Rapport

INDRE ØSTFOLD KOMMUNE

10.04.2024

Forvaltningsrevisjon
IKT-sikkerhet

Innhold

1 SAMMENDRAG

Revisjonens fremgangsmåte

BDO har gjennomført en forvaltningsrevisjon av IKT-sikkerhet i Indre Østfold kommune. Forvaltningsrevisjonen er gjennomført i tråd med «Standard for forvaltningsrevisjon» RSK 001. Østre Viken kommunerevisjons (ØVKR) mal for forvaltningsrevisjon er benyttet. BDO har benyttet en dedikert ressurs for å sikre kvalitet og etterlevelse av RSK 001 underveis i prosessen. Videre har revisor hatt kontinuerlig kontakt med ØVKR og Indre Østfold kommune om gjennomføring av revisjonen.

Fremdriftsplanen har bestått av tre faser:

1) Planlegging:
    a. Oppstartsmøte med BDO og Indre Østfold (3.11.23 og 05.12.23)
    b. Forankring av revisjonskriterier med Indre Østfold kommune
    c. Oppstartsbrev og oversendelse av revisjonskriterier
2) Gjennomføring
    a. Oversendelse av dokumentasjon
    b. Gjennomføring av intervju og spørreundersøkelse
    c. Analyse av datagrunnlag, vurdering og konklusjon
3) Sluttføring
    a. Utarbeidelse av rapport
    b. Verifisering faktagrunnlag fra Indre Østfold
    c. Utarbeidelse av rapport til ØVKR
    d. Utsending av høringsutkast til kommunedirektøren
    e. Ferdigstilling av endelig rapport til kontrollutvalget

Revisjonskriterier

Revisjonskriterier er en samlebetegnelse for de krav eller forventninger som brukes som grunnlag for å vurdere kommunens virksomhet. Revisjonskriterier fastsettes normalt med basis i autoritative kilder. Kommunens egne retningslinjer kan også utgjøre revisjonskriterier. Det skilles mellom krav som *må* (regulatoriske krav) og *bør* (beste praksis) gjennomføres (viser til 3.2 om revisjonskriterier for ytterligere informasjon). Fakta, omtalt som revisjonsbevis vurderes opp mot revisjonskriteriene, og disse vurderingene danner grunnlaget for de konklusjoner som trekkes.

Revisjonens funn og konklusjoner

Problemstilling 1: Har Indre Østfold kommune stilt tilstrekkelige sikkerhetskrav til IKT-leverandøren Ikomm, og hvordan følger kommunen opp disse kravene?

Revisor konkluderer, basert på den gjennomførte revisjonen, med at Indre Østfold kommune har stilt tilstrekkelige sikkerhetskrav til IKT-leverandøren Ikomm, og at kommunen følger opp disse kravene på en adekvat måte. Det er ikke avdekket alvorlige avvik knyttet til problemstilling 1.

Indre Østfold kommune jobber systematisk og grundig med teknisk informasjonssikkerhet. Kravene stilt fra kommunen til Ikomm er detaljerte og i hovedsak dekkende. Av de funnene som ikke er oppfylt har kommunen andre adekvate løsninger. Kravene følges opp i faste møter med leverandøren. Det er funn som viser manglende samordning av beredskapsplanene mellom kommunen og leverandøren. Revisor er imidlertid informert om at denne prosessen er påstartet. Det er identifisert enkelte mangler på krav som bør vurderes for å øke informasjonssikkerheten ytterligere.

Problemstilling 2: Har kommunens ansatte fått tilstrekkelig opplæring, sikkerhetsbevissthet og kompetanse til å ivareta sine primæroppgaver?
Revisor konkluderer, basert på den gjennomførte revisjonen, med at kommunens ansatte i noen grad har fått tilstrekkelig opplæring. Det er avdekket enkelte mangler som kan påvirke sikkerhetsbevissthet og kompetanse innen informasjonssikkerhet.

Revisor vurderer at Indre Østfold kommune har sørget for et adekvat opplæringsprogram for alle ansatte i kommunen, samt at kommunen jobber aktivt for å øke sikkerhetsbevisstheten og kompetansen. Dette gjelder blant annet innen dagsaktuelle risikoer, avvikshåndtering og sikkerhet på hjemmekontor. Indre Østfold kommune mangler imidlertid kompetansekrav for informasjonssikkerhet, spesielt for dedikerte sikkerhetsroller. Videre burde opplæringsprogrammet vært fordelt utover i året. Det er en stor andel (70-80 %) ansatte og ledere som ikke gjennomfører opplæringen, og for få ledere følger opp sitt ansvar med å formidle informasjon om informasjonssikkerhet til de ansatte. Revisor vurderer at fravær av gjennomføring kan påvirke ansattes evne til å ivareta sine primæroppgaver innen informasjonssikkerhet. Det gjenstår derfor et arbeid for å sikre at opplæringen utføres av kommunens ansatte.

Revisjonens anbefalinger

Anbefalingene er bygd opp ved følgende system:

1. Må rettes på snarest
2. Bør rettes på, men korrigerende tiltak kan skyves ut i tid
3. Bør vurderes rettes på, og korrigerende tiltak kan skyves ut i tid.

Basert på revisors vurderinger og konklusjon anbefaler revisor at Indre Østfold kommune bør:

Tiltak relatert til problemstilling 1:	Prioritet (1-3)
Samordne beredskapsplanen med Ikomm	1
Stille eksplisitte krav om beskyttelsestiltak på e-post og nettleser	2
Planlegge for en fremtidig revisjon av Ikomms etterlevelse av avtalekravene	3

Tiltak relatert til problemstilling 2:	Prioritet (1-3)
Etablere krav til ledere (eller andre tilsvarende rutiner) for å sikre gjennomføring av opplæring innen IKT-sikkerhet og varsling	2
Bevisstgjøre ledere om sitt ansvar for å følge opp at ansatte gjennomfører obligatorisk opplæring innen IKT-sikkerhet	2
Fastsette et årshjul for opplæringsaktiviteter for å spre opplæringsprogrammet utover året	2
Benytte signering ved gjennomført opplæring	2
Innarbeide et kurs for alle nyansatte om informasjonssikkerhet	2

Lage opplæringsmateriell om informasjonssikkerhetshåndboken for å gjøre innholdet mer forståelig og mindre tidkrevende	3
Benytte svar fra sikkerhetskulturkartleggingen til å justere opplæringsmateriellet	3
Formulere og fastsette kompetansekrav innen IKT-sikkerhet for dedikerte sikkershetsroller og kommunisere disse ut til kommunens ansatte	3
Legge til IKT-sikkerhet som et sjekkpunkt i systemet Framsikt	3
Gjennomføre kartlegging etter nye tiltak er iverksatt for å vurdere opplæringseffekten	3

Revisor gjør oppmerksom på at dette ikke er ment som en fullstendig liste over nødvendige tiltak, men etter revisors vurdering de mest vesentlige. Kommunen må selv vurdere hva som er nødvendige tiltak til enhver tid. Det er således ingen garanti at revisjonskriteriene er etterlevd ved å innføre de anbefalte tiltakene. Blant annet vil dette avhenge av ledelsens etterfølgende oppfølging av tiltakene for å sikre at de har den ønskede effekten.

2 MANDAT FOR FORVALTNINGSREVISJONEN

Revisjonen skal i henhold til kommunelovens § 24-2 (1) utføre forvaltningsrevisjon. Etter loven innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med god kommunal revisjonsskikk, som vil si å følge *Standard for forvaltningsrevisjon* (RSK 001) (NKRF[1], 2020). Dette innebærer blant annet at rapporten skal skille klart mellom innsamlede data (fakta) og revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger[2], vurderinger, konklusjoner og eventuelle anbefalinger. Etter kommuneloven skal revisor rapportere resultatene av sin revisjon til kontrollutvalget.

Forvaltningsrevisjonen er gjennomført på bakgrunn av plan for forvaltningsrevisjon vedtatt i kommunestyret i Indre Østfold kommune i sak 174/21 (08.12.2021). Plan for gjennomføring av forvaltningsrevisjonen ble vedtatt i kontrollutvalget 20.11.2023. Kontrollutvalget hadde innspill om å inkludere folkevalgte i revisjonens stikkprøvekontroll. Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet november 2023 til mars 2024. Det ble gjennomført et oppstartsmøte med kommuneadministrasjonen.

Revisor har kvalitetssikret innsamlet data/fakta underveis, både gjennom intervjuer og intern kvalitetssikring. I tillegg er faktaopplysningene i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp. Revisjonen avholdt avsluttende møte med administrasjonen 21.03.2024 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. Rapporten ble sendt på høring til kommunedirektøren. Kommunedirektørens uttalelse fremgår av rapportens kapittel 7.

Forvaltningsrevisjonen er gjennomført av Jolanta Betker, Casper Støten, Anine Klepp, Simen Bragen, Vetle Torstenbø og Mari Lekve Bjelle, og kvalitetssikret av Dagfinn Buset og Morten Thuve. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og den undersøkte virksomheten, og revisjonen finner de habile til å utføre forvaltningsrevisjonen.

Revisor vil takke kontaktpersoner og andre som har deltatt for et godt samarbeid i forbindelse med gjennomføringen av forvaltningsrevisjonen.

Østre Viken kommunerevisjon IKS
Rolvsøy, 10. april 2024

Dagfinn Buset	Casper Støten	
oppdragsansvarlig revisor	oppdragsansvarlig revisor	utførende forvaltningsrevisor

[1] NKRF er en faglig interesseorganisasjon og et kompetanseorgan for kontroll og revisjon av kommunal/offentlig virksomhet.

[2] Fakta er en gjengivelse av informasjonen vi har fått tilgang til gjennom datainnsamlingen.

3 FREMGANGSMÅTE

3.1 Problemstillinger og avgrensninger

Revisjonen har vært avgrenset til å besvare følgende problemstillinger:

Problemstilling 1: *Har Indre Østfold kommune stilt tilstrekkelige sikkerhetskrav til IKT-leverandøren Ikomm, og hvordan følger kommunen opp disse kravene?*

Med særlig fokus på:

i. Nedetid
ii. Digitale angrep
iii. Andre relevante krav basert på beste praksis

Avgrensning:
Indre Østfold kommune benytter flere IKT-leverandører i sine tjenester. Revisjonen er imidlertid avgrenset til IKT-leverandøren Ikomm ettersom det er hovedleverandøren til kommunen, og de drifter og leverer de fleste av kommunens tjenester. Revisor er kjent med at Ikomm er en leverandør hvor Indre Østfold kommune er en av eierne. Revisjonen har ikke inkludert aksjonæravtalen som en del av omfanget.

Indre Østfold kommune og Ikomm inngikk i 2019 en driftsavtale. Kommunen er p.t. i prosess med å inngå ny avtale med IKT-leverandøren, og dette skulle etter planen fullføres februar 2024. Da denne fristen på revisjonstidspunktet var i nærliggende fremtid har revisor valgt å vurdere kravene i den nye avtalen, ettersom vurdering av den gamle trolig ville gitt liten verdi. Revisjonsrapporten er dermed avgrenset til å gjelde utelukkende den nye avtalen mellom IKT-leverandøren Ikomm og Indre Østfold kommune, og oppfølging fra kommunen relatert til disse kravene.

Problemstilling 2: *Har kommunens ansatte fått tilstrekkelig opplæring, sikkerhetsbevissthet og kompetanse til å ivareta sine primæroppgaver?*

Med særlig fokus på:

i. Sikkerhet på hjemmekontor
ii. Ansattes evne til å forhindre/redusere risikoen for menneskelig svikt

Avgrensning:
Revisjonen har valgt ut enkelte seksjoner ved Indre Østfold kommune, deriblant administrasjonen, skole, barnehage og livsmestring (barnevern).

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisor fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriteriene er den objektive målestokk som setter revisor i stand til å gjøre vurderinger på de fleste områder uten å ha formell fagspesifikk kompetanse. Revisjonskriteriene og revisors kunnskap og erfaring innen forvaltningsrevisjonsmetodikk, gjør at revisor kan gjøre objektive og holdbare vurderinger.
Revisjonskriteriene etablerer den norm som de innsamlede dataene skal vurderes opp mot. I tillegg til dette skal revisjonskriteriene også gjøre det tydelig for den reviderte enhet hva de måles opp mot. Revisjonskriteriene klargjør også overfor folkevalgte, media og andre lesere av forvaltningsrevisjonen, hva

revisors vurderinger bygger på. Dette vil gjøre det enklere å etterprøve revisors vurderinger. Revisjonskriteriene skal være relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet. Revisjonskriterier som baseres på regulatoriske krav formuleres som *skal*-krav og anbefalte tiltak må gjennomføres av kommunen. Revisjonskriterier som baseres på standarder og anbefalinger formuleres imidlertid som *bør,* og videre anbefalinger formuleres som tiltak kommunen kan iverksette for å bedre informasjonssikkerhetsarbeidet

Revisjonskriterier fastsettes vanligvis med basis i en eller flere følgende kilder: lovverk, politiske vedtak og føringer, kommunens egne retningslinjer, anerkjent teori på området, eller andre sammenlignbare virksomheters løsninger og resultater.

Prosjektet har tatt utgangspunkt i følgende kilder for utledning av revisjonskriterier:

- Forskrift om kommunal beredskapsplikt
- NS-ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet
- Nasjonal sikkerhetsmyndighet – Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester
- Datatilsynets veileder – Informasjonssikkerhet og internkontroll
- Nasjonal sikkerhetsmyndighet - Grunnprinsipper for IKT-sikkerhet
- Digitaliseringsdirektoratet - Kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet

3.3 Revisjonsmetoder

I henhold til god revisjonsskikk skal praksis eller tilstand innen det reviderte området beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. I denne forvaltningsrevisjonen har vi benyttet data fra ulike kilder, og brukt ulike metoder for innsamling av data, for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet.

Utfordringer og begrensninger i rapportens faktagrunnlag beskrives nedenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene.

I denne forvaltningsrevisjonen er informasjonen hentet inn gjennom bruk av følgende metoder:

- Dokumentanalyse
- Intervjuer
- Stikkprøveteknikk
- Spørreundersøkelse

Dokumentanalyse

Revisor har gjennomgått sentrale dokumenter på området. Dokumentene er oversendt fra Indre Østfold kommune. Fullstendig oversikt over dokumentene fremgår av kildehenvisningene i kapittel «6. Kilder og litteratur».

Intervjuer

Det er gjennomført totalt 8 intervjuer. Blant de intervjuede er det informanter fra sentrale stillinger rettet mot IKT-sikkerhet, samt representanter med lederstillinger fra de ulike utvalgte seksjonene. Se liste over informanter i kapittel «6.Kilder og litteratur».

Alle intervjuer er gjennomgått av intervjuobjektene. Det betyr at den som er intervjuet har fått lese gjennom og eventuelt foretatt endringer i referatet fra intervjuet for å bekrefte at referatet er i overenstemmelse med det som ble sagt under intervjuet.

Under enkelte intervjuer ble det gjennomført stikkprøver. Stikkprøver benyttes som metode for å verifisere fakta ved å vise til konkrete og dokumenterte «bevis». Eksempelvis fikk revisor innsikt i programmet *Framsikt*, hvordan det er bygd opp, og hvordan brukere kan benytte dette.

Spørreundersøkelse

Det er gjennomført en spørreundersøkelse som ble utsendt til et utvalg ansatte i Indre Østfold kommune ved benyttelse av tilfeldig utvalg. De utvalgte sektorene var administrasjonen, skole, barnehage og livsmestring (barnevern). I tillegg gikk spørreundersøkelsen ut til et utvalg folkevalgte i kommunen. Svarene fra undersøkelsen som ble sendt til politikerne påvirker ikke revisjonsfunnene, men danner grunnlag for anbefalinger om tiltak. Undersøkelsen er gjennomført ved hjelp av det nettbaserte spørreundersøkelsesverktøyet Feedback.

Feedback er et verktøy for spørreundersøkelser som er utarbeidet av BDO. Spørreundersøkelsen bestod av 14 spørsmål, hvorav et av spørsmålene ga mulighet for tekstsvar. Formålet med spørreundersøkelsen var å kartlegge ansattes syn på kommunens opplærings- og bevisstgjøringsprogram innen informasjonssikkerhet, og effekten av dette.

Spørreundersøkelsen ble sendt ut til 10 % av de ansatte fra henholdsvis administrasjonen, skole, barnehage og livsmestring (barnevern). Svarprosenten for undersøkelsen fordelt på de ulike seksjonene i Indre Østfold fremgår av tabell 1 nedenfor:

Seksjon	Svarprosent	Antall
Administrasjonen (fellestjenester)	23,7 %	9
Barnehage eller barneskole	28,9 %	11
Ungdomsskole	5,3 %	2
Livsmestring	26,3 %	10
Annet	15,8 %	6
Totalt	**100 %**	**38**

Tabell 1, Svarprosent fra ansatte i Indre Østfold kommune – Kilde: spørreundersøkelse utført av BDO

Alder	Antall
30 år	2
31-40 år	3
41-50 år	14
51-60 år	16
61 eller over	3
Totalt	**38**

Tabell 2, Aldersfordeling blant de ansatte – Kilde: Spørreundersøkelse utført av BDO

Det var frivillig å delta i spørreundersøkelsen, og personopplysninger ble ikke samlet inn. Dataene ble benyttet til formålet i forvaltningsrevisjonen og ble slettet etter gjennomført analyse.

Det ble identifisert enkelte utfordringer ved spørreundersøkelsen:

1) For å holde spørreskjemaet anonymt, var det mulighet for å fylle ut skjemaet flere ganger. Dette kan vurderes som en metodisk svakhet. Revisor valgte imidlertid denne løsningen for å sikre anonymitet.
2) Lav svarprosent på spørreundersøkelsen kan påvirke grad av validitet, og at funnene ikke er representative for hele Indre Østfold kommune. Revisor vil dermed bemerke at svarenes gyldighet kan være noe begrenset i rapporten. Likevel mener revisor at oppfatningen til de som har svart har verdi ettersom representanter fra ulike seksjoner har gjennomført spørreundersøkelsen, og andre kilder blir benyttet i datagrunnlaget.
3) Grunnet begrenset tid i forvaltningsperioden ble spørreskjemaet sendt ut rett før juleferien med svarfrist andre uken i januar 2024. Det korte tidsrommet kan ha påvirket svarprosenten. Som et kompenserende tiltak ble det sendt ut to påminnelser per e-post om å gjennomføre spørreundersøkelsen.
4) På bakgrunn av ett tilfelle av manglende e-post og tre tilfeller av feilmelding ved utsendelse valgte revisor å sende undersøkelsen til den neste personen på uttrekkslisten. Revisor vurderer likevel at det ikke påvirker kravene for «tilfeldig utvalg».

Avgrensninger

Datainnhentingsmetodene som er benyttet i revisjonen kan alltid ha begrensninger, og vil ikke fullt ut dekke en representasjon av virkeligheten. Likevel er det etter revisors vurdering en styrke å benytte ulike datainnsamlingsmetoder da dette belyser temaet fra flere perspektiver.

BDO har basert våre analyser på mottatte data og kan ikke gå god for at det ikke er feil i datagrunnlaget.

3.4 Skala og symbolbruk for vurdering av funn

I tilknytning til evalueringen av revisjonsbevisene opp imot hvert enkelt revisjonskriterium benyttes symboler som uttrykk for vår oppfatning av resultatet av gjennomgangen (funn).

Symbolbruken og beskrivelsen av disse illustreres i figur 1 nedenfor.

Rød	Avdekkede forhold oppfyller ikke revisjonskriteriet. Det er avdekket vesentlige forbedringspotensial som bør gis høy prioritet.
Oransje	Avdekkede forhold oppfyller i liten grad revisjonskriteriet. Det er avdekket vesentlige forbedringspotensial.
Gul	Avdekkede forhold oppfyller i noen grad revisjonskriteriet. Det er avdekket forbedringspotensial.
Lysegrønn	Avdekkede forhold oppfyller i stor grad revisjonskriteriet. Det er imidlertid avdekket enkelte forbedringspotensial.
Grønn	Avdekkede forhold anses å være av uvesentlig betydning, og i praksis oppfylles dermed revisjonskriteriet.

Figur 1, Symbolbruk for vurdering av funn

4 SIKKERHETSKRAV TIL IKT-LEVERANDØREN

Problemstilling 1: Har Indre Østfold kommune stilt tilstrekkelige sikkerhetskrav til IKT-leverandøren Ikomm, og hvordan følger kommunen opp disse kravene?

4.1 Revisjonskriterier

Revisor har utledet revisjonskriterier basert på regulatoriske krav, beste praksis og veiledere fra relevante myndigheter.

I henhold til NSMs grunnprinsipper eksisterer det en rekke anbefalinger om hvilke tiltak virksomheter bør iverksette for å øke sikkerheten i sine tjenester. Anbefalingene dekker IKT-sikkerhet både under 1) identifisering og kartlegging, 2) beskyttelse og opprettholdelse, 3) oppdaging og 4) håndtering og gjenoppretting. Videre fremgår det av NSMs sikkerhetsfaglige anbefalinger ved tjenesteutsettelse ulike føringer til hvordan sikkerhet skal ivaretas ved anskaffelse av IKT-tjenester. I henhold til NSMs sikkerhetsfaglige anbefalinger ved tjenesteutsettelse og ISO/IEC ISO27001 bør virksomheter ha en kravspesifikasjon for IKT-tjenesten som skal tjenesteutsettes. Det vurderes derfor at Indre Østfold kommune bør benytte seg av en rekke av disse anbefalingene i kravsettingen til IKT-leverandøren Ikomm for å sikre kommunens verdier.

I henhold til NSMs grunnprinsipper bør virksomheter følge opp at krav til IKT-leverandører blir etterlevd for å sikre at kontraktsforpliktelsene etterleves. Dermed vurderes det at Indre Østfold kommune bør sette krav og etablere en prosess for å vurdere IKT-leverandøren Ikomms etterlevelse av kravene de har satt.

I henhold til forskrift om kommunal beredskapsplikt skal kommunens beredskapsplan samordnes med andre relevante offentlige og private krise- og beredskapsplaner. Det tolkes derfor at kommunen skal samordne sin beredskapsplan med IKT-leverandøren Ikomm.

Det skilles mellom krav som *må* og *bør* gjennomføres. Se under 3.2 revisjonskriterier for ytterligere informasjon.

4.1.1 Revisjonskriterier for problemstilling 1

Indre Østfold kommune skal:

- samordne sin beredskapsplan med andre relevante offentlige og private krise- og beredskapsplaner (jf. forskrift om kommunal beredskapsplikt § 4).

Indre Østfold kommune bør:

- ha utarbeidet skriftlige prosesser og prosedyrer for å ivareta sikkerhet i anskaffelses- og utviklingsprosesser (NSMs grunnprinsipper 2.2.1)
- sikre innsyn i hvordan IKT-leverandøren Ikomm ivaretar sine forpliktelser ved å avtalefeste dette (NSM – sikkerhetsfaglige anbefalinger ved tjenesteutsetting)
- følge opp at krav til IKT-leverandøren Ikomm blir etterlevd for å sikre at kontraktsforpliktelsene ivaretas (NSM – sikkerhetsfaglige anbefalinger ved tjenesteutsetting)
- ha en detaljert kravspesifikasjon for IKT-tjenesten som skal tjenesteutsettes (Jf. NSMs grunnprinsipper, NSM: Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester, ISO/IEC 27001)
- stille krav til at IKT-leverandøren Ikomm har et etablert styringssystem for informasjonssikkerhet (NSM – sikkerhetsfaglige anbefalinger ved tjenesteutsetting)

- stille krav om innsyn i sikkerhetsarkitekturen som benyttes av IKT-leverandøren Ikomm for å levere tjenester til kommunen (NSM – sikkerhetsfaglige anbefalinger ved tjenesteutsetting)
- stille krav til IKT-leverandøren Ikomm om tilgangsstyring, som inkluderer kryptering, aktivitetslogg, samt fysisk og logisk sikkerhet (NSM – sikkerhetsfaglige anbefalinger ved tjenesteutsetting)
- stille krav om at underleverandører skal godkjennes av kommunen før de gis tilgang til kommunens informasjon (NSM – sikkerhetsfaglige anbefalinger ved tjenesteutsetting)
- stille krav til IKT - leverandøren Ikomm at de har oversikt over hvem som skal ha innsyn i virksomhetens informasjon, hvor og hvordan denne skal behandles og lagres (NSMs grunnprinsipper 2.1.1 d)
- stille krav til IKT-leverandøren Ikomm om å etablere planverk for hendelseshåndtering – gjelder også plan for kommunikasjonskanaler (NSMs grunnprinsipper 4.1.1, 4.1.5)
- stille krav til at IKT-leverandøren Ikomm tester og øver på planer jevnlig (NSMs grunnprinsipper 4.1.6)
- stille krav om aktiviteter ved terminering av kontrakt med IKT-leverandøren Ikomm, herunder tilbakeføring/flytting eller sletting av kommunens informasjon (NSMs grunnprinsipp 1.2.1)
- stille krav til innsikt i enheter og programvare disponert av kommunen i IKT-leverandøren Ikomms IT-miljø
- stille krav til at IKT-leverandøren Ikomm gjennomfører periodiske gjennomganger for å kartlegge brukere og behov for tilgang (NSMs grunnprinsipp 1.3.1)
- stille krav til at IKT-leverandøren Ikomm har fordelt ansvar og roller innen IKT-sikkerhet (NSMs grunnprinsipp 1.3.3)
- stille krav til at leverandøren Ikomm gjennomfører ekstern sikkerhetstesting hvert år (NSMs grunnprinsipp 3.4.4)
- stille krav til at IKT-leverandøren Ikomm segregerer data fra andre kunder (NSMs grunnprinsipper 2.1.10 d)
- stille krav til at IKT-leverandøren Ikomm har sikkerhetsovervåkning for å avdekke sikkerhetshendelser som kan påvirke virksomheten (NSMs grunnprinsipp 2.1.10 f)
- stille krav til at IKT-leverandøren Ikomm har rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering (NSMs grunnprinsipp 2.1.10 g)
- stille krav til at IKT-leverandøren Ikomm har etablert et regime for sikkerhetsoppdatering (NSMs grunnprinsipp 2.3.1)
- stille krav til at IKT-leverandøren Ikomm har etablert tilgangskontroll på flest ulike nettverksporter (NSMs grunnprinsipp 2.4.1)
- stille krav til at IKT-leverandøren Ikomm benytter multi-faktor autentisering (NSMs grunnprinsipp 2.6.7)
- stille krav til at IKT-leverandøren Ikomm har beskyttelsestiltak på e-post og nettleser (NSMs grunnprinsipp 2.8.1)
- stille krav til at IKT-leverandøren Ikomm har plan for regelmessig sikkerhetskopiering av alle virksomhetsdata (NSMs grunnprinsipp 2.9.1)
- stille krav til at IKT-leverandøren Ikomm har plan og evne til å gjenopprette data (NSMs grunnprinsipp 2.9.1-2)
- stille krav til at IKT-leverandøren Ikomm bør benytte automatiserte verktøy for å håndtere skadevare (eksempelvis antivirus) (NSMs grunnprinsipper 2.2.5)
- *Aktuelt hvis Ikomm drifter både server og klienter for kommunen:* Indre Østfold kommune bør stille krav til at IKT-leverandøren Ikomm holder domenearkitekturen adskilt (NSMs grunnprinsipper 2.2.5)

4.2 Datagrunnlag

4.2.1 Indre Østfold kommune skal samordne sin beredskapsplan med IKT-leverandøren Ikomm

Revisor ble i intervju informert om at kommunen har delt sin beredskapsplan med Ikomm. Videre fremkom det i intervju at kommunen ønsker at Ikomm skal dele sin beredskapsplan med kommunen. Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at IKT-leverandøren Ikomm skal ha *«krise- og beredskapsplaner som er harmonisert med kundens beredskapsplaner»*. Videre fremgår det at

> *«kunden har krav om at leverandøren skal avsette ressurser til å bidra i arbeidet med å utvikle kundens krise- og beredskapsplaner for eKom og kan ved behov trekkes inn i kundens overordnede beredskapsarbeid og inngå i kundens beredskapsorganisasjon og ved øvelser».*

Revisor ble opplyst om at Indre Østfold og Ikomm bør samordne sine beredskapsplaner i ytterligere grad, og at dette prioriteres fremover. Videre fremkom det at Ikomm har bidratt i beredskapsøvelse som kommunen har avholdt.

4.2.2 Indre Østfold kommune bør ha utarbeidet skriftlige prosesser og prosedyrer for å ivareta sikkerhet i anskaffelses- og utviklingsprosesser

Det fremkom i intervju at Indre Østfold kommune har overført skriftlige avtaler fra de tidligere fem selvstendige kommunene. Kommunen er i dag i en prosess hvor de har utarbeidet kravspesifikasjon for Ikomm. Revisor ble informert om at ny avtale vil signeres i februar 2024. Videre ble revisor informert at kommunen har utarbeidet databehandleravtaler og DPIA[3] med leverandører. Det fremkom videre at avtalen med Ikomm er basert på *Store Sky*[4]. Videre informerte kommunen om at de på strategisk nivå har gjennomgått elementene i *Pestel*[5] og at det er gjennomført en *SWOT*[6] i fellesskap. Revisor ble opplyst om at dette har som hensikt å ha et fremtidsrettet blikk med tanke på tjenester, deriblant en samtale om hva kommunen mente at Ikomm kunne levere og til riktig kvalitet, kostnad og risiko.

Kommunens «skriftlige prosesser og prosedyrer knyttet til informasjonssikkerhet i leverandørforhold og anskaffelse av programvare eller skytjenester» fremgår av *Informasjonssikkerhetshåndbokens* kapittel 2. De skriftlige prosessene og prosedyrene som omhandler anskaffelse av programvare eller skytjenester skal det utføres følgende prosesser:

a. Vurdering av personvernkonsekvenser
b. Etablere databehandleravtale
c. Utarbeide behandlingsprotokoll

Videre fremgår det av *Informasjonssikkerhetshåndboken* at aktiv forvalting av IKT-systemet må inneholde et robust sikkerhetsrammeverk som inkluderer regelmessige sikkerhetsrevisjoner, oppdateringer av sikkerhetsprotokoller og responsplaner for sikkerhetshendelser. Det fremgår videre at et kritisk aspekt ved anskaffelse av IKT-systemer er opprettelsen og oppfølgingen av kontrakter med leverandører.

Det fremgår av *Informasjonssikkerhetshåndboken* at kommunen skal utarbeide en kravspesifikasjon

[3] "DPIA" står for Data Protection Impact Assessment. Etter personvernregelverket har virksomhetene plikt til å vurdere personvernkonsekvensene når løsninger tas i bruk.

[4] Store Sky refererer til en avtale som kan benyttes ved anskaffelse og vedlikehold av skybaserte løsninger

[5] Pestel refererer til et verktøy brukt til å analysere eksterne faktorers påvirkning på en organisasjon

[6] SWOT refererer til en strategisk planleggingsmetode brukt til å identifisere og analysere interne styrker og svakheter i en virksomhet.

ved anskaffelser. Kravspesifikasjonen til IKT-leverandøren Ikomm er dokumentert i *Leverandørens svar på kundens kravspesifikasjon.* Kommunen benytter statens standardavtale (SSA) som kontaktsmal for anskaffelse av IT-løsninger som programvare eller skytjenester.

Videre fremgår det av *Informasjonssikkerhetshåndboken* prosedyrer for følgende områder:

- Informasjonssikkerhet i leverandørforhold
- Anskaffelse og forvaltning av programvarelisens
- For å ta i bruk skytjenester
- Kontroll av leverandører

Det fremgår av *Informasjonssikkerhetshåndboken* at kommunen har en plikt til å inngå en databehandleravtale ved benyttelse av underleverandører. Kommune har fremlagt dokumentet *Databehandleravtale.*

4.2.3 Indre Østfold kommune bør sikre innsyn i hvordan IKT-leverandøren Ikomm ivaretar sine forpliktelser ved å avtalefeste dette

Det fremkom i intervju at kommunen har stilt krav til Ikomm innen IKT, og at Ikomm har besvart hvordan de ivaretar sine forpliktelser. Videre ble revisor informert om at Ikomm også har besvart hvilke forpliktelser de ikke ivaretar.

Det fremgår av *Informasjonssikkerhetshåndboken* at det er etablert prosedyre av kontroll av leverandører. Formålet med prosedyren er at den skal sikre at leverandørene oppfyller kommunens krav til informasjonssikkerhet. Denne omfatter:

- Risikovurdering av leverandører
- Kontroll av sikkerhetsdokumentasjon
- Revisjon ved behov.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at avtalen med Ikomm inneholder spesifikke krav til samhandlingsmodell og møtekrav for å sikre innsyn. Det fremgår av dokumentet at Ikomm bekrefter at de skal etterleve kommunens krav til samhandling.

Det ble opplyst i intervju at kommunen har jevnlige samhandlingsmøter med Ikomm. Det er fastsatt SLA[7] og kommunen har en dedikert, navngitt Key Account Manager.

4.2.4 Indre Østfold kommune bør følge opp at krav til IKT-leverandøren Ikomm blir etterlevd for å sikre at kontraktsforpliktelsene ivaretas

Revisor ble i intervju opplyst om at kommunen følger opp at Ikomm etterlever krav i jevnlige samarbeidsmøter. Videre fremkom det i intervju at kommunen i ny samhandlingsplan ønsker tre månedlige møter med Ikomm.

Viser til datamaterialet som er presentert under revisjonskriteriet 4.2.2 for ytterligere informasjon om prosedyre for kontroll av leverandør.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at leverandøren skal utarbeide en møteplan for 2024.

[7] SLA referer til Service level agreement som er en serviceavtale mellom tilbyder og kunde.

Møtekalender for 2024 inneholder følgende punkter:

1. *Driftsmøter: Disse skal avholdes én gang per måned med fokus på status SLA og andre driftsmessige forhold. Deltakere inkluderer kundeansvarlig, SLM og driftssjef IØK.*
2. *Samhandlingsmøter: Disse skal også avholdes én gang per måned. Møtene vil fokusere på informasjon om endringer, informasjonssikkerhet og kundens behov. Det vil også være en diskusjon om samhandling med andre kommuner.*
3. *Møter mellom servicedesk og brukerstøtte: Disse møtene skal avholdes én gang per måned.*
4. *Utviklingsmøter/-strategimøter: Disse skal avholdes én gang per kvartal. Møtene vil fokusere på budsjett-innspill og utfordringer.*

Det er videre fastsatt et årshjul for 2024 med datoer for gjennomføring av møtene.

4.2.5 Indre Østfold kommune bør ha en detaljert kravspesifikasjon for IKT-tjenesten som skal tjenesteutsettes

Det fremkom i intervju at kommunen har utarbeidet en detaljert kravspesifikasjon for IKT-tjenesten som skal tjenesteutsettes.

Det fremgår av *Informasjonssikkerhetshåndboken* at kommunen skal utarbeide en kravspesifikasjon ved alle anskaffelser. Kommunens krav til IKT-leverandøren Ikomm fremgår av *Leverandørens svar på kundens kravspesifikasjon* Det fremgår at målet med kravene er at Indre Østfold skal oppnå:

- *«En stabil og forutsigbar leveranse av robuste og kvalitetsmessige gode IT-tjenester*
- *Sikre tilgang til kompetanse som kan bidra til at kommunen kan levere digitale tjenester til innbyggere, ansatte, elever og lærere med høy kvalitet*
- *God informasjonssikkerhet slik at sårbarhet og risikoeksponering minimeres*
- *Stabil og forutsigbar applikasjonsforvaltning*
- *Rask implementering av nye løsninger*
- *Økt digital modenhet*
- *Fokus på tjenesteutvikling og innovasjon i tråd med det digitale målebildet*
- *Mer kostnadseffektiv leveranse av skytjenester»*

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt krav til følgende områder:

- Generelle krav til driftsplattform og administrasjon av denne
- Drift av applikasjon og løsninger i Microsoft Azure
- Drift og konfigurering av Norsk helsenett SF (NHN)
- Leveranse av kommunale IT-tjenester til Indre Østfold NAV
- Sikker utskrift
- Drift og vedlikehold av digital skoleplattform
- Drift av klienter (PCer og lesebrett)
- Drift av nettverk (LAN) og Wifi
- Forvaltning og utbygging Fibernettverk
- Mobile Device Management
- Lisensrådgivning
- Opplæring
- Integrasjoner med eksisterende og nye tjenester
- Rutineutvikling
- Dokumentasjon
- Brukerstøtte
- Masterdata og identitets- og tilgangsstyring

- Økonomioppfølging av variable skykostnader
- Drift- og sikkerhetsovervåkning
- Avslutning av avtale/overgang til ny leverandør
- Informasjonssikkerhet og sikkerhetsløsninger
- Beredskapsarbeid og samhandling med Kunden
- Bistand til Risiko og sårbarhetsvurdering
- Holde kundens data atskilt
- Avslutning av avtale/overgang til ny leverandør
- Samhandling.

4.2.6 Indre Østfold kommune bør stille krav til at IKT-leverandøren Ikomm har et etablert styringssystem for informasjonssikkerhet

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at kommunen har stilt følgende krav:

> *«Leverandøren skal anvende et dokumentert styringssystem for informasjonssikkerhet. Eksempelvis vil ISO/IEC 27001 eller tilsvarende oppfylle kravet. Styringssystemet skal være tilgjengelig for kunden».*

Det fremkom i intervju at Ikomm innehar gyldig ISO/IEC 27001-sertifisering og at Ikomm har etablert et styringssystem basert på denne standarden. Det fremgår av *Bilag 2C – Ikomm-iso-27001-no* at Ikomm er sertifisert etter ISO/IEC 27001:2017. Sertifikatet gjelder for driftstjenester OnPrem, sky og support.

4.2.7 Indre Østfold kommune bør stille krav om innsyn i sikkerhetsarkitekturen som benyttes av IKT-leverandøren Ikomm for å levere tjenester til kommunen

Det fremgår av *Bilag 2C – Leverandørens svar på kundens kravspesifikasjon* at kommunen har stilt følgende krav til Ikomm:

- *«Kunden har krav om dokumentasjon av installasjonsbeskrivelse av hvert enkelt system med hensyn til arkitektur, database, avhengigheter mot andre systemer/tjenester og integrasjoner»*
- *Dokumentasjon av driftsplattformens arkitektur, programvare, maskinvare, redundans, fysiske sikkerhetstiltak, nødstrøm, fysiske føringsveier for datanettverk og etablert redundans og annen relevant informasjon om driftsplattformen».*
- *Leverandør skal ha utarbeidet konfigurasjonskart som viser sikkerhetskontroller og teknisk beskrivelse av informasjonssystemene, inkludert dataflyt»*
  Dokumentasjon av informasjonssikkerheten i driftsplattformen, slik som kryptering, brannmurløsning, antivirusløsning, segmenteringsløsning, logging, autentiserings-løsning mv».

4.2.8 Indre Østfold kommune bør stille krav til IKT-leverandøren Ikomm om tilgangsstyring, som inkluderer kryptering, aktivitetslogg, samt fysisk og logisk sikkerhet

Det fremgår av *Bilag 2C – Leverandørens svar på kundens kravspesifikasjon* at kommunen har stilt krav om følgende:

> *Tilgangsstyring:*
> - *«Leverandøren skal dokumentere prosess for automatisert tilgangsstyring, herunder opprettelse, endring og sletting av brukere»*
>
> *Kryptering:*
> - *«Leverandøren skal sikre at datakommunikasjon over usikre nettverk (for eksempel Internett) skal være kryptert i henhold til beste praksis. Trafikk i klartekst skal ikke forekomme»*

- *«Leverandøren skal benytte de nyeste og sterkeste krypteringslogaritmer og at tilhørende protokoller og nøkler er på plass»*
- *«Data i ro eller transitt skal krypteres»*
- *«Ende til ende-kryptering mellom klient (bruker) og løsningen»*
- *«Kryptering av lagret data inkl. backup»*
- *«Kryptering mellom løsningen og eventuelle underleverandører»*
- *«Sikre protokoller (eksempelvis TLS) for transit skal benyttes»*

Fysisk sikring:

- *«Leverandør skal ha tilstrekkelig fysisk sikring knyttet til alle sine datarom, som adgangskontroll, brannsikring, ventilasjon, redundant strømforsyning og naturhendelser»*
- *«Tilgang til datarom skal kun gis de som har et tjenstlig behov. Kravet dekker også andre elementer, som for eksempel brannslukkingsapparat, alarm, kjøling og nødstrøm»*

Sikring av datautstyr:

- *«Datautstyr som er i kontakt med kundens informasjon skal være tilstrekkelig sikret»*

Logisk sikkerhet:

- *«Leverandøren skal drifte og sikre nettverk (Vlan) og eventuelt etablere nye logiske nettverk ved behov»*

Overvåkning og logging:

- *«Leverandør skal logge alle forsøk på autorisert og uautorisert tilgang til tjenesten, samt relevante sikkerhetshendelser som er tilknyttet løsningen»*
- *«Leverandør sal sikre at logger beskyttes mot uautorisert innsyn, endring og sletting»*
- *«Leverandør skal sikre følgende logging ved aksess av data i tjenesten:*
    1. *Hvem som aksesserte;*
    2. *Når data ble aksessert (dato og klokkeslett)*
    3. *Hvilke data som ble aksessert*
    4. *Ved endring skal alle data/felter som ble endret logges.*

4.2.9 Indre Østfold kommune bør stille krav om at underleverandører skal godkjennes av kommunen før de gis tilgang til kommunens informasjon

Det fremgår av *Informasjonssikkerhetshåndboken* at Indre Østfold kommune har plikt til å ha en databehandleravtale ved benyttelse av underleverandør. Revisor ble i intervju opplyst om at kommunen har inngått databehandleravtale med Ikomm. Det fremkom i intervju at sikkerhetsansvarlig kvalitetssikrer databehandleravtaler for de ulike kommunalområdene før signering.

Det fremgår av *Databehandleravtale* at Indre Østfold kommune har satt krav om følgende:

- *«Databehandler kan kun benytte Underdatabehandler etter forutgående generell eller spesifikk tillatelse fra Behandlingsansvarlig i samsvar med Databehandleravtalens Bilag B.*
- *«Dersom en Databehandler engasjerer en Underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Behandlingsansvarlige, plikter Databehandler å inngå skriftlig avtale med Underdatabehandleren som pålegger denne tilsvarende forpliktelser med hensyn til vern av personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen».*

4.2.10 Indre Østfold bør stille krav til IKT - leverandøren Ikomm at de har oversikt over hvem som skal ha innsyn i virksomhetens informasjon, hvor og hvordan denne skal behandles og lagres

Det fremgår av *Bilag 2C – Leverandørens svar på kundens kravspesifikasjon* at kommunen har stilt krav om følgende:

- *«Leverandøren skal dokumentere prosess for automatisert tilgangsstyring, herunder opprettelse, endring og sletting av brukere».*
- *«Sikring av grensesnitt mot uautorisert tilgang: Alle grensesnitt for nettjenester (web, API-er, endepunkter skal være sikret mot uautorisert tilgang.*
- *«Løsningen skal ha rollebasert tilgangsstyring»*
- *«Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet grunnprinsipper for IKT-sikkerhet som i skrivende stund er versjon 1.1. Her defineres et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene de tilbyr mot uautorisert tilgang, skade og misbruk. IKT-sikkerhet hos leverandør skal være på nivå med gjeldende grunnprinsipper som angitt av nasjonal sikkerhetsmyndighet eller bedre».*

4.2.11 Indre Østfold kommune bør stille krav til IKT-leverandøren Ikomm om å etablere planverk for hendelseshåndtering – gjelder også plan for kommunikasjonskanaler

Viser til revisjonskriteriet 4.2.1 som redegjør for kommunens krav til IKT-leverandøren Ikomms beredskapsplan.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Ikomm *«skal ha effektive varslingsrutiner for sikkerhetsbrudd som gjør at leverandøren raskt kan identifisere, rette og rapportere uønskede hendelser til kommunen».*

Revisor fikk opplyst at Indre Østfold ser behovet for økt samhandling med IKT-leverandøren Ikomm knyttet til rutiner for hendelseshåndtering.

4.2.12 Indre Østfold kommune bør stille krav til at IKT-leverandøren Ikomm tester og øver på planer jevnlig

Revisor ble i intervju informert om at kommunen skal samarbeide med Ikomm ved avholdelse av beredskapsøvelser. Videre ble revisor informert om at samhandling og beredskapsøvelser mellom de to aktørene er dokumentert i ny samhandlingsplan.

Revisjonen viser til revisjonskriteriet 4.2.1 som beskriver kommunens krav til IKT-leverandøren Ikomms beredskapsplan.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at *«leverandør skal sørge for jevnlig sikkerhetstesting av tjenesten».*

4.2.13 Indre Østfold kommune bør stille krav om aktiviteter ved terminering av kontrakt med IKT-leverandøren Ikomm, herunder tilbakeføring/flytting eller sletting av kommunens informasjon

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at:

«*leverandøren skal beskrive rutiner og/eller mekanismer for hvordan kundens data tilbakeleveres og slettes hvis kunden trekker seg ut av leverandørens skyplattform. Stikkord knyttet til scenariet:*

- *Kundens sikkerhetskopier*

- *Kundens brukerdata*
- *Eierskap til Tenant*
- *Overføring av eierskap til eAdm*

Listen er ikke utfyllende og bes fylles ut av leverandøren».

4.2.14 Indre Østfold bør stille krav til innsikt i enheter og programvare disponert av kommunen i IKT-leverandøren Ikomms IT-miljø

Revisor ble opplyst om at Indre Østfold kommune ikke spesifikt har stilt krav om dokumentasjon til PC-er o.l., men at dette er tilgjengelig gjennom Microsoft Intune portalen. Det fremkom i intervju at Indre Østfold kommune har mulighet til å hente ut rapporter.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold vil ha dokumentasjon av:

- *«Driftsplattformens arkitektur, programvare, maskinvare, redundans, fysisk sikkerhetstiltak, nødstrøm, fysiske føringsveier for datanettverk og etablering redundans og annen relevant informasjon om driftsplattformen»*
- *«Dokumentasjon av informasjonssikkerheten i driftsplattformen, slik som kryptering, brannmurløsning, antivirusløsning, segmenteringsløsninger, logging, autentiseringsløsninger mv.»*

4.2.15 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm gjennomfører periodiske gjennomganger for å kartlegge brukere og behov for tilgang

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt krav til tilgangsstyring (se for øvrig revisjonskriteriet 4.2.8 om tilgangsstyring). Videre har Indre Østfold stilt krav til Ikomm om at «*det ikke skal opprettes flere privilegerte leverandørkontoer enn nødvendig*».

Revisor ble opplyst om at Indre Østfold kommune benytter Visma eADM som en Identity and Accesss Management-løsning. Systemet oppretter og sletter brukere basert på kildedata fra kommunens personalsystem Visma HRM.

4.2.16 Indre Østfold kommune bør stille krav til at IKT-leverandøren Ikomm har fordelt ansvar og roller innen IKT-sikkerhet

Revisor ble i intervju informert om at Ikomm har fordelt roller og ansvar innen IKT-sikkerhet. Det fremkom i intervju at Ikomm ansetter ressurser med god kompetanse. Videre ble revisor informert om at Ikomm hadde lagt ut tre stillingsutlysninger innen overvåkningsløsninger samme dag som intervjuet ble gjennomført.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har satt følgende krav til roller:

- *«Leverandøren skal ha en Service Level Manager (SLM) som har det totale ansvaret for Leverandørens tjenesteleveranser. Rollen skal til enhver tid ha helthetsoversikt over Kundens situasjon og er Kundens eskaleringspunkt ved eventuelle avvik i forhold til avtalt leveranse.*
- *Vakttelefon og beredskap: Kunden skal ved alvorlige feil for kritiske leveranser/systemer kunne kontakte Vakttelefon 24/7 for bistand (feilmottak og feilretting ved A- og B-feil)».*

Videre fremgår det av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt krav om styringssystem for informasjonssikkerhet, hvor fordeling av ansvar og roller inngår.

I tillegg fremgår det av *Informasjonssikkerhetshåndboken* hvilke roller kommunen har internt. Se revisjonskriterium 5.2.2 for utfyllende informasjon.

4.2.17 Indre Østfold bør stille krav til at leverandøren Ikomm gjennomfører ekstern sikkerhetstesting hvert år

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav til sikkerhetstesting: *«Leverandør skal sørge for jevnlig sikkerhetstesting av tjenesten».*

Revisor ble opplyst om at Ikomm gjennomfører penetrasjonstester[8] årlig.

4.2.18 Indre Østfold kommune bør stille krav til at IKT-leverandøren Ikomm segregerer data fra andre kunder

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav til segregering av data:

> *«Kunden krever at kundens data til enhver tid holdes adskilt fra andre kunders data. Dette innebærer at ingen data skal være tilgjengelig eller kunne krysses mellom forskjellige kunder eller brukerkontoer».*

4.2.19 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm har sikkerhetsovervåkning for å avdekke sikkerhetshendelser som kan påvirke virksomheten

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav til sikkerhetsovervåkning:

> *«Driftsovervåkning:*
> *Kunden har krav om at Leverandøren overvåker og loggfører aktivitet i Kundens løsning. Leverandørens overvåkningssystem skal gi en god status på kundens løsning både for feilsøking og for generell statusrapportering på de tjenester som har avtalt SLA».*
>
> Det fremgår videre av *Leverandørens svar på kundens kravspesifikasjon*:
> *«Sikkerhetsovervåkning:*
> *Kunden har krav om at Leverandøren benytter sikkerhetsovervåkning i Microsoft Azure. Sikkerhetsovervåkning skal overvåke ressurser, aktiviteter og hendelser for å oppdage potensielle sikkerhetstrusler og uønsket aktivitet».*

Revisor ble opplyst om at kommunen hadde gjennomført strategisk samarbeidsmøte med eierkommunene (av Ikomm) 12.10.23 hvor det ble besluttet at eierkommunene ikke har økonomiske rammer til å si ja til å etablere sikkerhetsovervåkning som en tjeneste. Med sikkerhetsovervåkning menes sikkerhetssenter med 24/7-overvåkning. Revisor ble opplyst om at ny behandling av saken skal skje i februar 2024.

4.2.20 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm har rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav til varsling: *«Leverandøren skal ha effektive varslingsrutiner for sikkerhetsbrudd som gjør*

[8] Penetrasjonstest er en form for «etisk hacking» hvor man forsøker å finne sårbarheter i et teknisk system. Hensikten er å finne svakheter for å kunne redusere disse.

at Leverandøren raskt kan identifisere, rette og rapportere uønskede hendelser til Kunden». Revisor ble i intervju opplyst om at Ikomm har rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering.

Se revisjonskriteriet 4.2.19 for utfyllende informasjon om hvilke krav kommunen har stilt til sikkerhetsovervåkning.

4.2.21 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm har etablert et regime for sikkerhetsoppdatering

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav til sikkerhetsoppdatering: *«Leverandøren skal ha en dokumentert prosess for sikkerhetsoppdateringer som dekker alle komponenter i tjenesten».*

4.2.22 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm har etablert tilgangskontroll på flest ulike nettverksporter

Revisor ble opplyst om at Indre Østfold ikke har innført portsikkerhet på kommunens Cisco-utstyr[9], og at det ikke er stilt som et krav til IKT-leverandøren Ikomm. Revisor ble informert om at kommunen har kompetanse på Cisco-utstyr. Videre ble det opplyst at Indre Østfold har gjort vurderinger om at portsikkerhet kan være uegnet og skape problemer for brukerne. Revisor ble fortalt at Indre Østfold har fattet beslutningen på bakgrunn av:

- Økt kompleksitet og administrasjon
- Fleksibilitet
- Feilkonfigurasjon og nedetid
- MAC-adresseberegning
- Automatisk deaktivering av porter
- Behov for manuell reaktivering
- Kostnader.

Det ble videre opplyst at opplæring og bevisstgjøring, samt tofaktorautentisering er etablert som kompenserende organisatoriske tiltak. Videre har kommunen etablert brannmurer og Instruction Detection Systems som overvåker mistenkelig aktivitet. Kommunens nettverk er segmentert ved at de benytter VLAN.

4.2.23 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm benytter multi-faktor autentisering

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav til multifaktor-autentisering:

- *«Multifactor authentication (MFA): Beskriv hvilke Multifactor authentication (MFA) tjenester som tilbys og hvordan Kunden kan benytte denne for å sikre aksess ifm. Privilegert tilgang».*

Revisor ble videre opplyst om at tofaktorautentisering er en del av standard praksis som kommunen implementerer i alle avtaler. Dette kravet gjelder for alle brukere, herunder eksterne leverandører. Revisor ble opplyst om at muligheten for å benytte fellesbrukere er avviklet grunnet bruk av tofaktorautentisering. Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at *«Løsningene skal ikke bruke fellesbrukere. Alle registrerte brukere i tjenesten skal være unike og personlige. Leverandøren skal påse at dette kravet overholdes».*

[9] Cisco er en leverandør av nettverks- og sikkerhetsutstyr

4.2.24 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm har beskyttelsestiltak på e-post og nettleser

Revisor ble opplyst om at kommunen ikke har stilt eksplisitte krav til beskyttelsestiltak på e-post og nettleser. Årsaken til dette er at antivirus på PC-er, mobiltelefoner og lesebrett er obligatorisk i tjenesten Ikomm Cloud Basis. Revisor ble opplyst om at beskyttelsestiltakene på e-post og nettleser dekkes av kommunens krav til drift av klienter.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav:

- *«Kunden har behov for en administrert klientplattform med tilgang til Kundens applikasjoner og nettbaserte løsninger. Klientdrift skal være en del av Basis IT-tjeneste som skal leveres til alle ansatte og elever»*
- *«Leverandøren skal benytte Microsoft Intune for å sikre automatisk oppsett av klienter. Leverandøren skal tilby sikker drift av klienten når den er tilkoblet internett»*
- *«Drift av klienter vil omfatte: Administrative PC-er, Administrative lesebrett, Politiker lesebrett, Lærer PC-er, Elev PC-er».*

4.2.25 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm har plan for regelmessig sikkerhetskopiering av alle virksomhetsdata

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav til sikkerhetskopiering:

«Intervaller for sikkerhetskopier:

- *Leverandør skal dokumentere prosess for sikkerhetskopiering.*
- *Intervallene for sikkerhetskopiering skal være tilstrekkelig korte til at oppdragsgiver ikke blir vesentlig skadelidende i tilfeller der data må gjenopprettes.*

Test av sikkerhetskopi:

- *Leverandør skal jevnlig verifisere innhold i sikkerhetskopier og teste gjenoppretting av data for å verifisere kvaliteten på sikkerhetskopiene*

Oppbevaring av sikkerhetskopier:

- *Leverandør skal oppbevare sikkerhetskopier fysisk eller logisk atskilt fra produksjonsmiljøet.»*

4.2.26 Indre Østfold bør stille krav til at IKT-leverandøren Ikomm har plan og evne til å gjenopprette data

Se revisjonskriterium 4.2.25 for ytterligere informasjon om krav til sikkerhetskopiering.

Indre Østfold har ikke stilt eksplisitte krav til gjenoppretting av data i sine krav til Ikomm.

Revisor ble opplyst om at i eksisterende leveranseavtale med Ikomm, kjøper Indre Østfold kommune tilgang til sekundært datasenter. Videre ble revisor informert om at dersom Ikomm sitt primære datasenter blir utilgjengelig, kan applikasjonene kjøres fra det sekundære datasenteret. Det fremkom i intervju at kommunen benytter et sekundært datalager.

Indre Østfold kommune opplyste at de benytter seg av ekstra sikkerhetsløsning med blokkering av samtlige sikkerhetskopier slik at det ikke er mulig å endre innhold i sikkerhetskopiene (immutable). Kryptering og de-kryptering av sikkerhetskopiene gjøres av tredjepart.

4.2.27 Indre Østfold kommune bør stille krav til at IKT-leverandøren Ikomm bør benytte automatiserte verktøy for å håndtere skadevare (eksempelvis antivirus)

Indre Østfold kommune opplyste at de ikke har stilt eksplisitt krav til antivirus. Det fremgår av *Leverandørens løsningsbeskrivelse* at det benyttes Intune med endepunktssikkerhet.

Se revisjonskriterium 4.2.24 om krav til drift av klienter.

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt følgende krav:

- *«Sikring av datainnbrudd: Tjenesten skal være hensiktsmessig sikret mot ondsinnet kode og datainnbrudd. Kravet er et generelt krav om at leverandør skal ha gode sikkerhetstiltak på plass»*
- *«Patching og oppdatering: Leverandør skal ha en dokumentert prosess for sikkerhetsoppdateringer som dekker alle komponenter i tjenesten».*

4.2.28 *Aktuelt hvis Ikomm drifter både server og klienter for kommunen:* Indre Østfold kommune bør stille krav til at IKT-leverandøren Ikomm holder domenearkitekturen adskilt

Det fremgår av *Leverandørens svar på kundens kravspesifikasjon* at Indre Østfold kommune har stilt krav om at «*kundens data til enhver tid holdes adskilt fra andre kunders data*».

4.3 Vurderinger

Indre Østfold kommune har i noen grad samordnet sin beredskapsplan med IKT-leverandøren Ikomm	Gul

Revisor vurderer at avdekkede forhold i noen grad oppfyller revisjonskriteriet. Det er avdekket forbedringspotensial. Ikomm har tidligere deltatt i beredskapsøvelse med kommunen, men planene er etter vår oppfatning ikke samordnet. Det er allikevel positivt at det er planlagt mer samarbeid på dette området framover. Revisor anbefaler å fortsette samarbeidet og konkretisere samhandling i beredskapsplanene.

Indre Østfold kommune har utarbeidet skriftlige prosesser og prosedyrer for å ivareta sikkerhet i anskaffelses- og utviklingsprosesser	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut.

Revisor vurderer at kommunen har utarbeidet grundige prosesser og prosedyrer for å ivareta sikkerhet i anskaffelsesprosesser. *Informasjonssikkerhetshåndboken* er revidert i 2023, og inneholder blant annet kommunens styringssystem for informasjonssikkerhet som bygger på ISO/IEC 27001. Kommunen utvikler ikke programvare selv, og prosedyre for utviklingsprosesser vurderes dermed ikke som relevant.

Indre Østfold kommune har sikret innsyn i hvordan IKT-leverandøren Ikomm ivaretar sine forpliktelser ved å avtalefeste dette	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen og Ikomm har jevnlige møter.

Indre Østfold kommune følger opp at krav til IKT-leverandøren Ikomm blir etterlevd for å sikre at kontraktsforpliktelsene ivaretas	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av på bakgrunn av at kommunen og Ikomm har jevnlige møter.

Indre Østfold kommune har en detaljert kravspesifikasjon for IKT-tjenesten som skal tjenesteutsettes	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at Ikomm har en detaljert og utfyllende kravspesifikasjon til Ikomm.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm har et etablert styringssystem for informasjonssikkerhet	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om at Ikomm har etablert styringssystem i henhold til ISO/IEC 27001 eller tilsvarende.

Indre Østfold kommune har stilt krav om innsyn i sikkerhetsarkitekturen som benyttes av leverandøren	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om dokumentasjon av sikkerhetsarkitekturen Ikomm benytter.

Indre Østfold kommune har stilt krav til IKT-leverandøren Ikomm om tilgangsstyring, som inkluderer kryptering, aktivitetslogg, samt fysisk og logisk sikkerhet	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om tilgangsstyring, kryptering, fysisk sikring, sikring av datautstyr, logisk sikkerhet, overvåkning og logging.

Indre Østfold kommune har stilt krav om at underleverandører skal godkjennes av kommunen før de gis tilgang til kommunens informasjon	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om tillatelse ved bruk av underdatabehandler.

Indre Østfold kommune har stilt krav til IKT - leverandøren Ikomm at de har oversikt over hvem som skal ha innsyn i virksomhetens informasjon, hvor og hvordan denne skal behandles og lagres	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav til hvem som skal ha innsyn i kommunens informasjon, hvordan den skal behandles og lagres.

Indre Østfold kommune har stilt krav til IKT-leverandøren Ikomm om å etablere planverk for hendelseshåndtering – gjelder også plan for kommunikasjonskanaler	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn at kommunen har stilt krav om beredskapsplan og effektiv varslingsrutine.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm tester og øver på planer jevnlig	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om at Ikomm skal utføre jevnlig sikkerhetstesting av tjenesten.

Indre Østfold kommune har stilt krav om aktiviteter ved terminering av kontrakt med IKT-leverandøren Ikomm, herunder tilbakeføring/flytting eller sletting av kommunens informasjon	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om aktiviteter ved terminering av kontrakt.

Indre Østfold kommune har stilt krav til innsikt i enheter og programvare disponert av kommunen i IKT-leverandøren Ikomms IT-miljø	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav til innsikt i enheter og programvarer disponert av kommunen i IKT-leverandøren Ikomms IT-miljø.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm gjennomfører periodiske gjennomganger for å kartlegge brukere og behov for tilgang	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om tilgangsstyring og at kommunen benytter Visma eADM.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm har fordelt ansvar og roller innen IKT-sikkerhet	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at krav om fordeling av ansvar og roller er satt.

Indre Østfold kommune har i stor grad stilt krav til at leverandøren Ikomm gjennomfører ekstern sikkerhetstesting hvert år	Lysegrønn

Revisor vurderer at avdekkede forhold i stor grad oppfyller revisjonskriteriet. Det er imidlertid avdekket mindre forbedringspotensial knyttet til å presisere at ekstern sikkerhetstesting skal utføres årlig, istedenfor «jevnlig».

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm segregerer data fra andre kunder	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av kommunens krav om segregering av data.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm har sikkerhetsovervåkning for å avdekke sikkerhetshendelser som kan påvirke virksomheten	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av kommunens krav om sikkerhetsovervåkning for å avdekke sikkerhetshendelser.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm skal ha rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av kommunens krav om effektiv varslingsrutine, og informasjon om at Ikomm har rutiner for avvik- og sikkerhetsrapportering.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm har etablert et regime for sikkerhetsoppdatering	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av kommunens krav om sikkerhetsoppdatering.

Indre Østfold kommune har i stor grad stilt krav til at IKT-leverandøren Ikomm har etablert tilgangskontroll på flest ulike nettverksporter	Lysegrønn

Revisor vurderer at avdekkede forhold i stor grad oppfyller revisjonskriteriet.

Revisor vurderer at kommunen ikke har stilt eksplisitt krav om tilgangskontroll på nettverksporter, men har gjort en grundig vurdering av om det skal etableres et slikt krav. Blant annet er nettverket segmentert ved bruk av VLAN og brannmur og IDS brukes for å blokkere og oppdage mistenkelig trafikk. Revisor opplever at kommunens vurdering er grundig.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm benytter multi-faktor autentisering	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av kommunens krav om multi-faktor autentisering.

Indre Østfold kommune har i stor grad satt krav om beskyttelsestiltak på e-post og nettleser	Lysegrønn

Revisor vurderer at avdekkede forhold i stor grad oppfyller revisjonskriteriet. Det er imidlertid avdekket et mindre forbedringspotensial. Tjenestebeskrivelsen inneholder en løsning som i stor grad dekker kravet. Kommunen bør imidlertid stille dette som et eksplisitt krav.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm har plan for regelmessig sikkerhetskopiering av alle virksomhetsdata	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av kommunens krav om regelmessig sikkerhetskopiering.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm har plan og evne til å gjenopprette data	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at eksisterende leveranseavtale inneholder plan for gjenoppretting av data

Indre Østfold kommune har i stor grad stilt krav om at IKT-leverandøren Ikomm bør benytte automatiserte verktøy for å håndtere skadevare (eksempelvis antivirus)	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut. Det er ikke stilt som eksplisitt krav, men dette er oppgitt å være fordi tjenestebeskrivelsen allerede inneholder en løsning dekker kravet. Kriteriet dekkes videre indirekte av krav til at NSMs grunnprinsipper skal følges av leverandøren.

Indre Østfold kommune har stilt krav til at IKT-leverandøren Ikomm holder domenearkitekturen adskilt	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at kommunen har stilt krav om at Ikomm skal holde kommunens data adskilt fra andres.

4.4 Konklusjon og anbefalinger

Det skilles mellom krav som *må (regulatoriske krav)* og *bør* (beste praksis) gjennomføres (viser til 3.2 om revisjonskriterier for ytterligere informasjon). Fakta, omtalt som revisjonsbevis vurderes opp mot revisjonskriteriene, og disse vurderingene danner grunnlaget for de konklusjoner som trekkes.

Revisor konkluderer, basert på den gjennomførte revisjonen, med at Indre Østfold kommune har stilt tilstrekkelige sikkerhetskrav til IKT-leverandøren Ikomm, og at kommunen følger opp disse kravene på en adekvat måte. Det er ikke avdekket alvorlige avvik knyttet til problemstilling 1.

Indre Østfold kommune jobber systematisk og grundig med teknisk informasjonssikkerhet. Kravene stilt fra kommunen til Ikomm er detaljerte og i hovedsak dekkende. Av de funnene som ikke er oppfylt har kommunen andre adekvate løsninger. Kravene følges opp i faste møter med leverandøren. Det er funn som viser manglende samordning av beredskapsplanene mellom kommunen og leverandøren. Revisor er imidlertid informert om at denne prosessen er påstartet. Det er identifisert enkelte mangler på krav som bør vurderes for å øke informasjonssikkerheten ytterligere.

Basert på revisors vurderinger og konklusjon anbefaler revisor at Indre Østfold kommune bør:

Tiltak relatert til problemstilling 1:	Prioritet (1-3)
Samordne beredskapsplanen med Ikomm	1
Stille eksplisitte krav om beskyttelsestiltak på e-post og nettleser	2
Planlegge for en fremtidig revisjon av Ikomms etterlevelse av avtalekravene	3

Anbefalingene er bygd opp ved følgende system:

1. Må rettes på snarest
2. Bør rettes på, men korrigerende tiltak kan skyves ut i tid
3. Bør vurderes rettes på, og korrigerende tiltak kan skyves ut i tid.

Revisor gjør oppmerksom på at dette ikke er ment som en fullstendig liste over nødvendige tiltak, men etter revisors vurdering de mest vesentlige. Kommunen må selv vurdere hva som er nødvendige tiltak til enhver tid. Det er således ingen garanti at revisjonskriteriene er etterlevd ved å innføre de anbefalte tiltakene. Blant annet vil dette avhenge av ledelsens etterfølgende oppfølging av tiltakene for å sikre at de har den ønskede effekten.

5 TILSTREKKELIG OPPLÆRING, BEVISSTHET OG KOMPETANSE BLANT ANSATTE

Problemstilling 2: Har kommunens ansatte fått tilstrekkelig opplæring, sikkerhetsbevissthet og kompetanse til å ivareta sine primæroppgaver?

5.1 Revisjonskriterier

I henhold til ISO/IEC 27001 bør kommunen sikre at kompetansekrav innen informasjonssikkerhet er fastsatt. Videre bør kommunen sikre at alle ansatte er klar over og oppfyller sitt ansvar innen informasjonssikkerhetsarbeidet. Alle ansatte bør bli bevisstgjort, få opplæring, samt få regelmessige oppdateringer i organisasjonens interne føringer som er av relevans for arbeidet. Basert på føringer fra ISO/IEC 27001 vurderes det at ansatte bør få tilstrekkelig opplæring for å bli bevisstgjort kommunens behov og målsettingskrav.

I henhold til ISO/IEC 27001 bør kommunen sikre at ansatte er kjent med rutiner og retningslinjer innen informasjonssikkerhet, og at de som innehar ansvar og roller er kjent med dette. Videre fremgår det av ISO/IEC 27001 og Datatilsynets veileder at ansatte bør få opplæring for å sikre at de er kjent med og i stand til å etterleve rutiner for informasjonssikkerhet. Det tolkes derfor at kommunen bør ha opplæring for å sikre at ansatte kjenner retningslinjene for informasjonssikkerhet på arbeidsplassen.

Digitaliseringsdirektoratet uttrykker at alle ansatte har et ansvar for informasjonssikkerhet. Ansvaret innebærer å inneha kompetanse om behandling av informasjon, aktuelle risikoer, samt konsekvensomfanget ved en eventuell uønsket hendelse. Videre bør kommunen ha rutiner for avvikshåndtering for å være i henhold til ISO/IEC 27001 og Datatilsynet. Digitaliseringsdirektoratet viser til at virksomheter bør gi ansatte opplæring om interne rutiner for varsling av informasjonssikkerhetshendelser. Det tolkes dermed at kommunen bør legge til rette for at de ansatte får den nødvendige kompetansen innen informasjonssikkerhet og varsling.

NSMs grunnprinsipper for IKT-sikkerhet viser til behov for opplæring av personell etter evaluering av IKT-hendelser/øvelser. Det tolkes dermed at kommunen bør utføre justeringer i opplæringsmateriellet etter behov.

Det skilles mellom krav som *må* og *bør* gjennomføres. Revisor benytter begrepet *må* ved lovkrav, mens *bør* benyttes ved råd, retningslinjer eller anbefalinger.

5.1.1 Revisjonskriterier for problemstilling 2

Indre Østfold bør:

- sikre at kompetansekrav innen informasjonssikkerhet (herunder IKT-sikkerhet) er fastsatt (ISO/IEC 27001)
- sikre at ansvar og roller innen informasjonssikkerhet (herunder IKT-sikkerhet) er kjent i kommunen og at de som innehar roller er kjent med disse (ISO/IEC 27001)
- ha opplæringsprogram for å sikre at ansatte er kjent med og er i stand til å etterleve rutiner og retningslinjer innen informasjonssikkerhet (herunder IKT-sikkerhet) (Datatilsynets veileder – Informasjonssikkerhet og internkontroll, ISO/IEC 27001 og Digdir – Kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet).
- sikre at alle ansatte kjenner til hvilken informasjon de behandler og hvilke krav som stilles til arbeidet (Digdir - Kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet)

- sikre at alle ansatte har en tilstrekkelig forståelse for trusler og risiko for å forstå hvorfor arbeidsoppgavene bør utføres på en sikker måte (Digdir - Kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet)
- legge til rette for at ansatte har en forståelse av at uønskede informasjonssikkerhetshendelser kan hindre de i utførelse av arbeidet, eller få konsekvenser for andre parter (Digdir - Kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet
- ha rutiner for rapportering til ledere og ansvarlige for sikkerhetshendelser, avvikshåndtering og egenkontroll (ISO/IEC 27001)
- gi ansatte opplæring om interne rutiner for varsling av informasjonssikkerhetshendelser (Digdir - Kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet)
- gi opplæring av personell etter evaluering av IKT-hendelser/øvelser (NSMs grunnprinsipper for IKT-sikkerhet)

5.2 Datagrunnlag

5.2.1 Indre Østfold kommune bør sikre at kompetansekrav innen informasjonssikkerhet (herunder IKT-sikkerhet) er fastsatt

Det fremkom i intervju at kommunen ikke har fastsatt kompetansekrav til ansatte. I *informasjonssikkerhetshåndboken* fremgår det at det er etablert kompetanseplan for informasjonssikkerhet som beskriver hvilken opplæring de ansatte skal gjennomgå. I planen fremgår det at opplæringen skal gi alle ansatte tilstrekkelig informasjon om informasjonssikkerhet og gjøre de oppmerksomme på mulige trusler som kan påvirke den enkelte.
Det fremgår ikke av dokumentasjon at det er fastsatt kompetansekrav til utpekte sikkerhetsroller.
Det var 82 % som svarte *«i ganske stor grad eller i stor grad»* på spørsmål om de opplever at kommunen stiller tydelige krav om informasjonssikkerhet. På spørsmål om opplæringen har gitt ansatte kunnskap om hvilke forventninger ledelsen/arbeidsgiver har til de innen digital sikkerhet, svarte 76,3 % *«i ganske stor grad eller i stor grad»,* og 13,1 % svarte *«i ganske liten grad eller i liten grad».*

5.2.2 Indre Østfold kommune bør sikre at ansvar og roller innen informasjonssikkerhet

Det fremgår av *Informasjonssikkerhetshåndboken* at kommunen har fordelt roller med tilhørende ansvarsbeskrivelse. Følgende roller fremgår i *Informasjonssikkerhetshåndboken*:

Kommunedirektør	Sikkerhetsansvarlig	Behandlingsansvarlig	Eier av informasjonssikkerhetshåndbok	Ledelsen
Systemeier	Databehandler	Operativ systemeier	Systemforvalter	Superbrukere
Brukere	Elever	Konsulenter	IKT-brukerstøtte	Sikkerhetsrådgiver

Tabell 3, Oversikt over roller

Det fremgår av *informasjonssikkerhetshåndboken* at det er fordelt roller og ansvar knyttet til ulike kompetansehevingstiltak innen IKT-sikkerhet. Rollene og deres ansvar er definert slik:

- *«Nærmeste leder: sikre at ansatte har gjennomført relevante kompetansetiltak*
- *Sikkerhetsansvarlig: innholdet i kompetanseplan, samt initiere og gjennomføre opplæring».*

Revisor ble informert om at ledere skal lese informasjonssikkerhetshåndboken. Det fremkom i intervju at også ansatte bør gjennomgå og signere at de har lest informasjonssikkerhetshåndboken. Både ledere og ansatte signerer i systemet *Compilo* etter gjennomføring. I ett av intervjuene ble det gjennomført en stikkprøve hvor revisor fikk innsikt i hvordan signering i systemet gjennomføres. De fleste informantene kjente til sitt ansvar for å gjennomgå informasjonssikkerhetshåndboken, men en informant kjente ikke til om informasjonssikkerhetshåndboken var tilgjengelig for alle ansatte.

Revisor fikk innsikt i systemet *Digiorden* som viser de ulike rollene kommunen opererer med knyttet til informasjonssikkerhet.

Det fremkom i intervju at ledere også kan delta på fysiske kurs om IKT-sikkerhet. En informant fortalte at vedkommende ikke hadde vært på lederkurs i informasjonssikkerhet siden personen startet i jobben, mens en annen informant fortalte at det ofte er lavt oppmøte på disse kursene.

I intervjuene svarte samtlige informanter at de er kjent med hvem i kommunen som til daglig har informasjonssikkerhet som fokusområde. Det var enkelte informanter som trakk frem kommunedirektøren sin overordnede rolle i arbeidet. Det fremkom i intervju at det trolig er en del ansatte ikke kjenner til hvem som besitter ansvaret. Videre opplyste de fleste informantene at de hadde inntrykk av at de ansatte var kjent med sitt ansvar for å ivareta informasjonssikkerhet i kommunen.

I spørreundersøkelsen fikk ansatte spørsmål om hvem de mener har ansvar for informasjonssikkerhet i kommunen, hvorav 92,1 % svarte *«alle i kommunen»*. Spørreundersøkelsen viste også at opplæringen *i stor grad* hadde gjort de fleste (81,5 %) oppmerksom på at alle ansatte har et selvstendig ansvar for informasjonssikkerheten i kommunen.

5.2.3 Indre Østfold kommune bør ha opplæringsprogram for å sikre at ansatte er kjent med og er i stand til å etterleve rutiner og retningslinjer innen informasjonssikkerhet (herunder IKT-sikkerhet)

I *Informasjonssikkerhetshåndboken* fremgår det at Indre Østfold kommune skal ha opplæring innen et utvalg temaer ved å benytte metoder som:

- Kurs: Elektroniske kurs, interne kurs, eksterne kurs, seminarer og webinarer
- Møter: Medarbeidersamtaler, avdelingsmøter, ledermøter.

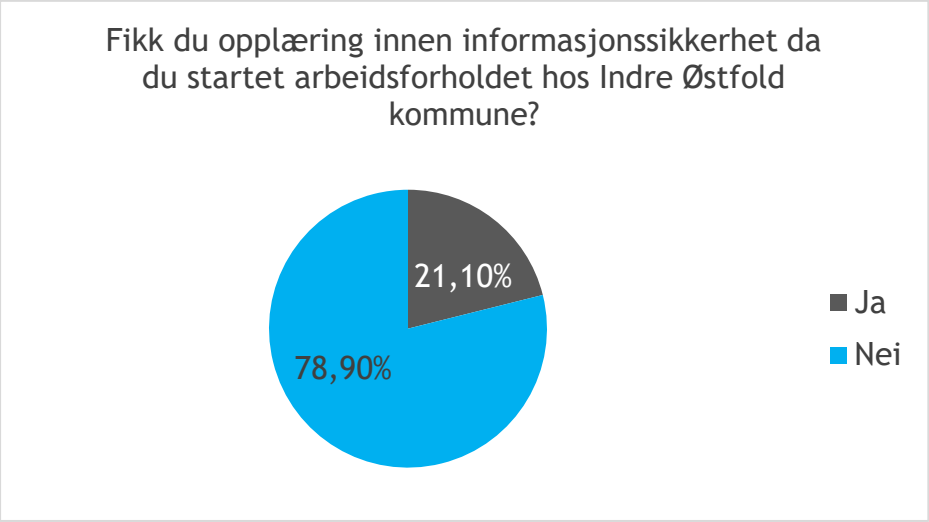
De ulike temaene som står oppført i *Informasjonssikkerhetshåndboken* var følgende:

- *«Unngå å klikke på ukjente lenker*
- *Forbedre praksis for passord*
- *Bevisstgjøre risikoen ved bruk av trådløse wifi-nettverk*
- *Skape en kultur hvor det er trygt å si ifra».*

Videre fremgår det av *Informasjonssikkerhetshåndboken* at nye ansatte og ledere skal gå gjennom informasjonssikkerhetshåndboken, samt gjennomføre andre kurs innen temaet. *Se for øvrig ytterligere redegjørelse for dette under revisjonskriteriet 5.2.2 informasjon om signering ved gjennomgang av informasjonshåndboken.*

Det fremgår av *sikkerhetsmåneden 2021, 2022 og 2023* at Indre Østfold kommune har gjennomført årlig opplæring av ansatte og ledere innen informasjonssikkerhet. I sikkerhetsmåneden benyttes e-post, intranett, plakater og nanoleksjoner for å bevisstgjøre kommunens ansatte. Dette bekreftes i samtlige intervjuer. Videre viser *Opplæring informasjonssikkerhet og personvern 6 jan – ledelsen* selve opplæringsmateriellet ledelsen har fått innen temaet. Det fremkom i intervju at temaet i tillegg blir tatt opp på ledermøter.

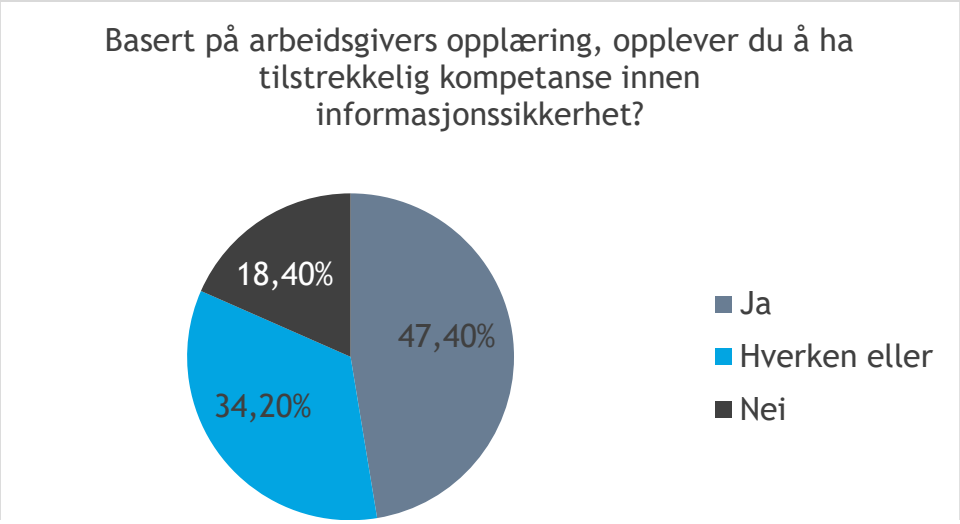
I spørreundersøkelsen ble det spurt om hvor ofte arbeidsgiver tilbyr opplæring innen informasjonssikkerhet til ansatte, hvorav 84,2 % svarte enten «*årlig eller halvårlig*». På spørsmål om ansatte fikk opplæring ved oppstart av arbeidsforholdet hos Indre Østfold kommune (figur 2) svarte respondentene følgende:



Figur 2, Opplæring ved start av arbeidsforholdet – Kilde: spørreundersøkelsen til ansatte i Indre Østfold

Svarene viser at en stor andel av de ansatte ikke fikk opplæring ved starten av arbeidsforholdet.

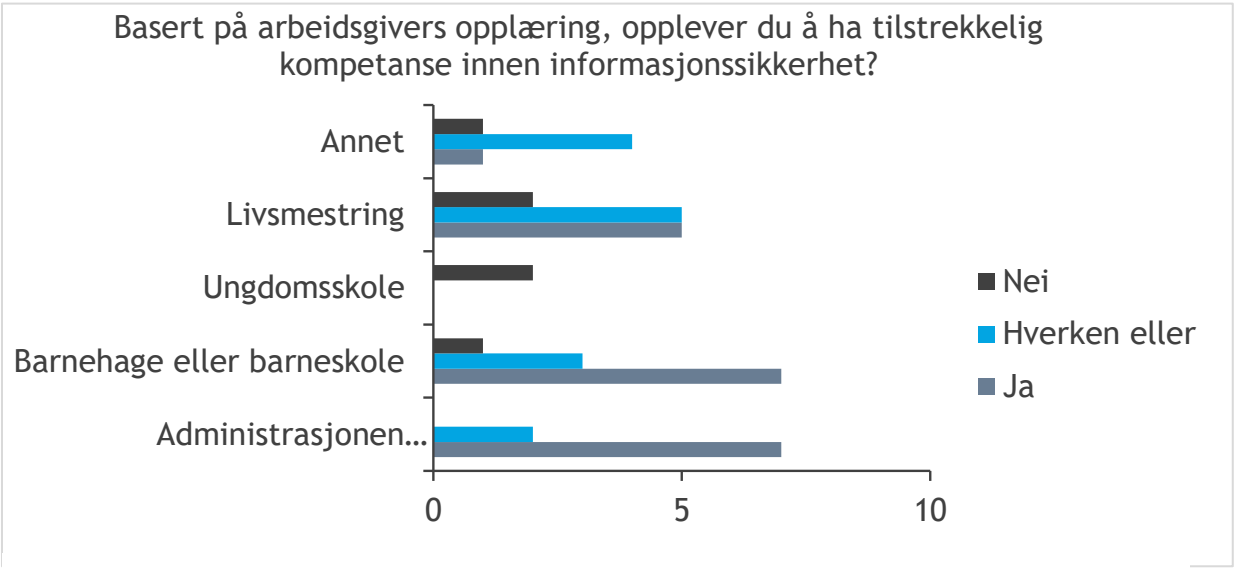
I spørreundersøkelsen ble ansatte videre spurt om de opplevde nanokursene under sikkerhetsmåneden som relevante, hvorav 79 % oppga at de var relevante, mens 7,9 % svarte *«i liten grad»*. På spørsmålet *«Basert på arbeidsgivers opplæring, opplever du å ha tilstrekkelig kompetanse innen informasjonssikkerhet»*, svarte 47,4 % *«Ja»,* 34,2 % *«Hverken eller»,* mens 18,4 % svarte *«Nei» (figur 3)*.



Figur 3, Opplevelse av tilstrekkelig kompetanse etter opplæring - Kilde: spørreundersøkelsen til ansatte i Indre Østfold

Spørreundersøkelsens funn peker på at ca. halvparten opplever å ha tilstrekkelig kompetanse innen informasjonssikkerhet, mens resterende svarer «hverken eller» eller «nei».

Revisor utførte en analyse for å vurdere om det var ulike svar mellom seksjonene på spørsmål om de ansatte opplevde å ha tilstrekkelig kompetanse innen informasjonssikkerhet (figur 4):



Figur 4, Opplevelse av tilstrekkelig kompetanse fordelt på seksjoner - Kilde: analyse utført av BDO

Av analysen fremkom det at det var større grad av opplevelse av tilstrekkelig kompetanse innen informasjonssikkerhet i seksjonene administrasjon, barnehage eller barneskole, og livsmestring. Analysen ga imidlertid lite grunnlag for å konkludere om betydelige forskjeller mellom seksjonene.

Mellom 60-80 % av respondentene svarte *«i stor grad eller i svært stor grad»* på spørsmål om opplæringen har gjort de oppmerksom på ulike informasjonssikkerhetstiltak som kan øke deres evne til å forhindre risikoen for menneskelig svikt. Spørsmålene handlet blant annet om:

- De skiller mellom passord som benyttes privat og i arbeidssammenheng (63,1 % *svarte i svært stor grad eller i stor grad*)
- De kjenner til at informasjon fra deres arbeidsdag kan komme på avveie ved manglende sikkerhet (76,1 % svarte *i svært stor grad eller i stor grad*)
- De låser digitale enheter når de forlater dem (79 % svarte *i svært stor grad eller i stor grad*)
- Hvordan de kan undersøke om en lenke eller et vedlegg er trygt før de åpner det (84,2 % svarte *i svært stor grad eller i stor grad*)

Videre svarte 81,6 % *«i stor grad eller i svært stor grad»* på spørsmål om at informasjonssikkerhet også gjelder ved arbeid på eksterne lokasjoner.

Det ble bekreftet i intervju at flere av informantene opplevde opplæringsmateriellet som relevant og at opplæringen har hatt effekt. Revisor ble opplyst av enkelte ledere og ansvarlige innen IKT-sikkerhet i kommunen at de har opplevd økt årvåkenhet fra de ansatte da de tar kontakt ved eventuell mistanke om hendelser.

Det fremgår videre av *sikkerhetsmåneden 2022 og 2023* at omtrent 80 % av de ansatte ikke gjennomfører opplæringen i forbindelse med sikkerhetsmåneden. Revisor ble informert i intervju at omtrent 20 % fullfører e-læringsmodulene i informasjonssikkerhet. I intervjuene ble følgende årsaker til manglende gjennomføring av opplæring trukket frem:

- Opplæringen er sentrert til sikkerhetsmåneden og noen opplever dette noe intensivt.
- Manglende oppfølging fra ledere om å påse at ansatte fullfører opplæringen.
- Det er variasjoner knyttet til hvorvidt ansatte er kjent med retningslinjer fra informasjonssikkerhetshåndboken og tilhørende opplæring.
- Informasjonssikkerhetshåndboken som opplæringsverktøy kan være ha mindre effekt ettersom det er mye informasjon og ansatte aktivt må oppsøke den.

Informantene påpekte følgende forbedringspotensial i intervju:

- Innlemme opplæring om informasjonssikkerhet som et sjekkpunkt i virksomhetsstyringsverktøyet *«Framsikt»* for å sikre at det blir gjennomgått
- Gjennomføre bevisstgjørende tiltak om informasjonssikkerhet i flere intervaller i løpet av ett år
- At flere ledere kan benytte seg av tilbudet hvor IKT-sikkerhetspersonell fra kommunen kan komme ut i enhetene og snakke om temaet.

5.2.4 Indre Østfold kommune bør sikre at alle ansatte kjenner til hvilken informasjon de behandler og hvilke krav som stilles til arbeidet

Se revisjonskriterium 5.2.3 for ytterligere revisjonsbevis om kommunens generelle opplæringsarbeid innen IKT-sikkerhet.

I spørreundersøkelsen ble de ansatte spurt om i hvilken grad opplæringen fra arbeidsgiver har gitt kunnskap om at informasjon de behandler som er unntatt offentlighet krever ekstra beskyttelse. Det var 73,7 % som svarte *«i stor grad eller svært stor grad»*, og 18 % *«i liten grad eller i svært liten grad»*. Videre svarte 76,3 % *«i stor grad eller svært stor grad»* på om opplæringen hadde gjort de oppmerksom på at informasjon fra deres arbeidsdag kan komme på avveie ved manglende sikkerhet. På samme spørsmål svarte 15,8 % *«i liten grad eller i svært liten grad».*

I intervjuene fremkom det at ansatte har meldt fra om tilfeller hvor de har behandlet informasjonen feil, eller oppdaget at de har fått tilgang til informasjon som burde vært utilgjengelig for dem. Flere informanter fortalte at ansatte fremstår opplyst og årvåkne, men at enkelte mangler kompetanse om temaet.

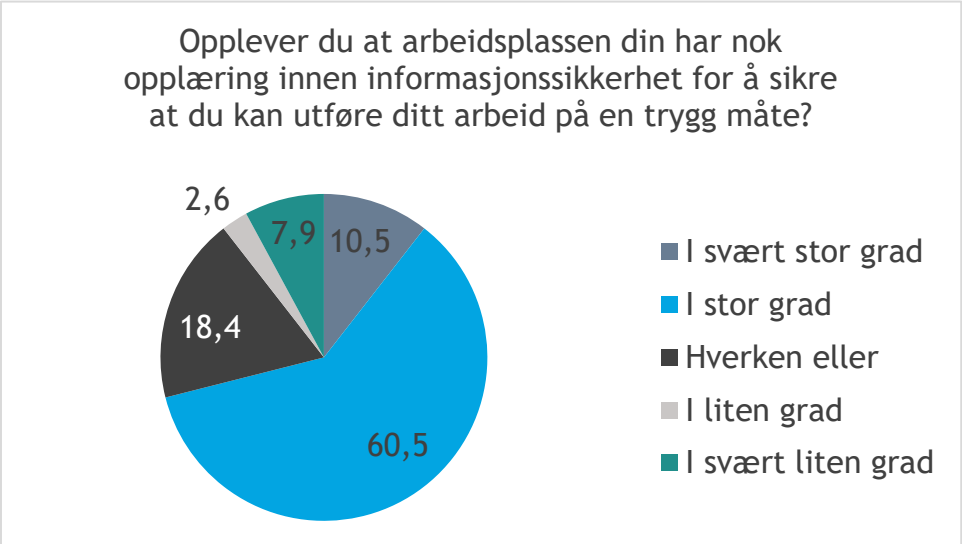
Enkelte informanter opplyste at de i sin lederrolle arrangerer ytterligere kurs hvis de identifiserer mangler i kommunens ulike enheter.

5.2.5 Indre Østfold kommune bør sikre at alle ansatte har en tilstrekkelig forståelse for trusler og risiko for å forstå hvorfor arbeidsoppgavene bør utføres på en sikker måte

Se revisjonskriterium 5.2.3 for ytterligere revisjonsbevis om kommunens generelle opplæringsarbeid innen IKT-sikkerhet.

Det fremgår av *informasjonssikkerhetshåndboken* at nye ledere og ansatte skal få opplæring innen relevante trusler, risikoer og muligheter. Videre er revisor opplyst om at kommunen med jevne mellomrom gjennomfører phishing-kampanjer[10] for å bevisstgjøre de ansatte.

På spørsmål om opplæringen har gjort ansatte oppmerksom på ulike dagsaktuelle hendelser, svarte rundt 70 % *«i stor grad eller i svært stor grad».* Videre svarte omtrent halvparten at opplæringen har gitt ansatte kunnskap om dagsaktuelle trusler som er relevant for Indre Østfold kommune. På spørsmål om de ansatte har fått nok opplæring innen informasjonssikkerhet for å sikre at de utfører arbeidet på en trygg måte, svarte de følgende (figur 5):



Figur 5, Opplærings påvirkning av trygg arbeidsutførelse - Kilde: spørreundersøkelsen til ansatte i Indre Østfold

Spørreundersøkelsens resultater viste at en stor andel (71 %) vurderer at de får nok opplæring innen informasjonssikkerhet, mens en mindre andel svarer «hverken eller» (18,4 %) eller «i liten grad» eller «svært liten grad» (10,5 %)

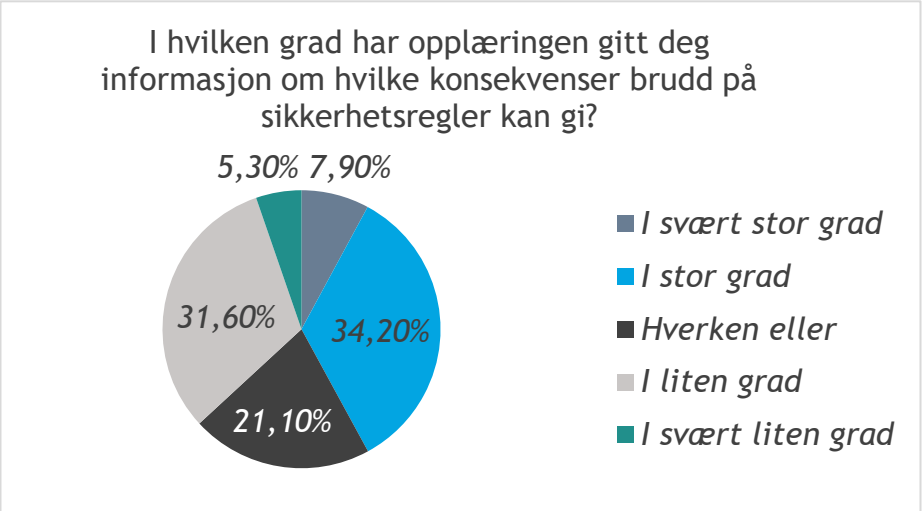
Flere informanter opplyste at mange ansatte er kjent med aktuelle trusler og risikoer, og at de trolig får denne kunnskapen fra opplæring, men også andre informasjonskanaler, som media. Enkelte informanter opplyste om kommunens bruk av informasjonsdeling på intranett om dagsaktuelle hendelser knyttet til informasjonssikkerhet, samt informasjon om hva ansatte bør være oppmerksomme på.

[10] Phishing-kampanje er øvelser hvor en virksomhet simulerer svindel på e-post eller meldinger hvor de utgir seg for å være en legitim kilde, med mål om å teste ansattes kunnskap og håndteringsevne knyttet til svindelmetoden.

5.2.6 Indre Østfold kommune bør legge til rette for at ansatte har en forståelse av at uønskede informasjonssikkerhetshendelser kan hindre de i utførelse av arbeidet, eller få konsekvenser for andre parter

Se revisjonskriterium 5.2.3 for ytterligere revisjonsbevis om kommunens generelle opplæringsarbeid innen IKT-sikkerhet.

Det fremgår av O*pplæring informasjonssikkerhet og personvern 6 jan – ledelsen* at ledelsen har fått opplæring om mulig konsekvensomfang ved eventuelle hendelser. På spørsmål om hvilken grad opplæringen har gitt ansatte kunnskap om hvilke konsekvenser brudd på sikkerhetsregler svarte de ansatte følgende, se figur 6 nedenfor.



Figur 6, Konsekvenser ved brudd på sikkerhetsregler - Kilde: spørreundersøkelsen til ansatte i Indre Østfold

Funnene fra spørreundersøkelsen viste en fordeling der omtrent halvparten opplever at opplæringen har gitt kunnskap om konsekvenser, mens resterende halvpart mener det motsatte.

Revisor ble opplyst at ansatte har ulik innsikt i konsekvensomfanget ved hendelser. Det ble uttrykt i intervju at det er utfordrende for ansatte å vurdere hva som er sikker praksis og hvilke sikkerhetstiltak som er ansett som tilstrekkelige. Dette fremgår av tekstsvar i spørreundersøkelsen hvor flere ansatte påpekte et behov for mer informasjon om hva som er «sikkert nok».

5.2.7 Indre Østfold kommune bør ha rutiner for rapportering til ledere og ansvarlige for sikkerhetshendelser, avvikshåndtering og egenkontroll

Det fremgår av *Informasjonssikkerhetshåndboken* at Indre Østfold kommune har rutiner for avviksrapportering i systemet *Compilo*.

I *Kontroll av avvikshåndtering* er følgende ansvarsoppgaver definert:

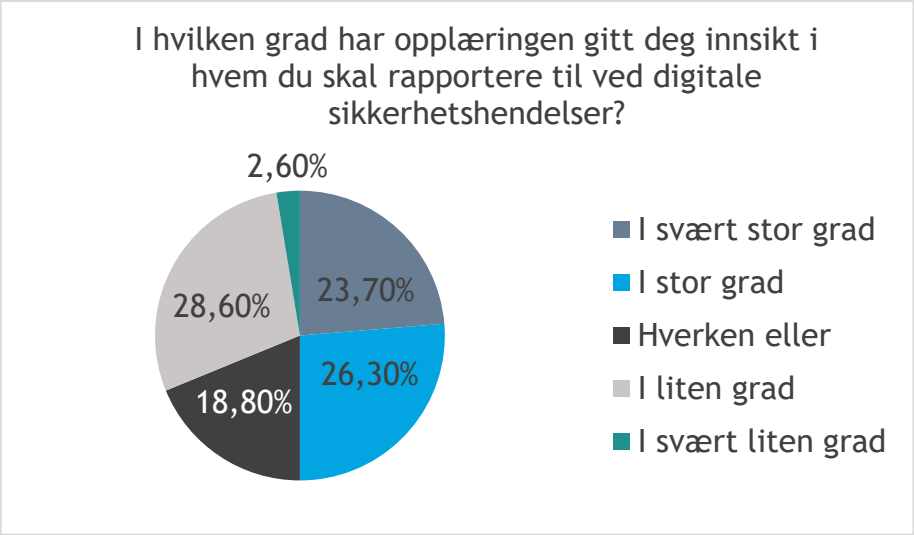
- *«Ansatte har ansvar for å melde avvik dersom informasjon ikke blir håndtert i samsvar med policy, eller om informasjon kommer på avveie*
- *Ledere har ansvar for oppfølging og iverksetting av tiltak*
- *Sikkerhetsansvarlig har ansvar for å etablere en samlet oversikt over alle avvik knyttet til brudd på informasjonssikkerheten.»*

Revisor er opplyst om at ledere skal undersøke om det forekommer avvik og dokumentere avviksoppfølgingen. Videre opplyste informantene at avvik automatisk blir sendt videre oppover i systemet ved fravær av behandling, eller ved behov for behandling på et høyere nivå.

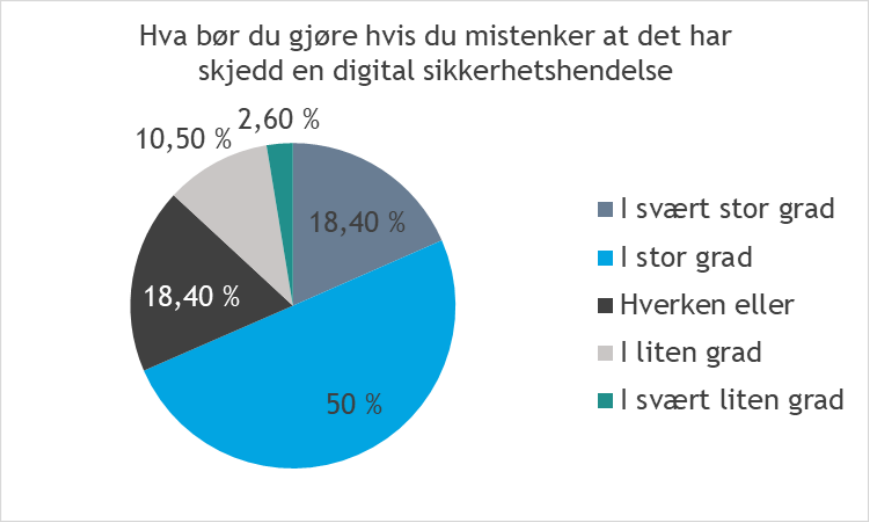
5.2.8 Indre Østfold bør gi ansatte opplæring om interne rutiner for varsling av informasjonssikkerhetshendelser

Det fremgår av *Informasjonssikkerhetshåndboken* at nye ledere og nyansatte får opplæring om registrering av avvik i kvalitetssystemet *Compilo*. Ledere er videre ansvarlig for å sikre at ansatte får opplæring og at de setter seg inn i gjeldende regler og prosedyrer. Revisor ble informert om at Indre Østfold kommune har opplyst de ansatte om viktigheten av varsling av informasjonssikkerhetshendelser og at dette var en del av opplæringen i sikkerhetsmåneden i 2023.

I spørreundersøkelsen fremkom det at 84,3 % ville varslet sin nærmeste leder og/eller IKT-brukerstøtte ved mistanke om digitale sikkerhetstruende hendelser. Som det fremgå av figur 7 og 8 ble ansatte spurt i hvilken grad opplæring fra arbeidsgiver har gitt de kunnskap om varsling og rapportering. De ansatte svarte følgende:



Figur 7, Rapportering digitale sikkerhetshendelser - Kilde: spørreundersøkelsen til ansatte i Indre Østfold

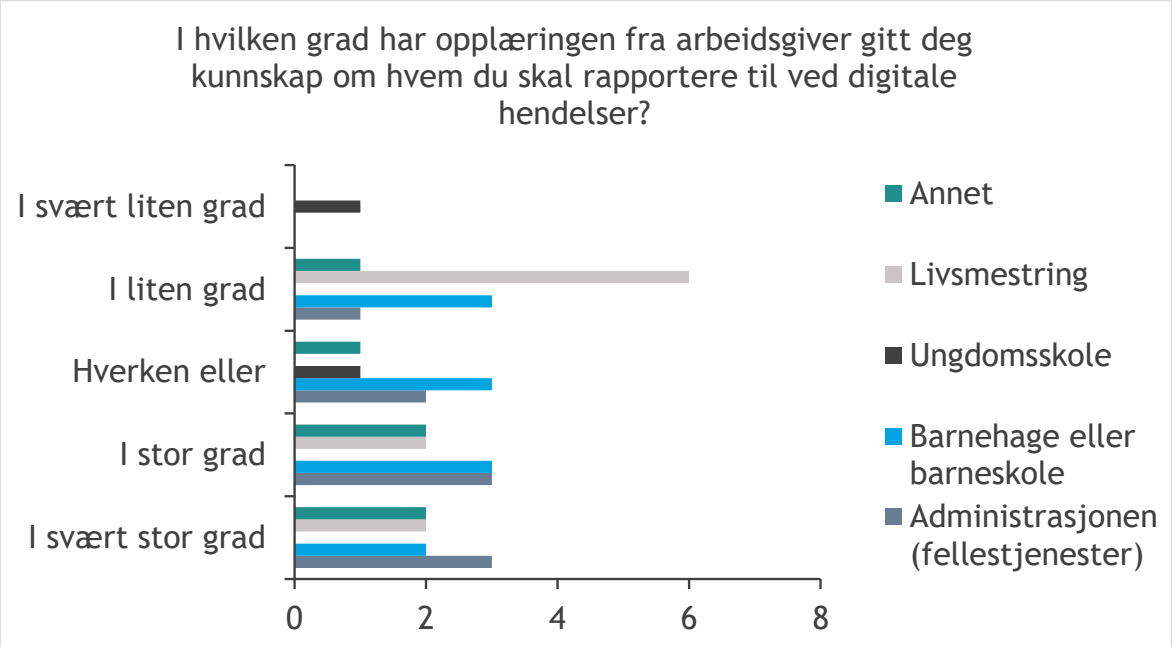


Figur 8, Grad av kjennskap til hva de skal gjøre ved en digital sikkerhetshendelse - Kilde: spørreundersøkelsen til ansatte i Indre Østfold

Svarene fra figur 7 viste en spredd fordeling på spørsmål om opplæringen har gitt innsikt i hvem ansatte skal rapportere til. Figur 8 viste at en stor andel (68,4 %) visste hva de bør gjøre ved mistanke om en digital sikkerhetshendelse.

Svarene fra *Sikkerhetskulturskartlegging 2023* viste at omtrent 30-50 % (fra seksjonene livsmestring, skole og barnehage) svarte at de ikke kjente til hvordan brudd på informasjonssikkerhet skal rapporteres.

Revisor utførte en analyse for å vurdere om det var ulike svar mellom seksjonene på spørsmål om ansatte hadde kunnskap om hvem en skulle rapportere til ved digitale hendelser:



Figur 9, Opplæring har gitt kunnskap om rapportering - fordelt på seksjoner Kilde: analyse utført av BDO

Analysen viste en relativ jevn fordeling mellom de ulike seksjonene på spørsmål om opplæring har gitt kunnskap om hvem de skal rapportere til. Det fremkom at særlig seksjon livsmestring opplevde liten grad av kunnskap om rapportering.

Informantene som innehadde lederroller, kjente til at de var ansvarlig for avvikshåndtering. Videre opplyste informantene at det ikke var gjennomført egen opplæring for avvikshåndtering i de ulike avdelingene. Det fremkom i intervju at hyppigheten av rapportering av avvik varierer. Enkelte informanter opplyste at ansatte rapporterte jevnlig, og andre opplyste at avvik sjeldent rapporteres.

5.2.9 Indre Østfold bør gi opplæring av personell etter evaluering av IKT-hendelser/øvelser

Det fremgår av *Informasjonssikkerhetshåndboken* at det «*må etableres en metode for å måle at kompetansen faktisk blir høyere*». Videre fremgår det at kommunen skal arrangere minimum en phishingkampanje årlig, i tillegg til andre øvelser i sammenheng med gjeldende trusselbilde.

Det fremgår av *sikkerhetsmåneden 2021, 2022 og 2023* at kommunen har hatt en nedgang i «vellykkede» phishing-forsøk. Videre fremgår det av *sikkerhetsmåneden 2021* at personer som trykket på lenken i phishing-testen ble plukket ut til å gjennomføre opplæring innen temaet. Videre utførte Indre Østfold kommune en sikkerhetskulturkartlegging i 2023. Revisor ble informert om at formålet med kartleggingen var å få innsikt i hvordan menneskelige faktorer påvirker den digitale sikkerheten i kommunen.

Revisor er opplyst om at Indre Østfold kommune har identifisert forbedringspotensialet når det gjelder samordning mellom Ikomm AS og Indre Østfold kommunes beredskapsplaner. Videre har kommunen utført en arbeidsøkt med et utvalg kommunalområder etter skriveøvelse med Statsforvalteren i 2022.

I intervjuene trakk flere informanter frem at kommunen ved ulike anledninger publiserer informasjon på mail eller intranett om dagsaktuelle hendelser som omhandler informasjonssikkerhet. Informantene opplyste at dette brukes som påminnelse om å prioritere informasjonssikkerhet i arbeidshverdagen.

I enkelte intervju fremkom det at resultatene fra hvert kommunalområde blir presentert i ledergrupper, men det var usikkert hva det ble benyttet til. I ett intervju ble det fortalt at resultatene skapte økt bevissthet omkring temaet i etterkant. Enkelte av informantene opplyste at de ikke var kjent med om det ble utført evalueringer. Flere av informanter hadde ikke kjennskap til om evalueringene påvirket opplæringsmateriellet. Det fremgikk av intervjuene at resultater fra sikkerhetsmåneden blir evaluert. I intervjuene opplyste informantene at de ikke var kjent med om opplæringen legger grunnlag for endring i opplæringsmateriellet utover det som er nevnt ovenfor.

5.3 Vurderinger

Indre Østfold kommune har i noen grad sikret kompetansekrav innen IKT-sikkerhet er fastsatt	Gul

Revisor vurderer at Indre Østfold kommune i noen grad oppfyller revisjonskriteriet. Det er avdekket forbedringspotensial knyttet til fastsettelse av kompetansekrav for utpekte sikkerhetsroller ettersom det fremkom i intervju og dokumentasjon at dette ikke eksisterer. Revisor vurderer at de personene som har et dedikert ansvar for informasjonssikkerhet bør inneha tilstrekkelig kompetanse for å sikre god informasjonssikkerhetsstyring. Revisor vurderer at det derfor må tas stilling til kompetansekrav for dedikerte sikkerhetsroller slik at det kan utarbeides kompetanseplaner som skal sikre at kravene oppfylles.

Indre Østfold har imidlertid fastsatt et overordnet mål med opplæringsarbeidet som kan relateres til hva ansatte og ledere på generell basis skal ha kunnskap om, som anses som tilstrekkelig.

Indre Østfold kommune har i stor grad sikret at ansvar og roller innen informasjonssikkerhet (herunder IKT-sikkerhet) er kjent i kommunen og at de som innehar roller er kjent med disse	Lysegrønn

Revisor vurderer at Indre Østfold kommune i stor grad oppfyller revisjonskriteriet. Revisor vurderer at kommunen har klare rollefordelinger og ansvarsbeskrivelser, samt at det er etablert rutiner og systemer for å sikre at kommunens ansatte er kjent med disse. Gjennom både intervju og spørreundersøkelsen fremkommer det at de fleste (>80 %) kjenner til sin egen rolle i IKT-sikkerhetsarbeidet.

Det er imidlertid avdekket et mindre forbedringspotensial knyttet til å bekjentgjøre rollene i kommunen. Det er flere ledere og ansatte som ikke har satt seg tilstrekkelig inn i informasjonssikkerhetshåndboken, som er kommunens beskrivelse av roller og ansvar innen IKT-sikkerhet. Dermed vurderer revisor at kommunen ikke i tilstrekkelig grad har etablert et system for å sikre at ansatte er tilstrekkelig kjent med sine roller, og hvilket ansvar rollen innebærer.

Indre Østfold kommune har i noen grad et opplæringsprogram for å sikre at ansatte er kjent med og er i stand til å etterleve rutiner og retningslinjer innen informasjonssikkerhet (herunder IKT-sikkerhet)	Gul

Revisor vurderer at Indre Østfold i noen grad oppfyller revisjonskriteriet.

Revisor vurderer at kommunen har etablert et godt opplæringsprogram for ledere, og at kommunen gjennomfører opplæringen de har planlagt. Det fremgår av spørreundersøkelsen og intervjuer at kommunen har etablert et opplæringsprogram som ansatte og ledere er godt fornøyd med. Kommunen har tatt opp ulike temaer, som hvordan ansatte skal redusere risikoen for menneskelig svikt og sikkerhet ved arbeid på eksterne lokasjoner. I tillegg benytter kommunen seg av ulike opplæringsmetoder, noe som styrker troen på at de har lagt til rette for at ansatte med ulike preferanser kan gjennomføre opplæringen.

Det er imidlertid avdekket forbedringspotensial knyttet til at hovedvekten av opplæringen kun gis i sikkerhetsmåneden. Videre har revisor avdekket at flere ansatte ikke gjennomfører opplæringen som kommunen har lagt til rette for. Revisor mener det er et ledelsesansvar å sikre at ansatte utfører obligatorisk opplæring. Revisor vurderer dermed at kommunen ikke i tilstrekkelig grad sikrer at ansatte er kjent med og i stand til å etterleve rutiner og retningslinjer.

Indre Østfold kommune sikrer i stor grad at alle ansatte kjenner til hvilken informasjon de behandler og hvilke krav som stilles til arbeidet	Lysegrønn

Revisor vurderer at Indre Østfold kommune i stor grad oppfyller revisjonskriteriet.

Revisor vurderer at ansatte og ledere får opplæring om hvilken informasjon de behandler, og hvordan de skal behandle denne. Det er fremdeles behov for og ønske om ytterligere opplæring utover sikkerhetsmåneden.

Indre Østfold kommune sikrer i stor grad at alle ansatte har en tilstrekkelig forståelse for trusler og risiko for å forstå hvorfor arbeidsoppgavene bør utføres på en sikker måte	Lysegrønn

Revisor vurderer at Indre Østfold kommune i stor grad oppfyller revisjonskriteriet.

Revisor vurderer at Indre Østfold kommune er oppdatert på dagsaktuelle trusler og risikoer, og legger opp til at denne informasjonen skal nå de ansatte. Dette fremgår av svar fra spørreundersøkelsen og intervju hvor det vises til jevnlige phishing-kampanjer, innhold i opplæringen, samt oppdateringer på interne sider etter hendelser i samfunnet. Revisor vurderer imidlertid at det er behov for tydeliggjøring og opplæring om hvilke tiltak og handlinger anses å være tilstrekkelig sikker for å redusere potensiale for sikkerhetstruende hendelser.

Indre Østfold kommune legger i noen grad til rette for at ansatte har en forståelse av at uønskede informasjonssikkerhetshendelser kan hindre de i utførelse av arbeidet, eller få konsekvenser for andre parter	Gul

Revisor vurderer at Indre Østfold kommune i noen grad oppfyller revisjonskriteriet.

Revisor vurderer at Indre Østfold kommune har opplæring som omhandler konsekvensomfanget av en eventuell digital hendelse. Det er imidlertid funn som indikerer at ansatte ikke sitter igjen med tilstrekkelig innsikt i dette, samt usikkerhet knyttet til hva som kan hindre hendelser og dermed konsekvensene.

Indre Østfold kommune har tilstrekkelige rutiner for rapportering til ledere og ansvarlige for sikkerhetshendelser, avvikshåndtering og egenkontroll	Grønn

Revisor vurderer at avdekkede forhold oppfyller revisjonskriteriet fullt ut på bakgrunn av at de har etablert et velfungerende system for rapportering og avvikshåndtering.

Indre Østfold gir i noen grad ansatte opplæring om interne rutiner for varsling av informasjonssikkerhetshendelser	Gul

Revisor vurderer at Indre Østfold i noen grad oppfyller revisjonskriteriet. Det er avdekket et forbedringspotensial.

Revisor vurderer at Indre Østfold kommune har etablert opplæring om avvikshåndtering, og tilbyr delvis tilstrekkelig opplæring innen temaet. Revisjonsbevisene indikerer at Indre Østfold kommune har etablert opplæring innen varsling. Det er imidlertid funn som indikerer at kommunen ikke har formidlet denne informasjonen ut til de ansatte i stor nok grad. Revisor vurderer at dette kan være årsak til at et stort antall ansatte (omtrent 50 %) ikke kjenner til hvor de skal melde fra om sikkerhetshendelser.

Indre Østfold gir i noen grad opplæring av personell etter evaluering av IKT-hendelser/øvelser	Gul

Revisor vurderer at Indre Østfold i noen grad oppfyller revisjonskriteriet.

Revisor vurderer at kommunen samler inn informasjon for å evaluere i etterkant av hendelser/øvelser. Enkelte av funnene blir benyttet til å finne fokusområder videre, eller minne ledere og ansatte på temaet. Det er imidlertid relativt få indikasjoner som viser til at Indre Østfold har gjort større endringer i opplæring etter evalueringer er utført.

5.3.1 Tilleggsvurderinger fra spørreundersøkelsen til de folkevalgte

Som beskrevet i punkt 3.3 Revisjonsmetoder, ble spørreundersøkelsen sendt ut til folkevalgte i Indre Østfold kommune. Utsendelse av spørreundersøkelsen til de folkevalgte ble gjennomført som følge av et innspill fra kontrollutvalget. Funnene påvirker ikke funn og konklusjoner i forvaltningsrevisjonen, men blir likevel løftet frem med hensikt om å belyse eventuelle forskjeller og behov for tiltak også for de folkevalgte.

Revisor viser til revisjonskriteriet 5.2.3: *Indre Østfold kommune bør ha opplæringsprogram for å sikre at ansatte er kjent med og er i stand til å etterleve rutiner og retningslinjer innen informasjonssikkerhet (herunder IKT-sikkerhet)*

Funnene fra spørreundersøkelsen viser at de folkevalgte ikke har mottatt opplæringsmateriell, og effekten av opplæringsprogrammet varierer. Funnene skiller seg dermed ikke stort fra funnene til de ansatte.

Revisor viser til revisjonskriteriet 5.2.4: *Indre Østfold kommune bør sikre at alle ansatte kjenner til hvilken informasjon de behandler og hvilke krav som stilles til arbeidet*

Funnene indikerer at de folkevalgte i stor grad kjenner til hvordan de skal behandle sensitiv informasjon. Funnene skiller seg dermed ikke nevneverdig fra funnene ellers i rapporten.

Revisor viser til revisjonskriteriet 5.2.8: *Indre Østfold bør gi ansatte opplæring om interne rutiner for varsling av informasjonssikkerhetshendelser*

Funnene kan indikere at de folkevalgte kjenner til hvem de bør varsle ved mistanke om en eventuell hendelse. Funnene skiller seg dermed litt fra funnene ellers.

5.4 Konklusjon og anbefalinger

Her omtales krav som *bør* (beste praksis) gjennomføres (viser til 3.2 om revisjonskriterier for ytterligere informasjon). Fakta, omtalt som revisjonsbevis vurderes opp mot revisjonskriteriene, og disse vurderingene danner grunnlaget for de konklusjoner som trekkes.

Revisor konkluderer, basert på den gjennomførte revisjonen, med at kommunens ansatte i noen grad har fått tilstrekkelig opplæring. Det er avdekket enkelte mangler som kan påvirke sikkerhetsbevissthet og kompetanse innen informasjonssikkerhet.

Revisor vurderer at Indre Østfold kommune har sørget for et adekvat opplæringsprogram for alle ansatte i kommunen, samt at kommunen jobber aktivt for å øke sikkerhetsbevisstheten og kompetansen. Dette gjelder blant annet innen dagsaktuelle risikoer, avvikshåndtering og sikkerhet på hjemmekontor. Indre Østfold kommune mangler imidlertid kompetansekrav for informasjonssikkerhet, spesielt for dedikerte sikkerhetsroller. Videre burde opplæringsprogrammet vært fordelt utover i året. Det er en stor andel (70-80 %) ansatte og ledere som ikke gjennomfører opplæringen, og for få ledere følger opp sitt ansvar med å formidle informasjon om informasjonssikkerhet til de ansatte. Revisor vurderer at fravær av gjennomføring kan påvirke ansattes evne til å ivareta sine primæroppgaver innen informasjonssikkerhet. Det gjenstår derfor et arbeid for å sikre at opplæringen utføres av kommunens ansatte.

Basert på revisors vurderinger og konklusjon anbefaler revisor at Indre Østfold kommune bør:

Tiltak relatert til problemstilling 2:	Prioritet (1-3)
Etablere krav til ledere (eller andre tilsvarende rutiner) for å sikre gjennomføring av opplæring innen IKT-sikkerhet og varsling	2
Bevisstgjøre ledere om sitt ansvar for å følge opp at ansatte gjennomfører obligatorisk opplæring innen IKT-sikkerhet	2
Fastsette et årshjul for opplæringsaktiviteter for å spre opplæringsprogrammet utover året	2
Benytte signering ved gjennomført opplæring	2
Innarbeide et kurs for alle nyansatte om informasjonssikkerhet	2
Lage opplæringsmateriell om informasjonssikkerhetshåndboken for å gjøre innholdet mer forståelig og mindre tidkrevende	3
Benytte svar fra sikkerhetskulturkartleggingen til å justere opplæringsmateriellet	3
Formulere og fastsette kompetansekrav innen IKT-sikkerhet for dedikerte sikkershetsroller og kommunisere disse ut til kommunens ansatte.	3
Legge til IKT-sikkerhet som et sjekkpunkt i systemet *Framsikt*	3
Gjennomføre kartlegging etter nye tiltak er iverksatt for å vurdere opplæringseffekten	3

Anbefalingene er bygd opp ved følgende system:

1. Må rettes på snarest
2. Bør rettes på, men korrigerende tiltak kan skyves ut i tid
3. Bør vurderes rettes på, og korrigerende tiltak kan skyves ut i tid.

Revisor gjør oppmerksom på at dette ikke er ment som en fullstendig liste over nødvendige tiltak, men etter revisors vurdering de mest vesentlige. Kommunen må selv vurdere hva som er nødvendige tiltak til enhver tid. Det er derfor ingen garanti at revisjonskriteriene er etterlevd ved å innføre de anbefalte tiltakene. Blant annet vil dette avhenge av ledelsens etterfølgende oppfølging av tiltakene for å sikre at de har den ønskede effekten.

6 KILDER OG LITTERATUR

Dokumentasjon tilsendt fra Indre Østfold kommune

- Besvarelse fra Indre Østfold kommune (Hoveddokument)
- Vedlegg 1 - Bilag 7B - Tjenestekatalog - Ikomm Allegro
- Vedlegg 2 - Bilag 2C - Leverandørens svar på kundens kravspesifikasjon
- Vedlegg 3 - Bilag 2C - Ikomm-iso-27001-no
- Vedlegg 5 - IØK Bilag 9-40, Drift av LAN-switch-utvidet
- Vedlegg 6 -IØK Bilag 9-46, Drift av kjerne- og distribusjonsswitcher
- Vedlegg 7 - Informasjonssikkerhetshåndboken v2
- Vedlegg 8 -Introduksjon for nye ledere Del 3
- Vedlegg 9 - Bilag 5C – Samhandlingsplan
- Vedlegg 10 -Møtekalender 2024
- Vedlegg 11 - Bilag 4B - Plan for avslutning av ytelsen
- Vedlegg 12 - Program for systemeierskap i IØK 23 mai 2022
- Vedlegg 13 - Bilag 2A - Generell løsningsbeskrivelse
- Vedlegg 14 A – Oversendelsesbrev
- Vedlegg 14 B - Innstramning i Ikomm-systemer og begrensinger i tilgang for å benytte privilegerte kontoer
- Vedlegg 15- Ansvarsmatrise IØK_IKOMM_Identum for eAdm
- Vedlegg 16 – Databehandleravtale
- Vedlegg 17 - Bilag til databehandleravtale
- Vedlegg 18 A -Planlegging av beredskapsøvelse til Brennemoen 25.04.2022
- Vedlegg 18 B- Planlegging av beredskapsøvelse til Brennemoen 04.04.2022
- Vedlegg 19 - Sikkerhetsmåneden 2021
- Vedlegg 20 - Sikkerhetsmåneden oktober 2022 1
- Vedlegg 21 - Nyhet på intranettet - Sikkerhetsmåneden 2023
- Vedlegg 22 - Sikkerhetsmåneden oktober 2023
- Vedlegg 24- Opplæring Informasjonssikkerhet og personvern 6 jan 2022 -ledelsen
- Vedlegg 25 A - Undersøkelse om digital sikkerhetskultur 2023 - Oppvekst (NAV og seksjon livsmestring)
- Vedlegg 25 B - Undersøkelse om digital sikkerhetskultur 2023 - Oppvekst (skoler -utvalg)
- Vedlegg 25 C - Undersøkelse om digital sikkerhetskultur 2023 - Økonomi og virksomhetsstyring
- Vedlegg 25 D - Undersøkelse om digital sikkerhetskultur 2023 - Innovasjon og kommunikasjon
- Vedlegg 25 E - Undersøkelse om digital sikkerhetskultur 2023 - Oppvekst (Stab og barnehage)
- Vedlegg 25 F - Undersøkelse om digital sikkerhetskultur 2023 - Plan og teknikk
- Vedlegg 25 G - Undersøkelse om digital sikkerhetskultur 2023 - Helse og mestring (Behandling og mestring) (1)
- Vedlegg 26 - Styringsdokument - Internkontroll i Indre Østfold kommune
- Vedlegg 28- Kontroll av avvikshåndtering -kontrollerende dokument
- Driftsavtale IØK (1) (002)

Informanter

- Wenche Folbeg - Kommunedirektør
- Tron Einar Kallum – IT-sjef
- Tommy André Otnes – Leder IKT-sikkerhet og personvernombud
- Linda Kristin Lorentsen – Barnevern
- Lisbeth Skjeldrum – Sentraladministrasjon
- Vegard Mysliwski – HR
- Thorfinn Oustorp – Rektor
- Ståle Ruud - Sentraladministrasjon

Referanser

- Datatilsynets veileder – Informasjonssikkerhet og internkontroll https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/
- Digdir - Kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet - https://www.digdir.no/informasjonssikkerhet/kompetansebeskrivelser-roller-innen-styring-og-kontroll-av-informasjonssikkerhet/1107
- Forskrift om kommunal beredskapsplikt - FOR-2011-08-22-894 - https://lovdata.no/dokument/SF/forskrift/2011-08-22-894
- Ledelsessystemer for informasjonssikkerhet – ISO/IEC 27001:2023 – Standard Norge
- Nasjonal sikkerhetsmyndighet - Grunnprinsipper for IKT-sikkerhet - https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/
- Nasjonal sikkerhetsmyndighet – Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester - https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/

7 KOMMUNEDIREKTØRENS UTTALELSE

Kommunedirektør i Indre Østfold kommune har avgitt følgende uttalelse til forvaltningsrevisjonsrapporten:

«Det er gjennomført en omfattende forvaltningsrevisjon som til sammen bestod av 37 kriterier. Med bakgrunn i at kommunerevisjonen har benyttet ressurser med sikkerhetskompetanse fra BDO har det vært en sikkerhetsfaglig grundig revisjon. I tiden etter at den nye kommunen ble opprettet, har det vært en omfattende og systematisk innsats i kommunen for å styrke informasjonssikkerheten. Dette arbeidet har funnet sted både internt i organisasjonen og gjennom samarbeid med driftsleverandøren IKOMM AS.

Forvaltningsrevisjonen viser at kommunen i stor grad tilfredsstiller fullt ut de fleste kriteriene, men at det er noen kriterier som det bør arbeides mer med, men som ikke er av kritisk art. Dette sammenfaller med kommunedirektørens vurderinger og kommunerevisjonens anbefalinger tas til etterretning.

Kommunedirektøren takker for et godt samarbeid vedrørende forvaltningsrevisjonen av IKT-sikkerhet.»