5000-19999	130	-	135	-	109	-
> 20000	56	-	58	-	56	-
Totalt	**377**	**16**	**399**	**16**	**325**	**8**

*) Gjelder kun tabell 12042 da tabell 12041 kun har tall fra 2018

Ved utgangen av 2016 var det 427 kommuner i Norge, fra 1. januar 2020 er det 356 kommuner.[59]

Ved utgangen av 2019 var det 18 fylkeskommuner i Norge, fra 1. januar 2020 er det 11 fylkeskommuner.[60]

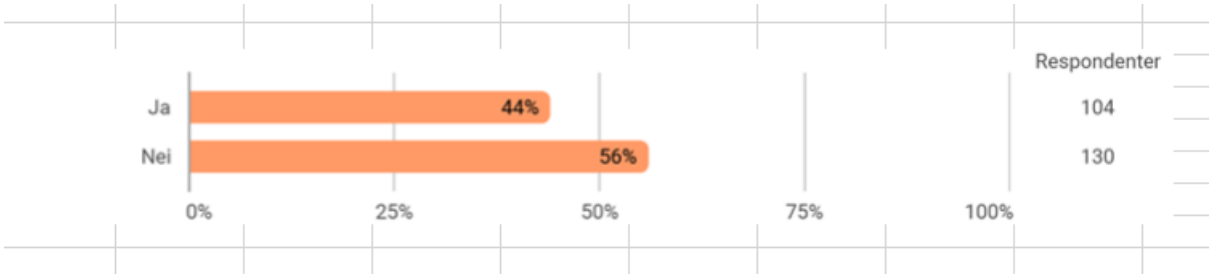
[59] https://www.ks.no/fagomrader/demokrati-og-styring/kommunereform/noen-fakta-om-nye-kommuner-fra-2020/

[60] https://www.ks.no/fagomrader/demokrati-og-styring/regionreform/noen-fakta-om-norges-fylker-fra-2020/

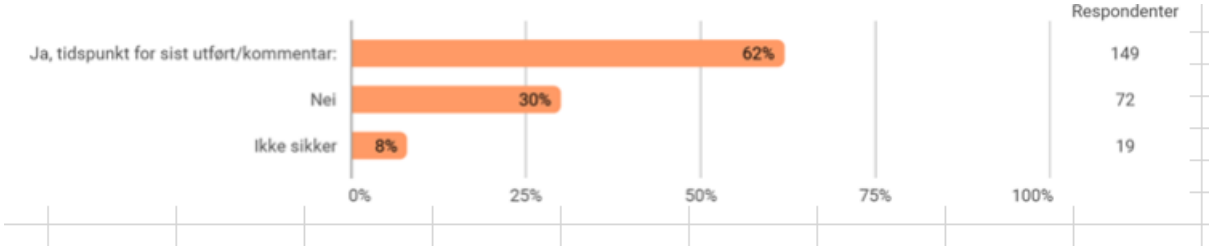
8 Vedlegg C: Utvalgte grunnlagsdata for rapport «IKT-sikkerhet på lokalt og regionalt nivå»

Utvalgte grunnlagsdata for rapport «IKT-sikkerhet på lokalt og regionalt nivå», 2018, Direktoratet for samfunnssikkerhet og beredskap (DSB):

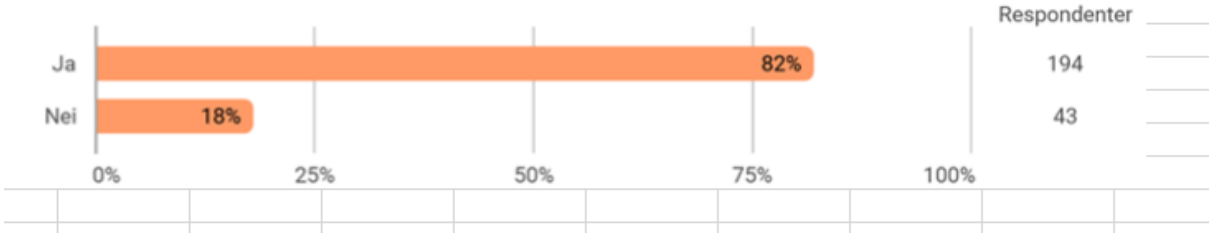
Er informasjonssikkerhet et fast punkt i kommuneledelsens styringsdialog i egen organisasjon?



Gjør kommunen rutinemessig risiko- og sårbarhetsanalyser av sine IKT-systemer?



Har kommunen etablert et system/rutiner for håndtering av varsler om sårbarheter/trusler og sikkerhetshendelser mot sine IKT-systemer?



9 Vedlegg D: Pågående og planlagte tiltak i regi av Direktoratet for samfunnssikkerhet og beredskap (DSB)

Historikk
I oppfølging av Difi-rapport 2018:4 *«Arbeidet med informasjonssikkerhet i statsforvaltningen»* ble det definert fem prioriterte områder; etatsstyring, sikkerhetskultur, kompetanse, øvelser og risiko. En del av oppdraget under delprosjekt øvelser er å utvikle fire øvingspakker til bruk i både offentlige og private virksomheter (prosjektgruppen har utvidet med noen flere scenarioer). Ved utvikling av øvelse Digital 2020 (i regi av DSB) er det et tilsvarende delprosjekt, hvor hensikten er å gi øvingsmulighet for de virksomhetene som ikke får anledning til å delta i Digital 2020. Styringsgruppen/prosjektledelse fant det hensiktsmessig å slå disse to prosjektene sammen, hvilket er gjort med hell. DSB, Digitaliseringsdirektoratet, NSM, NorSIS, NTNU/CyberRange er deltakere i prosjektet.

Øvingskonsept
Øvelsene utvikles som diskusjonsøvelser, med læringsspørsmål underveis. Det er ikke lagt opp til noen form for tilbakemelding fra øvet virksomhet, men det gis en enkel veileder for hvordan å egenevaluere egen øvelse.

Tema for de utviklede scenarioene er:

- Insidere - vitende og uvitende
- Direktør/leder svindel
- Kompromitterte servere
- Sårbarhetsvarsling
- Personopplysninger på avveie
- Hjemmekontor
- Bevissthet rundt egen teknologi på reise/privat
- Samfunnskritiske funksjoner ute av spill - strøm slåes ut
- Samfunnskritiske systemer ute av spill - nettbanker og betalingsterminaler svikter

Målgrupper
Prosjektet ønsker å treffe bredt, og scenarioene er utviklet på en slik måte at de skal kunne treffe både offentlige og private virksomheter.

Plattform
Det utvikles en nettbasert plattform med en sikret pålogging. Løsningen er todelt; en del for øvingsleder og en for de øvede. Det er lagt betydelig vekt på at løsningen skal ha en lav brukerterskel. Plattformen skal kunne utvides til å håndtere fremtidige øvingskonsepter – også innenfor andre fagområder (f.eks. flom, skogbrann, ekomutfall). Løsningen legger til rette for utvidelser. Vi forventer at det vil komme forslag/ ønsker om nye scenarioer når løsningen har kommet i bruk.

Løsningen vil ligge på www.ovelse.no

Lansering / distribusjon
Tilbud om å benytte løsningen gis til alle virksomheter som ønsker det, og dette lanseres i Sikkerhetsmåneden (oktober 2020). Lanserings-/markedsføringsplanen er i korte trekk distribusjon i departementsfellesskapene, på direktoratsnivå, til fylkesmennene og til kommunene via disse. I privat sektor oppfordres næringslivsorganisasjonene til å bidra til å informere sine virksomheter.

Vil dette bedre tilstanden i kommunene?
Øvingskonseptet er kun et tilbud til virksomhetene. Det er en enkel måte å øve på, og skal bedre forståelsen for de aktuelle problemstillingene. Den teknologiske plattformen vil gi oss et statistikkmateriale på bruken av løsningen.

10 Vedlegg E: Pågående og planlagte tiltak i regi av Kommunal informasjonssikkerhet (KiNS)

Prosjektbeskrivelse
Samarbeid om kompetanse og forvaltning for LSIS i kommunesektoren

Bakgrunn
KiNS har blitt oppfordret av medlemmer til å gjøre noe for å lette arbeidet med implementering og gjennomføring av ledelsessystem for informasjonssikkerhet og personvern i kommunene. Gjennom arbeidet med å etablere en handlingsplan for KiNS sin strategi, har et samarbeid om kompetanse og forvaltning for LSIS i kommunene blitt satt opp som hovedprioritet nr. 2 for hele strategiperioden.

Organisering
Inntil videre ledes prosjektet av daglig leder. Skulle det vise seg å være formålstjenlig at andre i KiNS leder prosjektet kan det vurderes å bytte prosjektleder. Det legges opp til bruk av nettmøter for å komme i gang. Når det er avklart hvem som deltar i den endelige prosjektgruppe er det naturlig å invitere til et eller flere fysiske møter.

Involvering
Flere kommuner har meldt sin interesse. I tillegg er det naturlig å invitere inn kommunene til styremedlemmer og varamedlemmer hvis det skulle være interesser for å bidra. Følgende kommuner har meldt interesse for å delta i prosjektet:
• Ringerike kommune
• Nordre Follo IKT
• Sarpsborg kommune

Digitaliseringsdirektoratet og KS er informert om arbeidet og det er tatt initiativ til faste møtepunkt for gjensidig informasjonsutveksling og koordinering. Det er gjensidig interesse blant de nevnte aktører for å avstemme kommunikasjonen og arbeidet som gjøres ut mot kommunene, slik at den enkelte kommune opplever at vi er samstemte og peker i samme retning.

Økonomi
Prosjektet vil søke ekstern finansiering der det er relevant. I første omgang peker KS og deres OU-midler seg ut som aktuelle. Dette har vært gjennomført i tidligere prosjekter til positive effekter for både KS, kommunene og KiNS. Digdir er en annen aktuell aktør å søke midler hos, da prosjektet kan fungere som en katalysator for bruken av deres veiledere, maler og eksempler i kommunene.

Framdriftsplan
• August 2020 – oppstart av prosjektet.
• Oktober 2020 - prosjektplan etablert der modell, progresjonsplan, milepæler og kostnader med mer er avklart.
• Januar 2021 - Finansiering avklart
• Juni 2020 - løsning 1.0 for samarbeid om kompetanse og forvaltning av LSIS
• Oktober 2021 - Avklaring knyttet til driftsfase i etterkant av prosjektet.
• Utgangen av 2021 - Prosjektet ferdigstilles innen utgangen av 2021.

Vedtak i KiNS styret 25. juni 2020 Styret godkjenner opprettelsen av prosjektet «Kommunalt samarbeid for kompetanse og forvaltning av LSIS» og ber administrasjonen gjennomføre nødvendige tiltak for etablering, gjennomføring og kvalitetssikring av prosjektet.I tillegg deltar KiNS i KS sitt Skolesec-prosjekt med et klart uttalt mål om å bidra til at det opprettes et delprosjekt i regi av KiNS for etablering av Code of Conduct/Norm for informasjonssikkerhet i grunnopplæringen.

Ut over dette arbeider vi kontinuerlig med å få opp bruken av våre kompetansepakker. Alle disse tre satsningene henger sammen og utfyller hverandre.

11 Vedlegg F: Pågående og planlagte tiltak i regi av KS

KS arbeider med følgende aktiviteter for å øke kunnskapsnivået innen informasjonssikkerhet-, digital beredskap, og personvern innen kommunal og fylkeskommunal sektor.

FOU prosjektene
Kommuner og fylkeskommuner vet at de skal etabler styringssystem for informasjonssikkerhet og det finnes allerede gode veiledere og standarder for etablering av slike systemer, eksempelvis ISO/IEC 27001/2. I KS' FoU-prosjekt "Kartlegging av digital modenhet i kommunesektoren" oppgis flere utfordringer knyttet til arbeid med informasjonssikkerhet. Utfordringer er gjerne knyttet til etterlevelse og prioritering og forståelse fra ledelsen. Ofte blir rapporteringer, risikovurderinger, kurs i informasjonssikkerhet og personvern med videre veldig omfattende og med et vanskelig språk. Videre strever mange med å etterleve og gjennomføre alle kravene i en travel hverdag, hvor man har mer enn nok med å gjennomføre de daglige faglige arbeidsoppgaver.

Det er derfor viktig å relatere regelverket og forklaringen av regelverket til noe som er mer praktisk knyttet til egen hverdag. Erfaringen er at mange vil følge retningslinjer, rutiner, lovverk men de vet ikke alltid hvordan de skal gjøre det i praksis når hendelser oppstår i deres daglige arbeide. Det er «lett» å få alle «systemene» på plass, utfordringen er å få dette til å bli levende praksis.

FOU1 - Tverrsektoriell digital samhandling i et informasjonssikkerhetsperspektiv - hvordan kan kommuner og fylkeskommuner ivareta sitt eget behov for informasjonssikkerhet og personvern?

Prosjektet har toppledelsen i kommuner og fylkeskommuner som målgruppe og ikke informasjonssikkerhetsansvarlige og personvernombud. Prosjektet skal bidra til at toppledere i kommuner og fylkeskommuner får en «verktøykasse» som de kan bruke for å sikre at de «har kontroll», eventuelt hvordan de «kan oppnå kontroll», på informasjonssikkerhets- og personvernområdet fra et topplederperspektiv.

Prosjektet skal rettes inn mot hvordan oppnå prioritering, ledelsesfokus, ressurser mv til arbeidet med personvern og informasjonssikkerhet. Rapporten skal også være praktisk anlagt med «ofte spurte spørsmål». Verktøykassen vil være i samme format som veiledningen (eller eventuelt inngå i) «Rådmannens internkontroll – Hvordan få orden i eget hus». Prosjektet er spesielt rettet mot små og mellomstore kommuner.

Forventet ferdigstillelse Q4 2020.

FOU2 - Veiviser for kommunal sektors etterlevelse av krav til informasjonssikkerhet og personvern

Prosjektet har alle ansatte i kommuner og fylkeskommuner som er målgruppe og ikke informasjonssikkerhetsansvarlige og personvernombud. Prosjektet skal bidra til at alle ansatte i kommuner og fylkeskommuner får en "verktøykasse" som de kan bruke for å sikre at informasjonssikkerhet og personvern blir en naturlig integrert faktor i utøvelse av dere daglige virke.

Prosjektet skal rettes inn mot det menneskelig aspekt med utgangspunkt i bl.a. adferds økonomi (Behavioral economics), beslutningslære (Decision-making), og kommunikasjon for å utforme en «verktøykasse» som inngår som en naturlig faktor i de ansattes hektiske hverdag. Formålet med en slik tilnærming er å kunne redusere risiko langs naturlig arbeidsstrøm, hensynta informasjonssikkerhet og personvern i arbeidsutførelsen, og legge til rette for innovasjon og evolusjon i et tjenesteleveranseperspektiv.

Forventet oppstart august 2020, forventet ferdigstillelse Q2 2021.

Prosjekt SkoleSEC

Skolesektorens har et stort mangfold av leverandører av digitale produkter å forholde seg til. For de aller fleste digitale tjenester skal det inngås databehandleravtaler, vurderes risiko (ROS) og gjøre personvernskonsekvensutredning (DPIA).

Å gjennomføre denne type oppgaver er svært ressurs- og tidkrevende. Mange kommuner har utfordringer med rutiner, ressurser, kapasitet, eller kompetanse til å gjennomføre disse oppgavene godt nok. Lærere trenger trygghet i valg og bruk av digitale tjenester. Elever og foreldre trenger trygghet i at de ressursene de pålegges å bruke forvalter deres data på en god måte.

Det er viktig å understreke at den enkelte kommune er behandlingsansvarlig for digitale løsninger. Samtidig vil endel punkter i risikovurderinger, sjekklister, og råd for trygg og sikker bruk av enkelttjenester i stor grad være sammenfallende på tvers av skoleeierne. KS har derfor etablert et prosjekt med formål å støtte kommunene og fylkeskommunene i arbeidet med informasjonssikkerhet og personvern i skolesektoren.

Prosjektet er oppstartet og varer i første omgang ut 2020.

RSB – Referanse arkitektur for informasjonssikkerhet, digital beredskap og personvern

Det finnes ingen helhetlig tilnærming til referansearkitektur for informasjonssikkerhet, digital beredskap og personvern for kommunal (herunder fylkeskommunal) sektor på strategisk nivå. KS har derfor i samarbeid med kommunal sektor og Interkommalene IKT-selskaper (IKS) igangsatt arbeidet med å utforme RSB.

RSB omhandler hvordan man finner kritikalitet på tjenesten, og om man har nødvendig sikkerhets- og beredskapsmessig evne for å kunne levere sikre og trygge tjenester i tråd med tjenestens kritikalitet. RSB omhandler ikke om sikkerhetsstyring på virksomhets- og operativnivå. RSB har spesielt fokus på tjenesteleveranser, sammenhengende tjenester og verdikjeder og kaskadevirkninger. RSB kan ses på som krav til tjenesteyter for levering av trygge og sikre digitale tjenester til kommunal sektor.

I første omgang er RSB spesielt rettet mot Akson prosjektet for å sikre at Akson journal AS har tilstrekkelig sikkerhets- og beredskapsmessig evne for å kunne levere sikre og trygge tjenester til kommunalsektor. I neste fase som starter august 2020 vil RSB generaliseres slik at denne kan benyttes av kommunal sektor på et generelt grunnlag.

Prosjektet er påstartet.

Fagråd for informasjonssikkerhet og personvern

Fagrådet for informasjonssikkerhet og personvern er en del av i samstyringsmodellen for kommunal sektor sammen med Digitaliseringsutvalget og KommIT-rådet som øverste organ. KommIT-rådet er et strategisk råd for digitalisering og smart bruk av teknologi i kommunal sektor. KommIT-rådet skal bidra til en samordnet kommunal sektor som leverer helhetlige digitale tjenester til innbyggere og næringsliv. Digitaliseringsutvalget (DU) er et arbeidsutvalg som forbereder saker til KommIT-rådet. DU er også pådriver for det samlede digitaliseringsarbeidet i kommunesektoren, og skal bidra til forankring og oppfølging av dette arbeidet.

Fagrådet for informasjonssikkerhet og personvern er et fagråd bestående av eksperter fra kommuner og fylkeskommuner og er rådgivende til Digitaliseringsutvalget. Fagrådet er også rådgivende ovenfor felles kommunale digitaliseringsprosjekter innen informasjonssikkerhets- og personvern. Fagrådet koordinerer også aktiviteter av felles art innen informasjonssikkerhets og personvern området i kommunal sektor.

SNIP – Strategisk nettverk for informasjonssikkerhet og personvern i kommunal sektor

Kommunal sektor (herunder fylkeskommunene og IKSer) er inne i en fase med rask digitalisering. Med økende digitaliseringstakt er informasjonssikkerhet, digital beredskap, og personvern viktig for å sikre at kommunal sektor kan fortsette å levere sikre og trygge tjenester til innbyggerne.

For å bidra til at kommunal sektor har nødvendig informasjonssikkerhets-, digital beredskaps-, og personvernmessig evne har KS opprettet et S*trategisk nettverk for informasjonssikkerhet, digital beredskap og personvern for kommunal sektor – SNIP*. Deltakerne i SNIP vil være personer som har et overordnet ansvar innen informasjonssikkerhet, digital beredskaps, eller personvern i kommunene/fylkeskommune.

Formålet med SNIP er å sørge for at kommunal sektor har en arena for felles problemstillinger av strategisk art innen informasjonssikkerhet, digital beredskap, og personvern. Det tas sikte på at alle kommuner, fylkeskommuner, og IKS deltar i SNIP. SNIP vil være direkte tilknyttet fagrådet for informasjonssikkerhet og personvern.

12 Referanseark for Digdir

Tittel på notat:	Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner Kunnskapsgrunnlag – En dokumentstudie
Digdirs rapportnummer:	2020:3
Forfatter(e):	Svanhild Gundersen, Elisabeth Aspaas Runsjø, Zoya Shah
Evt. eksterne samarbeidspartnere:	KS
Saksnummer:	20/00167
Prosjektnummer:	-
Prosjektnavn:	Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner
Prosjektleder:	Svanhild Gundersen
Prosjektansvarlig avdeling:	Digital Transformasjon
Oppdragsgiver(e):	KMD
Resymé/omtale: Digitaliseringsdirektoratet har på oppdrag fra Kommunal- og moderniseringsdepartementet (KMD) undersøkt hvordan fylkeskommuner og kommuner arbeider med informasjonssikkerhet. Arbeidet er utført i samarbeid med KS.	
Emneord: Informasjonssikkerhet, internkontroll, risikostyring, sikkerhetskultur og beredskapsøvelse.	
Totalt antall sider til trykking:	
Dato for utgivelse:	
Utgiver:	Digitaliseringsdirektoratet Postboks 1382 Vika 0114 OSLO www.digdir.no