Rapport

HVALER KOMMUNE

26.09.2024

Forvaltningsrevisjon
Personopplysnings- og informasjonssikkerhet

Innhold

1 SAMMENDRAG

Revisjonens fremgangsmåte

BDO har på oppdrag fra Østre Viken kommunerevisjon gjennomført en forvaltningsrevisjon av informasjonssikkerhet og personopplysningssikkerhet i Hvaler 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 revisjonslaget hatt kontinuerlig kontakt med ØVKR og Hvaler kommune om gjennomføring av revisjonen.

Fremdriftsplanen har bestått av tre faser:

1) Planlegging:
    a. Oppstartsmøte med BDO og Hvaler kommune (18.03.24)
    b. Planleggingsmøte med BDO og Hvaler kommune (14.05.24)
    c. Forankring av revisjonskriterier med Hvaler kommune
    d. Oppstartbrev og oversendelse av revisjonskriterier
2) Gjennomføring
    a. Oversendelse av dokumentasjon
    b. Gjennomføring av intervju
    c. Analyse av datagrunnlag, vurdering og konklusjon
3) Sluttføring
    a. Utarbeidelse av rapport
    b. Verifisering faktagrunnlag fra Hvaler
    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 delkapittel 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 Hvaler kommune et internkontrollsystem for personopplysningssikkerhet og informasjonssikkerhet som inneholder alle forventede elementer etter anerkjente standarder og regulatoriske krav?

Revisjonslaget konkluderer, basert på den gjennomførte revisjonen, med at Hvaler kommune har et internkontrollsystem som i stor grad inneholder forventede elementer etter anerkjente standarder og regulatoriske krav. Det er avdekket enkelte avvik som Hvaler kommune bør prioritere videre for å oppfylle regulatoriske krav.

Hvaler kommune jobber grundig med etablering av internkontrollsystem innen informasjonssikkerhet og personopplysningssikkerhet. Dokumentasjon i form av policyer, prosedyrer og rutiner, samt ansvarsfordeling og målsetning innen henholdsvis informasjonssikkerhet og personopplysningssikkerhet vurderes som tilfredsstillende.

Det er imidlertid avdekket funn som kan redusere kvaliteten av internkontrollsystemet, og fører til at systemet ikke inneholder alle forventede elementer etter anerkjente standarder og regulatoriske krav. Hvaler kommune har i liten grad gjennomført risikovurderinger innen informasjonssikkerhet, noe som kan medføre at risikoene ikke er kjent og ikke håndteres på riktig måte. Manglende risikovurderinger gjør det også vanskelig å konkludere med at internkontrollsystemet er tilstrekkelig. Videre er det avdekket manglende kontrollerende elementer, noe som medfører at kommunen ikke oppfyller krav i anerkjente standarder. Det skal imidlertid bemerkes at Hvaler kommune er i etableringsfasen av internkontrollsystemet, og at kontrollerende elementer kan tilkomme på et senere tidspunkt. Avslutningsvis er det avdekket mangler knyttet til beredskapsøvelser innen informasjonssikkerhet.

Revisjonslaget har gjort følgende vurderinger knyttet til revisjonskriteriene for problemstilling 1 (Tabell 1):

Hvaler kommune har i stor grad et internkontrollsystem som er tilpasset behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene for personvernet. Internkontrollsystemet er dokumentert og består av styrende, gjennomførende og kontrollerende elementer.	Lysegrønn
Hvaler kommune har i tilfredsstillende grad beskrevet mål og strategi for informasjonssikkerhet og vern av personopplysninger, som legger grunnlaget for kommunens internkontroll på informasjonssikkerhetsområdet.	Grønn
Hvaler kommune har i noen grad etablert egnede tiltak for å oppnå kommunens mål for informasjonssikkerhet og vern av personopplysninger, basert på risikovurderinger.	Gul
Hvaler kommune har i noen grad et internkontrollsystem på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for internkontroll for informasjonssikkerhet.	Gul
Hvaler kommune har i tilfredsstillende grad utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39.	Grønn
Hvaler kommune har i stor grad en beredskapsplan.	Lysegrønn
Hvaler kommune har i tilfredsstillende grad etablert og dokumentert rutiner og prosesser for gjennomføring av personvernkonsekvensvurderinger når det er sannsynlig at en behandling vil medføre en høy risiko for personvernet.	Grønn
Hvaler kommune har i tilfredsstillende grad etablert dokumenterte rutiner og prosesser for å kunne håndtere og dokumentere hendelser, avvik og sikkerhetsbrudd som berører personopplysninger, inkludert rapportering til Datatilsynet og de registrerte når det er nødvendig.	Grønn
Hvaler kommune har i stor grad sikret at det er avsatt tilstrekkelige ressurser, kompetanse og handlingsrom til å arbeide med informasjonssikkerhet, samt sikre etterlevelse.	Lysegrønn
Hvaler kommune oppfyller ikke revisjonskriteriet om at de bør gjennomføre risikovurderinger for informasjonssikkerhet	Rød
Hvaler kommune iverksetter i noen grad tiltak som blir identifisert etter gjennomføring av risikovurderinger, hendelser eller andre kontrollaktiviteter for å sikre kontinuerlig forbedring.	Gul
Hvaler kommune oppfyller revisjonskriteriet med å fastsette ansvar og roller i styringsdokumenter for forebyggende sikkerhet. Disse skal være kjent i kommunen.	Grønn

Hvaler kommune oppfyller revisjonskriteriet om å ha et system for rapportering og håndtering av hendelser, avvik og informasjonssikkerhetsbrudd	Grønn
Hvaler kommune har i stor grad et system for å evaluere internkontroll for informasjonssikkerhet for å sikre kontinuerlig forbedring av arbeidet	Lysegrønn
Hvaler kommune oppfyller ikke revisjonskriteriet om å gjennomføre beredskapsøvelser for informasjonssikkerhet	Rød

Tabell 1: Funn problemstilling 1

Problemstilling 2: Har Hvaler kommune gjort internkontrollsystemer for informasjonssikkerhet og personopplysningssikkerhet kjent i kommunen og etterleves det?

Revisjonslaget konkluderer, basert på den gjennomførte revisjonen, med at Hvaler kommune har etablert et internkontrollsystem for informasjonssikkerhet som er kjent i kommunen. Det er ikke avdekt alvorlige avvik knyttet til problemstilling 2. Revisjonens funn viser at både ansatte og ledere i stor grad kjenner til sin rolle og sitt ansvar. Kommunen har de siste årene kommet godt i gang med etablering av internkontrollsystemet, men er fremdeles i en implementeringsfase. Det gjenstår arbeid for å sikre at internkontrollarbeidet og ansvarsrollene etterleves, men ut fra revisjonslagets forståelse etterlever en stor del av ansatte og ledere det som forventes av dem.

Revisjonslaget har gjort følgende vurderinger knyttet til revisjonskriteriene for problemstilling 2 (tabell 2):

Hvaler kommune har sikret at ansvar og myndighet innen informasjonssikkerhet er delegert og kommunisert	Grønn
Hvaler kommune har i stor grad opplærings- og bevisstgjøringstiltak for å sikre at alle ansatte er bevisst eget ansvar for informasjonssikkerhet	Lysegrønn
Hvaler kommune har sikret at ansatte blir informert om eventuelle endringer i internkontroll for informasjonssikkerhet	Grønn
Hvaler kommune har i stor grad sikret at ansatte kjenner til rutiner for varsling av informasjonssikkerhetshendelser	Lysegrønn

Tabell 2: Funn problemstilling 2

Revisjonens anbefalinger

Anbefalinger tilknyttet problemstilling 1:

Basert på revisjonslagets vurderinger og konklusjon anbefaler revisjonslaget at Hvaler kommune bør:

a) gjennomføre risikovurdering for å sikre at omfang og innretting av internkontrollen er tilpasset relevante personvern- og informasjonssikkerhetsrisikoer. Videre bør det gjennomføres oppdaterte risikovurderinger på personvernområdet for alle behandlingsaktiviteter i kommunen. Risikovurderingene bør fastsettes basert på en prioritert liste. Formålet med risikovurderingen bør være å
   - vurdere hvorvidt eksisterende sikkerhetstiltak er tilstrekkelig, eller om det burde vært etablert ytterligere.
   - vurdere hvorvidt internkontrollsystemet er tilstrekkelig, eller om det burde ha vært etablert ytterligere rutiner. Hva som anses som tilstrekkelig er en kontinuerlig prosess og må bestemmes ut fra risikobildet.
   - vurdere tiltak i kommunens beredskapsplan.

Basert på revisjonslagets vurderinger og konklusjon anbefaler revisjonslaget at Hvaler kommune bør vurdere å:

b) legge til telefonnummer til kontaktene i beredskapsplanen for IKT-hendelser.
c) gjennomføre kontrollaktiviteter av internkontrollsystemet i sin helhet, samt aktiviteter som inngår. Dette skal sikre at Hvaler kommune kan teste og vurdere sikkerhetstiltakenes effekt, samt etterlevelse av regulatoriske krav.
d) implementere og øve på beredskapsplanen for IKT-hendelser. Hensikten er å kontrollere og teste beredskapsplanverket for å sikre at det fungerer som planlagt. Videre vil øvelser teste samarbeidet og kommunikasjonen mellom Hvaler og Fredrikstad i krisehendelser som omhandler informasjonssikkerhet. Dette vil bli et regulatorisk krav dersom Hvaler kommune identifiserer IKT-hendelser som en risiko ved utførelse av helhetlig risiko- og sårbarhetsanalyse (jf. § 2 forskrift om kommunal beredskapsplikt).

Anbefalinger tilknyttet problemstilling 2:
Basert på revisjonslagets vurderinger og konklusjon anbefaler revisjonslaget at Hvaler kommune bør vurdere å:

e) strukturere opplæring innen informasjonssikkerhet ved å:
    - innføre obligatorisk opplæring for nye og nåværende ansatte som gjentas jevnlig.
    - sørge for at gjennomført opplæring blir dokumentert.
f) styrke kulturen for rapportering av personvern- og informasjonssikkerhetsavvik samt øke ansattes bevissthet og kompetanse på området. Dette kan omfatte utvikling og gjennomføring av opplæringsprogrammer eller workshops som øker ansattes forståelse av hva som utgjør et personvern- og informasjonssikkerhetsavvik, samt viktigheten av å rapportere alle typer avvik, inkludert mindre alvorlige hendelser. Det kan også inkludere etablering av enkle og tydelige sjekklister for identifisering og rapportering av avvik, slik at alle ansatte enkelt kan følge opp og handle riktig.

Revisjonslaget gjør oppmerksom på at dette ikke er ment som en fullstendig liste over nødvendige tiltak, men etter revisjonslagets 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 revisjonslaget rapportere resultatene av sin revisjon til kontrollutvalget.

Forvaltningsrevisjonen er gjennomført på bakgrunn av plan for forvaltningsrevisjon vedtatt i kommunestyret i Hvaler kommune i sak 88/21 (16.12.2021). Det fremgår av «særutskrift av sak 23-28» fra 25.05.23 at kontrollutvalget Hvaler valgte å utsette forvaltningsrevisjonen av «personvern og informasjonssikkerhet» til 2024. Plan for gjennomføring av forvaltningsrevisjonen ble vedtatt i kontrollutvalget 02.05.2024. Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet mai - september 2024. Det ble gjennomført et oppstartsmøte med kommuneadministrasjonen.

Revisjonslaget 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 12.09.2024 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. Rapporten ble deretter sendt til rådmannen for en uttalelse. Revisjonen har ikke mottatt noen uttalelse fra rådmannen.

Forvaltningsrevisjonen er gjennomført av Anine Klepp, Mari Lekve Bjelle og Elisabeth Runsjø og kvalitetssikret av Dagfinn Buset og Morten Thuve. Fagleder for forvaltningsrevisjon Casper Støten fra Østre Viken kommunerevisjon IKS har vært oppdragsansvarlig revisor og har kvalitetssikret forvaltningsrevisjonen underveis. Revisjonslagets habilitet og uavhengighet er vurdert opp mot kommunen og den undersøkte virksomheten, og revisjonen finner de habile til å utføre forvaltningsrevisjonen.

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

Østre Viken kommunerevisjon IKS
Rolvsøy, 26. september 2024

Dagfinn Buset
oppdragsansvarlig revisor

Casper Støten
oppdragsansvarlig revisor

Anine Klepp
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 hovedproblemstilling:

> *«Etterlever Hvaler kommune regulatoriske krav og beste praksis på området informasjons- og personopplysningssikkerhet?»*

For å besvare hovedproblemstillingen ble følgende underproblemstillinger utledet:

3.1.1 Problemstilling 1: Har Hvaler kommune et internkontrollsystem[3] for personopplysningssikkerhet og informasjonssikkerhet som inneholder alle forventede elementer etter anerkjente standarder og regulatoriske krav?

Ved gjennomgang av det som omfatter informasjonssikkerhet ble det vurdert hvordan Hvaler kommune hadde innrettet informasjonssikkerhet i sin internkontroll. Hvaler kommune plikter å ha styring og kontroll på informasjonssikkerhetsrisikoer[4]. Dette gjelder all informasjonsbehandling internt og eksternt. Offentlige virksomheter er videre pålagt å ha internkontroll for informasjonssikkerhet som baserer seg på anerkjente standarder. Videre bør dette være en integrert del av øvrig virksomhetsstyring (jf. eForvaltningsforskriften §15). Det er naturlig å legge til grunn de mest anerkjente rammeverkene for internkontroll relatert til informasjonssikkerhet; ISO/IEC 27001 eller andre anerkjente standarder[5], som beskriver hvilke elementer som bør være på plass i et helhetlig internkontrollsystem. Hvaler kommune bør derfor ha en strukturert tilnærming i arbeidet med informasjonssikkerhet, og det forventes at følgende elementer er del av en tilfredsstillende internkontroll: roller og ansvar, risikovurderinger, risikohåndtering, kontrollhandlinger og evaluering, samt kontinuerlig forbedring (ISO/IEC 27001).

I henhold til EUs personvernforordning, plikter Hvaler kommune å etablere internkontroll for personvern, inkludert for personopplysningssikkerhet. Personvernforordningen stiller ikke eksplisitte krav til utformingen av internkontrollen, utover at den skal være tilpasset behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene som virksomheten står overfor. Datatilsynet har imidlertid utarbeidet en veileder for etablering av internkontroll, hvor det presiseres at internkontrollen skal være ledelsens verktøy for å ivareta deres ansvar og demonstrere etterlevelse etter personvernregelverket, samtidig som den skal være de ansattes verktøy for å utføre oppgavene på en forsvarlig måte. For å møte kravet om en systematisk tilnærming, bør internkontrollen ifølge Datatilsynet (Veileder - Informasjonssikkerhet og internkontroll) bestå av styrende, gjennomførende og kontrollerende elementer.

Avgrensning:
Revisjonen er avgrenset til å vurdere informasjonssikkerhet og personopplysningssikkerhet. Personopplysningssikkerhet henger tett sammen med informasjonssikkerhet og refererer til tiltak og prosedyrer som beskytter personopplysninger mot uautorisert tilgang, endring, utlevering eller ødeleggelse. Tiltakene inkluderer tekniske tiltak som kryptering, organisatoriske prosedyrer som tilgangskontroll, rutiner og retningslinjer for sikker håndtering av personopplysninger. Videre er revisjonen avgrenset til å ikke omfatte bestemmelser etter lov om nasjonal sikkerhet (sikkerhetsloven).

[3] Internkontrollsystem er i denne revisjonen tilsvarende det som også kan omtales som styringssystem eller ledelsessystem.

[4] Informasjonssikkerhet innebærer å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet.

[5] Eksempelvis COSO-rammeverket eller andre anerkjente ISO-standarder.

3.1.2 Problemstilling 2: Har Hvaler kommune gjort internkontrollsystemet for informasjonssikkerhet og personopplysningssikkerhet kjent i kommunen og etterleves det?

Ifølge anerkjente standarder innen internkontrollsystem for informasjonssikkerhet og personopplysningssikkerhet bør internkontrollsystemet *etterleves* (ISO/IEC 27001). Revisjonslaget mener det dermed er en forutsetning at Hvaler kommune følger det etablerte internkontrollsystemet for å vurdere om mål oppnås, om internkontrollsystemet fungerer etter hensikt, og om justeringer er nødvendig dersom systemet ikke oppnår ønsket effekt. Videre legger anerkjente standarder opp til at innholdet i internkontrollsystemet skal gjøres kjent i kommunen. På bakgrunn av dette har revisjonslaget vektlagt Hvaler kommunes arbeid med å synliggjøre roller og ansvar, samt hvordan tiltak har vært implementert for kommunens ansatte.

Avgrensning:
Hvaler kommune består av ulike sektorer. For å besvare problemstillingen har revisjonslaget valgt å fokusere på sektorer, hvor det etter revisjonslagets vurdering er forhøyet risiko knyttet til brudd på informasjonssikkerhet og hvor det behandles personopplysninger av særlig viktighet. Revisjonslaget har valgt ut områdene «Skole, oppvekst og kultur» og «Helse og friskliv». Revisjonslaget mener at det er tilstrekkelig med et utvalg for å få innsikt i hvordan kommunen arbeider med informasjonssikkerhet ut mot sine ansatte.

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisjonslaget fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriteriene er den objektive målestokk som setter revisjonslaget i stand til å gjøre vurderinger. Revisjonskriteriene og revisjonslagets kunnskap og erfaring innen forvaltningsrevisjonsmetodikk og fagkompetanse innen feltet, gjør at revisjonslaget kan gjøre objektive og holdbare vurderinger.

Revisjonskriteriene etablerer en 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 revisjonslagets vurderinger bygger på. Dette vil gjøre det enklere å etterprøve revisjonslagets 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
- Lov 15. juni 2018 om behandling av personopplysninger (personopplysningsloven)
- EUs generelle personvernforordning 2016/679 av 27. april 2016 (GDPR)
- 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 revisjonslaget vurderinger og konklusjoner. I denne forvaltningsrevisjonen har revisjonslaget benyttet ulike datakilder og datainnsamlingsmetoder 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.

Dokumentanalyse

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

Intervjuer

Det er gjennomført totalt ni intervjuer. Blant de intervjuede er det informanter fra sentrale stillinger rettet mot informasjonssikkerhet og personopplysningssikkerhet, samt representanter fra de sektorene «helse og friskliv» og «skole, oppvekst og kultur». Se fullstendig liste over informanter i kapittel «6.Kilder og litteratur».

Alle intervjureferater 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 i intervjuet.

Stikkprøver

Ved avholdelse av enkelte intervjuer ble det gjennomført stikkprøver. Stikkprøver benyttes som metode for å verifisere fakta ved å vise til konkrete og dokumenterte «bevis». Eksempelvis fikk revisjonslaget innsikt i opplæringsmateriellet innen informasjonssikkerhet og personvern.

Avgrensninger

Datainnsamlingsmetodene som er benyttet i revisjonen innehar sine begrensninger, og vil ikke fullt ut dekke en representasjon av virkeligheten. Likevel er det etter revisjonslagets vurdering en styrke å benytte ulike datainnsamlingsmetoder da temaet vil belyses fra flere perspektiver.

BDO har basert våre analyser på mottatte data. BDO kan ikke utelukke at det kan være 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.
Mørkegrønn	Avdekkede forhold anses å være av uvesentlig betydning, og i praksis oppfylles dermed revisjonskriteriet.

Figur 1, Symbolbruk for vurdering av funn

4 PROBLEMSTILLING 1

Har Hvaler kommune et internkontrollsystem for personopplysningssikkerhet og informasjonssikkerhet som inneholder alle forventede elementer etter anerkjente standarder og regulatoriske krav?

4.1 Revisjonskriterier

Hvaler kommune skal:

- ha et internkontrollsystem som er tilpasset behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene for personvernet. Internkontrollsystemet bør bestå av styrende, gjennomførende og kontrollerende elementer. Dette skal være dokumentert. (GDPR art. 5 nr. 2, 24, 32 og Datatilsynet: Veileder for informasjonssikkerhet og internkontroll).
- ha beskrevet mål og strategi for informasjonssikkerhet og vern av personopplysninger, som legger grunnlaget for kommunens internkontroll på informasjonssikkerhetsområdet (eForvaltningsforskriften §15, GDPR artikkel 32 og Datatilsynet: Veileder for informasjonssikkerhet og internkontroll).
- ha etablert egnede tekniske og organisatoriske tiltak for å oppnå kommunens mål for informasjonssikkerhet og vern av personopplysninger, basert på risikovurderinger. Dette skal være dokumentert. (GDPR artikkel 32 og Datatilsynet: Veileder for informasjonssikkerhet og internkontroll).
- ha et internkontrollsystem på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for internkontroll for informasjonssikkerhet (eForvaltningsforskriften §15).
- ha utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39.
- ha en beredskapsplan (forskrift om kommunal beredskapsplikt §4).
- ha etablert og dokumentert rutiner og prosesser for gjennomføring av personvernkonsekvensvurderinger når det er sannsynlig at en behandling vil medføre en høy risiko for personvernet (GDPR artikkel 35).
- etablert dokumenterte rutiner og prosesser for å kunne rapportere hendelser, avvik og sikkerhetsbrudd som berører personopplysninger til Datatilsynet og de registrerte når det er nødvendig (GDPR artikkel 33 og 32).

Hvaler kommune bør:

- sikre at det er avsatt tilstrekkelige ressurser, kompetanse og handlingsrom til å arbeide med informasjonssikkerhet, samt sikre etterlevelse (ISO/IEC 27001, ISO/IEC 27701, Digdir: Internkontroll i praksis – ledelsens styring og oppfølging).
- iverksette tiltak som blir identifisert etter gjennomføring av risikovurderinger, hendelser eller andre kontrollaktiviteter for å sikre kontinuerlig forbedring (Datatilsynet: Informasjonssikkerhet og internkontroll, Digdir: Internkontroll i praksis – Vurdering av risiko, ISO/IEC 27001, ISO/IEC 27701).
- ha fastsatt ansvar og roller i styringsdokumenter for forebyggende sikkerhet. Disse skal være kjent i kommunen (Digdir: Informasjonssikkerhet – kompetansebeskrivelser for styring og kontroll av informasjonssikkerhet).

- gjennomføre risikovurderinger for informasjonssikkerhet (forskrift om kommunal beredskapsplikt §2, Digdir: Internkontroll i praksis – Vurdering av risiko, ISO/IEC 27001, ISO/IEC 27701).
- ha et system for rapportering og håndtering av hendelser, avvik og informasjonssikkerhetsbrudd (Digdir: Internkontroll i praksis - Overvåking og hendelseshåndtering).
- ha system for å evaluere internkontroll for informasjonssikkerhet for å sikre kontinuerlig forbedring av arbeidet (ISO/IEC 27001, ISO/IEC 27701, Digdir: Internkontroll i praksis – virksomhetsledelsens gjennomgang, Datatilsynet: Informasjonssikkerhet og internkontroll).
- gjennomføre beredskapsøvelser for informasjonssikkerhet (forskrift om kommunal beredskapsplikt §7).

4.2 Datagrunnlag

4.2.1 Hvaler kommune skal ha et internkontrollsystem som er tilpasset behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene for personvernet. Internkontrollsystemet bør bestå av styrende, gjennomførende og kontrollerende elementer. Dette skal være dokumentert.

Det fremgår av dokumentet *Styringssystem Hvaler kommune* en illustrasjon over internkontrollsystem for informasjonssikkerhet og personvern (heretter internkontroll/internkontrollen) i kommunen. Videre fremgår det av dokumentet at internkontrollen er bygd opp av styrende, gjennomførende og kontrollerende elementer. Revisjonslaget ble informert om at dokumentene er lagret i kommunens Kvalitetssystem.

Styrende dokumenter:
Det fremgår av dokumentet *Styringssystem Hvaler kommune* at de styrende dokumentene utgjør følgende dokumenter: *Informasjonssikkerhetspolicy, Styringsdokument for personvern* og *Styringsdokument for Informasjonssikkerhet i Hvaler kommune.* Videre at dokumentet inneholder overordnede føringer, mål og strategi, for kommunens arbeid med informasjonssikkerhet og personvern.

Ifølge *Styringsdokument for informasjonssikkerhet i Hvaler kommune* er IT-sikkerhetsråd ansvarlig for å bistå informasjonssikkerhetsansvarlig i arbeidet med å utarbeide og vedlikeholde retningslinjer og rutiner for informasjonssikkerhet og personvern.

Gjennomførende dokumenter:
Det fremgår av dokumentet S*tyringsdokument for informasjonssikkerhet i Hvaler kommune* at de gjennomførende dokumentene utgjør følgende: dokumentasjon, oversikter, rutinebeskrivelser, instrukser og andre dokumenter som benyttes i det daglige arbeidet med informasjonssikkerhet og personvern. Ifølge dokumentet *Styringssystem Hvaler kommune* er de gjennomførende dokumentene gruppert i følgende hovedområder:

Personvernorientert	Teknologiorientert
E-post bruk	IT-reglement Hvaler kommune
Innsyn i epost og annet elektronisk materiale	Lagring av data i Office365
Skjema for innsyn i epost, personlig lagringsområde og annet elektronisk materiale	Lagring av filer i eksterne skyløsninger
Kameraovervåkning	Passord
Skjema for utlevering av kameraopptak	Antivirusprogram
Avvik personvern	Oppgradering og vedlikehold av programvare

DPIA – Personvernkonsekvensutredning	Adgang til utstyr
Gjennomføring av DPIA – Personvernkonsekvensutredning	Digitalt fjernarbeid utland
Personvernerklæring	Retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser
Retningslinjer for personvernerklæring	Styrende retningslinjer for autentiseringsløsninger
Rutine for informasjon til berørte av sikkerhetsbrudd	Konfigurasjonskontroll
Forespørsel om innsyn i elektronisk arkiv	Låserutiner og adgangskontroll
Signering av retningslinjer for ansatte	Sikkerhetsarkitektur
Innsynsbegjæring (dagligarkiv)	Beredskapsplan IKT
Mal for personvernkonsekvensutredning	
Retting og sletting av personopplysninger	
Taushetserklæring	
Taushetsplikt	

Tabell 3: Oversikt over dokumenter i internkontrollsystemet

I dokumentet *IKT-reglement Hvaler kommune* oppstilles det nærmere instrukser med hensikt om å sikre ivaretagelse av forsvarlig bruk av IKT, informasjonssikkerhet og personvern i Hvaler kommune, innenfor følgende hovedområderområder:

Område:
Tildeling, endring og sletting av tilganger
Passord, pålogging og avlogging
Fysisk sikring
Logging og sporbarhet
Søk i registre/IT-systemer/databaser
Eierskap, saksbehandling, lagring av informasjon og IKT-utstyr
Bruk av eksterne lagringsmedier
Bruk av programvare
Kartlegging av systemsvakheter
Informasjon gradert etter sikkerhetsloven
Særlige kategorier av personopplysninger
Rapportering av hendelser/avvik
Brukerstøtte
Dokumentsikkerhet
Mobiltelefoner, nettbrett, bærbare PC-er m.m.
Bruk av e-post
Bruk av internett og sosiale medier
Arbeidsgivers innsynsrett

Tabell 4: Instrukser

Det fremgår videre at IKT-reglementet skal etterleves av ansatte i Hvaler kommune, eksterne konsulenter, folkevalgte og andre som gis tilgang til kommunens IKT-relaterte utstyr og systemer, i eller utenfor kommunens lokaler.

Kontrollerende dokumenter:
Det fremgår av S*tyringsdokument for informasjonssikkerhet i Hvaler kommune* at de kontrollerende dokumentene utgjør: rutiner for å fange opp avvik og rutiner for å sikre at det gjennomføres og dokumenteres periodiske gjennomganger. Revisjonslaget er fremlagt dokumentet *Rådmannens IKT-sikkerhetsråd* som eksempel på kontrollerende dokumentasjon. Dokumentet utgjør en retningslinje hvor det er beskrevet at ledelsens gjennomgang inkluderer følgende agenda:

- Aktuelle eksterne saker (Nye retningslinjer, ny lovgivning og revisjoner)
- Aktuelle interne saker (Nye systemer, behandlinger)
- Rutiner (Styringssystem)
- Avvik i perioden (Personvern, IT sikkerhet)

Det fremkom i intervju at Hvaler kommune har utarbeidet egne rutiner for ansatte i kommunens seksjoner. Kommunen har etablert en rolle som kvalitetskoordinator som utgjør en 40%-stilling. Kvalitetskoordinator skal bistå i arbeidet med å tilse at enhetene dokumenterer og etterlever rutiner og prosedyrer. Det fremkom i intervju at Hvaler kommune er i prosess med å etablere en årlig revidering av rutinene i hver sektor, men at det fremdeles gjenstår arbeid før rutinene er etablert.

Behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene for personvernet:
Hvaler kommunes formål med behandling av personopplysninger fremgår av kommunens behandlingsprotokoll, og utgjør kommunens lovpålagte tjenester innen både helse og omsorg, oppvekst og utdanning, sosiale tjenester, tekniske tjenester, kultur og fritid, miljø og klima, samt næringsutvikling. Ifølge behandlingsprotokollen omfatter dette behandling av både ordinære og særlige kategorier av personopplysninger etter GDPR artikkel 9. De registrerte inkluderer både barn, innbyggere, eldre, ansatte, foresatte, kunder og klienter.

Det fremkom av stikkprøver at det ikke er iverksatt tiltak, som ytterligere dokumenter, rutiner og retningslinjer, som følge av risikovurdering i perioden 01.01.23-25.06.24 (for ytterligere informasjon les revisjonskriteriet 4.2.13)

4.2.2 Hvaler kommune skal ha beskrevet mål og strategi for informasjonssikkerhet og vern av personopplysninger, som legger grunnlaget for kommunens internkontroll på informasjonssikkerhetsområdet

Mål og strategi for informasjonssikkerhet og vern av personopplysninger fremgår av *Styringsdokument for informasjonssikkerhet i Hvaler kommune* og *Informasjonssikkerhetspolicy.*

Ifølge *Styringsdokument for informasjonssikkerhet i Hvaler kommune* har kommunen et overordnet mål om å etterleve personopplysningsloven, eForvaltningsforskriften og andre lover og krav som regulerer informasjonssikkerhet og personvern. Styringsdokumentet oppstiller videre krav om at kommunens IKT-sikkerhetsarbeid skal imøtekomme NSMs grunnprinsipper for IKT-sikkerhet. For å imøtekomme dette fremgår det av *Styringsdokument for informasjonssikkerhet i Hvaler kommune* at:

- Informasjonssikkerhet og personvern skal være forankret i toppledelsen, og følges opp med faste intervaller for rapportering (Kommunaldirektørens IKT-sikkerhetsråd)
- Det skal være definert eierskap til informasjon i digitale tjenester
- Informasjon i størst mulig grad skal innhentes en gang, ett sted, for deretter å gjenbrukes når det er lovmessig grunnlag for ny behandling

Det fremgår videre av dokumentet at kommunens sikkerhetsmål for informasjonssikkerhet og personvern er fordelt på tre hovedområder:

1. «Tilgjengelighet
   - Personopplysningene og annen sensitiv informasjon skal være tilgjengelig og anvendelig for autorisert bruk til beste for den registrerte, ansatte og driften.
2. Konfidensialitet
   - Personopplysninger og annen sensitiv informasjon i kommunen skal ikke være tilgjengelig for eller bli kjent for uautorisert personell eller uvedkommende.
3. Kvalitet/ Integritet
   - All personinformasjon i kommunen skal til enhver tid være korrekt, relevant og et resultat av autoriserte aktiviteter. Informasjonen skal ikke kunne endres ukontrollert.
   - Kommunen skal ha et bevisst forhold til risikoene som gjelder ved elektronisk behandling av personopplysninger. Sikkerhetstiltak skal baseres på etablerte og velprøvde løsninger som gir god margin i forhold til sikkerhetsbehovet. Ved behandling av sensitive personopplysninger skal krav til konfidensialitet ikke vike til fordel for krav til tilgjengelighet.
   - Informasjonssikkerheten i kommunen skal kontinuerlig etterprøves og forbedres. Medarbeidere skal ha tilstrekkelig kompetanse og gis nødvendig opplæring slik at tilfredsstillende informasjonssikkerhet opprettholdes.
   - Alle ansatte, elever eller andre som får tilgang til informasjon gjennom IKT-infrastruktur som Hvaler kommune eier eller leier, skal være kjent med og etterleve definerte krav til informasjonssikkerhet og personvern.»

Det fremgår av dokumentet *Informasjonssikkerhetspolicy* at kommunens informasjonsbehandling skal være i samsvar med regulatoriske, interne og avtalerettslige krav til informasjonssikkerhet. Videre skal personopplysninger og annen beskyttelsesverdig informasjon sikres på en betryggende måte gjennom fysiske, tekniske og organisatoriske tiltak. Sikkerhetsmålene er videre fordelt på fire hovedområder:

1. **«Konfidensialitet**: Personopplysninger og annen beskyttelsesverdig informasjon som behandles i Hvaler kommune skal være beskyttet mot uautorisert tilgang. Personopplysninger behandles konfidensielt og kan bare deles med andre medarbeidere i den grad det er tjenstlige behov. Personopplysninger om egne arbeidstakere kan kun behandles av den som har tjenstlig behov.
2. **Integritet**: Informasjon som Hvaler kommune har ansvaret for blir bare produsert og endret av ansatte, eller av eksterne som har fullmakt til dette. Informasjon skal ikke endres utilsiktet.
3. **Tilgjengelighet**: Informasjonssystemet er tilgjengelig for autoriserte brukere ved behov.
4. **Robusthet**: Virksomheten og informasjonssystemet er motstandsdyktig og robust. Når uønskede fysiske eller tekniske hendelser inntreffer, bidrar beredskapstiltak til å begrense skaden og at Hvaler kommune raskt kommer tilbake til normal drift. Dette inkluderer å gjenopprette tilgjengelighet og tilgang til personopplysninger i rett tid.»

Det fremgår av dokumentet *Informasjonssikkerhetspolicy* at informasjonssikkerhetsarbeidet skal være forankret i linjen og utføres systematisk, gjennomføres for å nå målene for informasjonssikkerhet, være risikobasert og følge anerkjente standarder, samt følge prinsippene for læring og kontinuerlig forbedring. Ifølge dokumentet innebærer denne strategien systematiske og periodiske risikovurderinger, risikoreduserende tiltak basert på risikovurderinger og ledelsens føringer, systematisk melding og oppfølging av hendelser som kan påvirke sikkerhetsmålene negativt, og at ledelsen styrer og følger opp informasjonssikkerhetsarbeidet systematisk.

4.2.3 Hvaler kommune skal ha etablert egnede tekniske og organisatoriske tiltak for å oppnå kommunens mål for informasjonssikkerhet og vern av personopplysninger, basert på risikovurderinger. Dette skal være dokumentert.

Det fremgår av dokumentene *Styringsdokument for informasjonssikkerhet i Hvaler kommune* og *Styringssystem Hvaler kommune* beskrivelser av dokumentasjon, oversikter, rutinebeskrivelser, instrukser og andre dokumenter som Hvaler kommunen benytter seg av i det daglige arbeidet med informasjonssikkerhet og personvern. Det følger av disse dokumentene at kommunen blant annet har beskrevet rutiner, instrukser og føringer for innsyn i e-post, kameraovervåkning, retting og sletting av personopplysninger, taushetsplikt og -erklæringer, mal og rutine for gjennomføring av personvernkonsekvensvurderinger, rutiner for å følge opp avvik, og for å sikre at det gjennomføres og dokumenteres periodiske gjennomganger. Det følger videre av disse dokumentene at kommunen har retningslinjer for lagring av data i Office 365, lagring av filer i eksterne skyløsninger, passord, antivirusprogram, oppgradering og vedlikehold av programvare, adgang til utstyr, digitalt fjernarbeid utland, autentiseringsløsninger, konfigurasjonskontroll, samt låserutiner og adgangskontroll. Revisjonslaget ble opplyst i intervjuer at kommunen har utpekt et personvernombud.

I dokumentet *IKT-reglement Hvaler* fremgår kommunens nærmere instrukser for forsvarlig bruk av IKT, som tilgangsstyring, logging og sporbarhet, brukerstøtte, nærmere instrukser om passord og bruk av eksterne lagringsmedier og programvare.

Dokumentet *Gjennomføring av risiko- og sårbarhetsanalyse* inneholder kommunens rutiner for gjennomføring av risikovurderinger. Det fremkom av stikkprøver at det ikke er iverksatt tiltak som følge av risikovurdering i perioden 01.01.23-25.06.24 (for ytterligere informasjon les revisjonskriteriet 4.2.13).

4.2.4 Hvaler kommune skal ha et internkontrollsystem på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for internkontroll for informasjonssikkerhet

Det fremgår av *Styringsdokument for informasjonssikkerhet* i Hvaler kommune at kommunens IKT-sikkerhetsarbeid baserer seg på NSMs grunnprinsipper for IKT-sikkerhet når det gjelder de tekniske tiltakene. Det ble opplyst i intervju at internkontrollsystemet for informasjonssikkerhetsarbeidet baserer seg på ISO/IEC 27001-standarden.

4.2.5 Hvaler kommune skal ha utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39

Det fremkom i intervju at Hvaler kommune har utpekt et personvernombud med en stillingsbrøk på 20%. Det ble opplyst i intervju at Hvaler kommune kjøper sine personvernsombudstjenester av Fredrikstad kommune, inkludert personvernombud. Videre fremkom det at personvernombudet også har en hjemmel på 50% som personvernombud i Fredrikstad kommune.

Det fremgår av dokumentet *Personvernombud* at personvernombudets hovedoppgave er å informere og gi råd om kommunens forpliktelser etter personvernlovgivningen. Videre fremgår det av dokumentet at personvernombudet skal:

- «involveres i alle spørsmål om vern av personopplysninger
- ha nødvendige ressurser for å utføre pålagte arbeidsoppgaver, jf. artikkel 38 (2)
- ha en uavhengig rolle og ikke motta instrukser om utførelsen av sine oppgaver
- være tilgjengelig for alle registrerte som har spørsmål eller krav knyttet til behandlingen av deres personopplysninger
- være bundet av taushetsplikt eller konfidensialitet under arbeidsutførelsen
- gi råd til den behandlingsansvarlige eller databehandleren, og til de ansatte som utfører behandlingen av personopplysninger

- se til at alle dokumenter i styringssystemet for personvern holdes oppdatert.
- tilrettelegge for registrering av behandlinger. (Eier er ansvarlig for å registrere behandlingen.)
- i samarbeid med Digitaliseringssjefen kontrollere og se til at sikkerhetsdokumentasjonen er oppdatert
- tilrettelegge for, samt rapportere fra sikkerhetsopplæringen til ansatte i kommunen
- gi råd og veiledning til behandlingsansvarlig om behandling av personopplysninger og reglene for dette
- gi råd og bistå med kontroll ved risikovurderinger
- ha oversikt over avviksbehandling om informasjonssikkerhet og personvern. Ved alvorlige brudd på personopplysningssikkerheten skal Datatilsynet varsles i h.h.t. Personopplysnings-forskriften innen 72 timer, personvernombudet gjør dette via Altinn
- forberede og gjennomføre halvårlige ledelsesgjennomganger, ansvarlig for å skrive rapport / referat
- gjennomføring av sikkerhetsrevisjoner dersom slike blir vedtatt av Rådmannens IKT-sikkerhetsråd, ansvarlig for å skrive rapport / referat
- bistå de registrerte (innbyggere/ansatte) med å ivareta deres rettigheter etter reglene om be-handling av personopplysninger
- gi Datatilsynet opplysninger dersom tilsynet ber om det, herunder foreta undersøkelser i konk-rete saker».

Det fremkom i intervju at det er bevissthet rundt personvernombudets uavhengige rolle. Det fremkom videre at Hvaler kommune ikke hadde utarbeidet tilstrekkelige skriftlige instrukser eller rutiner for per-sonvern før personvernombudet ble ansatt i 2023. Revisjonslaget ble informert i intervju om at person-vernombudet har ansvaret for å revidere dokumenter og rutiner, og bidrar til etableringen av internkon-trollsystemet for personvern. Det fremgår av dokumentasjonen at det ikke er personvernombudet som godkjenner rutinene vedkommende utarbeider, men at godkjennerrollen ivaretas av stabssjefen i Hvaler kommune. Revisjonslaget fikk dette bekreftet i intervju.

Revisjonslaget ble opplyst i intervju at etableringen av internkontrollsystemet for personvern er et pågå-ende arbeid i Hvaler kommune, og at kommunen fremdeles er i startfasen med dette arbeidet. Videre fremkom det i intervju at personvernombudet avholdt et personvernkurs høsten 2023 for alle ansatte, med mål om å gjøre alle kjent med personvernrutinene.

Det fremkom i intervju at personvernombudet rapporterer til kommunens ledelse ved halvårlige møter i Rådmannens IKT-sikkerhetsråd. Personvernombudet deltar i sikkerhetsrådet sammen med digitalise-ringssjefen og kommuneledelsen. Videre deltar personvernombudet i ukentlige møter med digitalise-ringsavdelingen i Fredrikstad kommune.

4.2.6 Hvaler kommune skal ha en beredskapsplan

Det fremgår av *Beredskapsplan Hvaler kommune* at kommunen har utarbeidet en beredskapsplan. Pla-nen tar for seg ulike hendelser og det er henvist til delplan for IKT-hendelser.

Det fremgår av *Beredskapsplan IKT* at Hvaler kommune har utarbeidet en beredskapsplan for hendelser med delvis eller totalt bortfall av kommunens data/IT-løsninger. Planen er delt opp i følgende delkapittel: 1.organisering av ressurser og ansvar, 2. varsling eksternt og internt, 3. skadebegrensning, 4. kartleg-ging/status, 5. feilretting, 6. informasjon om situasjonen og forventet tidshorisont, 7. iverksetting av kri-senettsted, 8. utstyr til organisasjonen, 9. tilgjengelige tjenester, 10. reetablering av on prem-tjenester, 11. kriseøvelser. *Beredskapsplan IKT* ble godkjent i administrasjonen18.06.24.

4.2.7 Hvaler kommune skal ha etablert og dokumentert rutiner og prosesser for gjennomføring av personvernkonsekvensvurderinger når det er sannsynlig at en behandling vil medføre en høy risiko for personvernet

Dokumentet *Styringsdokument internkontroll personvern* inneholder kommunens retningslinje og sjekkliste for gjennomføring av personvernkonsekvensvurdering. Det følger av denne retningslinjen at kommunen skal gjennomføre en personvernkonsekvensutredning (risikovurdering av personvernet) ved oppstart og store endringer av systemer, dersom behandlingen kan medføre høy risiko for den registrerte.

Det følger av *DPIA-Personvernkonsekvensutredning* at en personvernkonsekvensutredning skal gjøres når en behandling av personopplysninger omfatter mange registrerte, når behandlingen gjelder sårbare grupper og/eller når behandlingen inneholder særskilte kategorier av personopplysninger. Formålet med vurderingen angis å være «*å identifisere risiko for den registrerte og sette inn egnede tiltak slik at risikoen er innenfor de akseptkriterier kommunen har fastlagt*». Videre fremgår det av dokumentet hvem som er ansvarlig for at prosedyren utføres, tidspunkt for utførelse av prosedyren, hvilke resultater som skal oppnås, aktiviteter som inngår i vurderingen, krav til utførelse og hvem resultatet av vurderingen skal rapporteres til.

Gjennomføring av DPIA-Personvernkonsekvensutredning er en intern veileder, og det fremgår av dokumentet at det er lagt opp til en prosess med tre faser; planleggingsfasen, gjennomføringsfasen og etterarbeidet. For hver fase beskrives hvilke oppgaver og aktiviteter som bør utføres for å oppnå best mulig prosess og resultat.

Det fremkom i intervju at kommunen gjennom rutinene i Digitaliseringsrådet skal sikre at alle som bør gjennomføre en personvernkonsekvensvurdering får beskjed om å gjøre dette. I kommunens protokoll over behandlingsaktiviteter er det en egen kolonne hvor det opplyses om hvorvidt det er gjennomført risikovurdering eller DPIA for den aktuelle behandlingsaktiviteten. Det ble opplyst i intervju at kommunen har gjennomført to personvernkonsekvensvurderinger, og at personvernombudet var involvert i begge vurderingene. Hvaler kommune har fremlagt de to nevnte personvernkonsekvensvurderingene. For begge disse personvernkonsekvensvurderingene er det benyttet en mal for DPIA som er utarbeidet av Direktoratet for e-helse.

4.2.8 Hvaler kommune skal ha etablert dokumenterte rutiner og prosesser for å kunne rapportere hendelser, avvik og sikkerhetsbrudd som berører personopplysninger til Datatilsynet og de registrerte når det er nødvendig

Det fremgår av dokumentet *Avvik informasjonssikkerhet og personvern,* rutiner for avvikshåndtering, hvem som har ansvar for at rutinen etterleves, aktiviteter/eksempler på avvik og hvilke avvik som skal meldes Datatilsynet og berørte parter.

Ifølge *Avvik informasjonssikkerhet og personvern* skal avvik og brudd på informasjonssikkerheten som har medført uautorisert utlevering av sensitive personopplysninger, eller ved mistanke om slik utlevering, straks meddeles Personvernombudet som meddeler videre til Datatilsynet. Slik melding til datatilsynet skal gjøres innen 72 timer, de berørte parter skal også varsles. Kommunens plikt til å melde slike brudd på personopplysningssikkerheten til Datatilsynet innen 72 timer, følger også av kommunens *Styringsdokument internkontroll personvern.* Rutinene angir ikke hvordan slik melding til Datatilsynet skal skje.

Det fremgår av dokumentet *Retningslinje for informasjon til berørte av sikkerhetsbrudd* at Hvaler kommune har etablert en egen rutine for varsling av berørte. Det fremgår av denne rutinen at dersom personopplysninger kommer på avveie skal de registrerte informeres dersom det er sannsynlig at avviket vil medføre høy risiko for deres rettigheter og friheter.

Det fremkom i intervju at Hvaler kommune har et system for rapportering og håndtering av avvik. Avvikssystemet som benyttes er Risk Manager som er integrert med kommunens intranett «Hvalnett». I avvikssystemet registreres avvik under ulike kategorier, herunder egne kategorier for informasjonssikkerhet og personvern. Det ble opplyst at personvernavvik ikke meldes inn så ofte, men at avvikssystemet er godt kjent blant de fleste ansatte gjennom tjenesteområder hvor avvik oftere rapporteres, som helse og omsorg.

Hvaler kommune har fremlagt en oversikt over registrerte personvernavvik, som viser at det er registrert syv personvernavvik det siste året. Det fremkom i intervju at det er noe ulik forståelse blant ansatte om forskjellen på ulike typer hendelser og hvor skillet går mellom personvernavvik som bør rapporteres og ikke. Det ble uttrykt at den generelle kompetansen på dette området kunne ha vært høyere.

Det fremkom i intervju at de registrerte avvikene rapporteres i rådmannens IKT-sikkerhetsutvalg halvårlig. Videre ble revisjonslaget opplyst om at rutinene ofte gjennomgås på nytt i forbindelse med oppfølgingen av avvik, og at denne gjennomgangen ofte fører til at rutinene konkretiseres og forbedres som en del av det kontinuerlige forbedringsarbeidet i kommunen.

4.2.9 Hvaler kommune bør sikre at det er avsatt tilstrekkelige ressurser, kompetanse og handlingsrom til å arbeide med informasjonssikkerhet, samt sikre etterlevelse

Se revisjonskriteriet 4.2.12 for ytterligere informasjon om hvordan Hvaler kommune har fastsatt ansvar og roller for forebyggende sikkerhet.

Det fremkom i intervju at ressursbehovet per nå anses å være tilstrekkelig da mye av arbeidet knyttet til informasjonssikkerhet og personopplysningssikkerhet er utkontraktert til Fredrikstad kommune, som har erfaring og kompetanse innen fagområdene. Informantene opplyste om at digitaliseringsavdelingen i Fredrikstad består av 45 ressurser og at 17 av disse arbeider direkte med IKT-sikkerhet. Det fremkom videre i intervju at det er utfordrende å vurdere om det er avsatt tilstrekkelig med ressurser for arbeidet med informasjonssikkerhet da Fredrikstad kommune relativt nylig ble involvert i arbeidet. Flere av informantene påpekte at det tidligere har vært avsatt for få ressurser i kommunen. Det ble videre opplyst om at det er avsatt for få ressurser dedikert til behandlingsaktiviteter. Det fremkom i intervju at flere av ressursene opplevde å ha for lite tid til å jobbe med og prioritere opplæring innen informasjonssikkerhet.

Det fremgår av dokumentet *Informasjonssikkerhetspolicy* at Hvaler kommune har spesifisert fire ulike krav til ansattes kompetanse som skal understøtte sikkerhetsstrategien:

- «ha et bevisst forhold til virksomhetens sikkerhetsmål og målenes viktighet
- vite hvilke type informasjon de behandler og hvilke krav som stilles til deres egen informasjonsbehandling og bruk av IKT
- etterleve krav, retningslinjer, prosedyrer, rutiner mv. som gjelder for dem og det arbeidet de utfører.
- strategiene implementeres gjennom ledelsesforankrede sikkerhetsvalg.»

Det fremkom i intervju at temaet informasjonssikkerhet og personvern blir tatt opp på utvidede ledermøter. Det fremkom videre at informantene i hovedsak opplever at lederne prioriterer temaet og informerer sine ansatte.

Revisjonslaget fikk bekreftet i intervju at informantene var kjent med at det høsten 2023 ble gjennomført e-læringskurs i informasjonssikkerhet som bestod av 12 moduler med varighet på 3 minutter per modul.

Se ytterligere informasjon om kommunens opplæring innen informasjonssikkerhet og personvern under revisjonskriteriet 5.2.2.

4.2.10 Hvaler kommune bør gjennomføre risikovurderinger for informasjonssikkerhet

Det fremgår av dokumentet *Gjennomføring av risiko- og sårbarhetsanalyse* at

> *«[…] tiltakshaveren eller eier av et IT-system skal, dersom systemet inneholder personopplysninger, sensitiv informasjon, eller annen kritisk infrastruktur for å opprettholde kritiske samfunnsfunksjoner, gjennomføre risiko- og sårbarhetsanalyser før innføring av et nytt IT-system».*

Det fremgår videre av dokumentet hvilke vurderinger som kan gjøres ved risikovurderinger i Hvaler kommune. Det fremkom i intervju at alle risikovurderinger gjennomføres ved bruk av systemet Risk Manager, hvor det er mulighet for å utføre spesifikke risikovurderinger for informasjonssikkerhet og personvern. Revisjonslaget utførte stikkprøver for å få innsikt i hvordan vurderingene gjennomføres i systemet.

Det fremkom i intervju at risikovurderinger skal utføres i forbindelse med anskaffelse av systemer, i forbindelse med et avvik, samt på overordnet nivå. Det fremkom i intervju at flere kommuner i fellesskap har utført risikoanalyser og dokumentasjon innen informasjonssikkerhet. Videre fremkom det at kommunen har gjennomført risikovurderinger av arkivsystemet. Én informant opplyste om at risikovurderingene ikke utføres jevnlig.

Det fremkom i intervju at det ikke er gjennomført risikovurderinger i Risk Manager for informasjonssikkerhet og personvern i løpet av perioden 01.01.23-25.06.24. Videre ble det formidlet at det er planer om å gjennomføre workshops om risikovurderinger innen personvern ettersom at mange opplever dette som krevende. Dette er per i dag ikke igangsatt.

4.2.11 Hvaler kommune bør iverksette tiltak som blir identifisert etter gjennomføring av risikovurderinger, hendelser eller andre kontrollaktiviteter for å sikre kontinuerlig forbedring

Det fremgår av *Rådmannens IKT-sikkerhetsråd* at resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet, samt endringer i trusselbildet skal gjennomgås. Det fremgår av *Referat fra møte i rådmannens IKT-sikkerhetsråd 21.5.24* at enkelte tiltak på styrende nivå er planlagt for tiden fremover, deriblant påminnelse om gjennomføring av opplæring, samt formidle viktigheten av avviksrapportering. Det fremkom videre i intervju at Rådmannens IKT-sikkerhetsråd har vært gjennomført én gang. Videre ble det formidlet at Rådmannens IKT-sikkerhetsråd er i implementeringsfasen og at det dermed var utfordrende å uttale seg om tiltak blir iverksatt etter møtene. Det fremkom fra en av informantene at det var igangsatt tiltak om sikkerhet på reise.

Det fremgår ikke av *Retningslinje for gjennomføring av risiko og sårbarhetsanalyser* hvordan tiltak skal håndteres etter gjennomført risikovurdering. Det ble opplyst om at tiltakene håndteres gjennom modul for risikovurdering i kommunens kvalitets- og internkontrollsystem.

Det fremkom i intervju at iverksettelse av tiltak er en integrert del i avvikssystemet, og at dette blir benyttet i kommunen. Videre fremkom det i intervju at større og gjentakende avvik blir tatt opp i Rådmannens IKT-sikkerhetsråd. For ytterligere informasjon om avvikssystemet se revisjonskriteriet 4.2.14.

Det fremkom av stikkprøver at det ikke er iverksatt tiltak som følge av risikovurdering i perioden 01.01.23-25.06.24 (for ytterligere informasjon les revisjonskriteriet 4.2.13).

4.2.12 Hvaler kommune bør ha fastsatt ansvar og roller i styringsdokumenter for forebyggende sikkerhet. Disse skal være kjent i kommunen.

Det fremgår av *Styringsdokument for informasjonssikkerhet i Hvaler kommune* en oversikt over hvordan sikkerhetsorganisasjonen er fastsatt i kommunen. Sikkerhetsorganisasjonen er delt opp i «IKT-sikkerhetsråd» og «IT-sikkerhetsråd». Følgende roller inngår:

IKT-sikkerhetsråd	IT-sikkerhetsråd (under digitaliseringssjef)
Rådmann	Utviklingssjef digitalisering
Digitaliseringssjef	IT driftssjef
Personvernombud	Sikkerhetsarkitekt
Direktører	
HVO	

Tabell 5, Sikkerhetsorganisasjon i Hvaler

Det fremgår av dokumentet *Rådmannens IKT-sikkerhetsråd* at kommunens ledelse er pålagt å føre tilsyn med at Hvaler kommunes styringssystem for IKT-sikkerhet og personvern etterleves.

Det fremgår av *Styringsdokument for informasjonssikkerhet i Hvaler kommune* at IT-sikkerhetsråd bistår i det daglige med besvarelse av spørsmål om informasjonssikkerhet og personvern. Det fremkom i intervju at IT-sikkerhetsrådet ivaretar oppgaver som omhandler trusler, cyberkriminalitet etc. I tilfeller hvor det oppdages noe, skal IKT-sikkerhetsrådet rapportere til Rådmannens IKT-sikkerhetsråd.

De fastsatte rollene er beskrevet med ansvarsområder i *Styringsdokument for informasjonssikkerhet i Hvaler kommune.* Informasjonssikkerhetsansvar og behandlingsansvar er delegert til henholdsvis digitaliseringssjef og direktører. Det fremgår videre en beskrivelse av etatsleder/virksomhetsleder og ansatte. Det fremgår videre at *«alle nivåer i kommunen, som behandler informasjon i det daglige, skal involveres i arbeidet for å sikre at kommunen har tilstrekkelig informasjonssikkerhet*».

Det fremkom i intervju at flere informanter hadde kjennskap til hvem som var ansvarlig for IKT-sikkerhet, og at flere av ressursene holdt til i Fredrikstad. Flere av informantene formidlet at informasjonssikkerhetsarbeidet, med tilhørende ansvar og roller, har blitt synligere etter at Fredrikstad kommune tok over. Enkelte informanter hadde ikke kjennskap til hvem som innehar det overordnede ansvaret.

Det ble bekreftet i intervju at informantene hadde innsikt i at ledere har et overordnet ansvar for informasjonssikkerhet i enhetene. Det fremgikk av intervju at det gjerne kunne vært bedre oversikt over lederes oppfølging av om ansatte gjennomfører obligatorisk opplæring. Informantene formidlet at de selv og andre ansatte prioriterer å overholde taushetsplikten. Samtlige informanter var av den oppfatning at informasjonssikkerhet og personvern er viktig å prioritere. Videre formidlet informantene at de kjente til hva som var forventet av dem, og de hadde inntrykk av at sine kollegaer kjente til sitt ansvar.

4.2.13 Hvaler kommune bør ha et system for rapportering og håndtering av hendelser, avvik og informasjonssikkerhetsbrudd

Det fremgår av dokumentet *Avvik informasjonssikkerhet og personvern* at Hvaler kommune har et system for rapportering og håndtering av hendelser, avvik og sikkerhetsbrudd. Formålet med avviksregistreringen er beskrevet som "*å behandle uønskede hendelser i informasjonssystemene for å gjenopprette normal tilstand og hindre gjentagelse*". Videre fremgår det av dokumentet at avviksbehandlingen skal iverksettes ved sikkerhetsbrudd og/eller når oppgaver er utført i strid med de prosedyrer som er besluttet.

I dokumentene *Avvik informasjonssikkerhet og personvern, Styringsdokument for informasjonssikkerhet i Hvaler kommune* og *Retningslinje for informasjon til berørte av sikkerhetsbrudd* fremgår det at ulike enheter er ansvarlig for rapportering og håndtering av avvik, og at avvikets karakteristikker er førende for hvem som håndterer det og hvordan det skal håndteres. Dette er redegjort for i avsnittene som følger.

Det fremgår av dokumentet *Avvik informasjonssikkerhet og personvern* at den som oppdager avvik og dens leder er ansvarlig for avvikets håndtering. Selve rapporteringen av avviket utføres av personen som oppdager avviket. Om avviket er systemteknisk, behandles det av drift og utviklingssjef i virksomhet Digitalisering. Når et avvik oppstår ved en virksomhet/ etat fremgår det, av *Styringsdokument for informasjonssikkerhet i Hvaler kommune*, at leder har et overordnet ansvar for at avviket følges opp etter instruks og i samarbeid med informasjonssikkerhetsansvarlig og/eller Personvernombudet. Videre fremgår det av *Styringsdokument for informasjonssikkerhet i Hvaler kommune* at ved alvorlige sikkerhetsbrudd/ hendelser skal digitaliseringssjef varsle Nasjonal sikkerhetsmyndighet (NSM).

Etter rapportering og vurdering av avviket fremgår det av *Avvik informasjonssikkerhet og personvern* at enten "strakstiltak", eller "korrigerende tiltak" skal iverksettes. Dette er tiltak for å avgrense eventuelle følgeskader, eller permanent gjenopprette normal tilstand.

Som beskrevet i revisjonskriteriet 4.2.8 har Hvaler kommune et system for rapportering og håndtering av avvik. Se hen til revisjonskriteriet for beskrivelse av avviksprosessen.

Avvikssystemet *Risk Manager* muliggjør differensiering av avvik og forbedringsforslag. Nærmeste leder, som står ansvarlig for å lukke avviket, har mulighet til å delegere forbedringstiltak, men har ikke mulighet til å delegere ansvaret for selve avviket. Systemet har en rapportmodul som muliggjør utarbeidelse og uttak av hensiktsmessige rapporter. Rapportmodulen inkluderer funksjonen for å filtrere på avvikskategorier som personvern eller informasjonssikkerhet. Alle i kommunen har tilgang til å registrere avvik. Det fremkom i intervju at lærerne sine systemer ikke fungerer opp mot avvikssystemet, men at de har tilgang til egne PC-er for å registrere avvik.

4.2.14 Hvaler kommune bør ha system for å evaluere internkontroll for informasjonssikkerhet for å sikre kontinuerlig forbedring av arbeidet

Det fremgår av *Styringsdokument for informasjonssikkerhet i Hvaler kommune* at kommunens internkontrollsystem for informasjonssikkerhet består av rutiner for å fange opp avvik, og for å sikre at det gjennomføres og dokumenteres periodiske gjennomganger.

Videre fremgår det *av Informasjonssikkerhetspolicy* at Hvaler kommunes informasjonssikkerhetsarbeid skal følge prinsippene for læring og kontinuerlig forbedring. Det presiseres i dokumentet at dette innebærer at:

- «Risikovurderinger gjennomføres systematisk, periodisk og ved vesentlige endringer i oppgaver eller omgivelsene»
- «Ledelsen systematisk styrer og følger opp informasjonssikkerhetsarbeidet»
- «Ledelsen systematisk følger opp måloppnåelse, etterlevelse, kompetanse og kultur».

Det fremkom i intervju at Hvaler kommune er i en innføringsfase av internkontrollsystemet for informasjonssikkerhet og personopplysningssikkerhet, som innebærer at dokumentene som utgjør internkontrollsystemet tilpasses fra Fredrikstad til Hvaler kommune. Det ble opplyst om at dette arbeidet i hovedsak ble ferdigstilt i 2023. Ved endringer i rutiner og retningslinjer, sendes det ut et varsel i *Risk Manager* for alle som berøres av endringen. Videre ble det opplyst om at endringer blir lagt inn på kommunens intranettside, samt som oppsummeringsmail ved endt arbeidsuke. Hva gjelder ansvarliggjøring av at internkontrollsystemet for informasjonssikkerhet oppdateres, ble det opplyst om at ansvaret er delt mellom digitaliseringsavdelingen og personvernombudet.

Det fremkom i intervju at kommunens rutiner for rapportering av avvik sikrer kontinuerlig forbedring av internkontroll for informasjonssikkerhet og personopplysningssikkerhet. Det ble videre opplyst om at forbedringsforslagene ofte ender i reviderte rutiner og prosedyrer.

Det ble opplyst i intervju at Hvaler i liten grad har påbegynt kontrollaktivitetsarbeidet som følge av at Hvaler kommune er i en innføringsfase av internkontrollsystemet. Det ble videre opplyst om at det ikke foreligger utstrakt rapportering i leddene, samt at internkontrollaktiviteter får for lite fokus. Samtlige informanter opplyser i intervju om at kontrollaktivitetene som er innført er halvårlige møter med Rådmannens IKT-sikkerhetsråd, og at dette kun er gjennomført én gang. Det ble opplyst om at Hvaler kommune foretar evaluering av internkontrollsystemet under Rådmannens IKT-sikkerhetsråd. Her gjennomgås alle rutinerevisjoner, avviksrapporter og oppfølging av disse, nytt lovverk og konsekvensene for styringssystemet.

4.2.15 Hvaler kommune bør gjennomføre beredskapsøvelser for informasjonssikkerhet

Det fremkom i intervju at Fredrikstad kommune gjennomfører jevnlige tester av teknisk drift og kontinuitetsvurderinger, men at Hvaler kommune ikke har gjennomført beredskapsøvelser for informasjonssikkerhet. Det fremkom i et intervju at Hvaler kommune har vært med på en øvelse hvor en «bug» ble lagt inn i et helsesystem kommunen benytter seg av.

4.3 Vurderinger

Hvaler kommune har i stor grad et internkontrollsystem som er tilpasset behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene for personvernet. Internkontrollsystemet er dokumentert og består av styrende, gjennomførende og kontrollerende elementer.	Lysegrønn

Revisjonslaget vurderer at Hvaler kommune i stor grad oppfyller revisjonskriteriet. Basert på revisjonslagets overordnede gjennomgang av personopplysningene som kommunen behandler, vurderer revisjonslaget at Hvaler kommune har et internkontrollsystem som i stor grad er tilpasset behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene for personvernet. Internkontrollsystemet er dokumentert og bygd opp av styrende, gjennomførende og kontrollerende elementer som samsvarer med Datatilsynets veiledning. Styrende dokumentasjon inkluderer policyer, mål, identifiserte krav og plikter, intern organisering, ansvar og myndighet. For gjennomførende dokumentasjon har Hvaler kommune utarbeidet rutiner og retningslinjer. Når det gjelder kontrollerende elementer, har Hvaler kommune planlagt aktiviteter som ledelsens årlige gjennomgang, hvor avvik, rutiner og nye eksterne og interne saker vurderes.

Revisjonslaget vurderer imidlertid at Hvaler kommune ikke har gjennomført risikovurderinger i tilstrekkelig grad. Dette gjør det vanskelig for revisjonslaget å vurdere hvorvidt internkontrollsystemet er tilpasset behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene for personvernet, eller om det burde ha vært etablert ytterligere rutiner.

Revisjonslaget ser imidlertid positivt på at kommunen synes å ha en helhetlig tilnærming til internkontrollsystemet for informasjonssikkerhet og personvern. Dette kan bidra til både synergier og økt effektivitet.

Hvaler kommune har i tilfredsstillende grad beskrevet mål og strategi for informasjonssikkerhet og vern av personopplysninger, som legger grunnlaget for kommunens internkontroll på informasjonssikkerhetsområdet.	Grønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet om å ha beskrevet mål og strategi for informasjonssystem på en måte som dekker informasjonssikkerhetsområdet og vern av personopplysninger på en tilfredsstillende måte.

Hvaler kommune har i noen grad etablert egnede tiltak for å oppnå kommunens mål for informasjonssikkerhet og vern av personopplysninger, basert på risikovurderinger.	Gul

Revisjonslaget vurderer at Hvaler kommune i noen grad oppfyller revisjonskriteriet. Hvaler kommune har etablert flere egnede tiltak for å oppnå kommunens mål for informasjonssikkerhet og vern av personopplysninger. Revisjonslaget vurderer imidlertid at Hvaler kommune ikke har gjennomført risikovurderinger i tilstrekkelig grad. Dette gjør det vanskelig for revisjonslaget å vurdere hvorvidt de eksisterende tiltakene er tilstrekkelige, eller om det burde vært etablert ytterligere tiltak.

Hvaler kommune har i noen grad et internkontrollsystem på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for internkontroll for informasjonssikkerhet.	Gul

Hvaler kommune har i noen grad oppfylt revisjonskriteriet. Hvaler kommune har dokumentert at de baserer sitt internkontrollsystem på NSMs grunnprinsipper og redegjort for at de benytter ISO/IEC 27001-standarden. Revisjonslaget vurderer at standarden og retningslinjen kommunen benytter seg av, gir grunnlag for et velfungerende internkontrollsystem.

Det er imidlertid avdekket forbedringspotensial knyttet til utøvelsen av ISO-standarden. For å være i henhold til ISO-standarden burde kommunen gjennomført en overordnet risikovurdering med tilhørende tiltaksplan for organisatoriske og menneskelige tiltak i Hvaler kommune.

Hvaler kommune har i tilfredsstillende grad utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39.	Grønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet om at det skal utpekes et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39. Revisjonslaget vurderer også at personvernombudets adgang til å rapportere til øverste leder i kommunen er ivaretatt gjennom fast halvårlig rapportering i rådmannens IKT-sikkerhetsråd. Etter samtaler er revisjonslagets oppfatning at personvernombudet involveres i sentrale aktiviteter knyttet til personvern i kommunen. Funnene viser også at personvernombudets uavhengighet ivaretas.

Revisjonslaget ser det som positivt at personvernombudet har erfaring som personvernombud i Fredrikstad kommune. Kommunen sikrer med dette personvernombudet får utviklet sin kompetanse gjennom et tett faglig samarbeid med Fredrikstad kommune.

Hvaler kommune har i stor grad en beredskapsplan.	Lysegrønn

Hvaler kommune oppfyller i stor grad revisjonskriteriet. Det vurderes at Hvaler kommune har en grundig beredskapsplan som dekker over flere typer hendelser, samt har en delplan for IKT-hendelser. Revisjonslaget påpeker at det er mangler i kontaktlisten i planen for IKT-hendelser i form av telefonnummer.

Hvaler kommune har i tilfredsstillende grad etablert og dokumentert rutiner og prosesser for gjennomføring av personvernkonsekvensvurderinger når det er sannsynlig at en behandling vil medføre en høy risiko for personvernet.	Grønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet. Kommunens rutiner for personvernkonsekvensvurdering samsvarer med kravene i GDPR. I tillegg til en overordnet retningslinje for personvernkonsekvensvurderinger, har kommunen en dokumentert retningslinje for selve gjennomføringen av personvernkonsekvensvurderinger. Kommunens behandlingsprotokoll viser også at det er lagt til rette for å vurdere behovet for gjennomføring av personvernkonsekvensvurdering for hver enkelt behandlingsaktivitet som registreres.

Revisjonslaget vurderer at de gjennomførte personvernkonsekvensvurderingene kommunen har fremlagt inneholder de momentene som kreves etter GDPR. Det understrekes at revisjonslaget ikke har gjort en fullstendig kvalitetssikring av personvernkonsekvensvurderingene som er fremlagt. Revisjonslaget har heller ikke hatt grunnlag for å vurdere hvorvidt det burde ha vært gjennomført flere personvernkonsekvensvurderinger i kommunen.

Hvaler kommune har i tilfredsstillende grad etablert dokumenterte rutiner og prosesser for å kunne håndtere og dokumentere hendelser, avvik og sikkerhetsbrudd som berører personopplysninger, inkludert rapportering til Datatilsynet og de registrerte når det er nødvendig.	Grønn

Revisjonslaget vurderer at Hvaler kommune i stor grad oppfyller revisjonskriteriet. Kommunens system for registrering og håndtering av brudd på personopplysningssikkerheten vurderes i som tilfredsstillende. Kvalitetssystemet kommunen benytter seg av sikrer at hendelser og personvernavvik dokumenteres og rapporteres til riktig ledelsesnivå for håndtering. Videre sikrer systemet at personvernombudet involveres for å gi råd om eventuell meldeplikt til Datatilsynet og berørte registrerte. Ledelsens gjennomgang i Rådmannens IKT-sikkerhetsråd sikrer at kommunen ser avvikene i sammenheng og at kommuneledelsen informeres halvårlig.

Basert på opplysninger fra intervjuer og fremlagt oversikt over avvik, er det revisjonslagets vurdering at kommunen sikrer at personvernavvik blir registrert. Revisjonslaget bemerker at det er registrert 7 personvernsavvik. Vurdert ut fra kommunens størrelse og kompleksitet kan det anses som noe lavt.

Hvaler kommune har i stor grad sikret at det er avsatt tilstrekkelige ressurser, kompetanse og handlingsrom til å arbeide med informasjonssikkerhet, samt sikre etterlevelse.	Lysegrønn

Revisjonslaget vurderer at Hvaler kommune i stor grad oppfyller revisjonskriteriet. Kommunen har sikret ressursbehovet ved å definere flere roller innen informasjonssikkerhetsarbeidet, samt tydeliggjort deres rolle. Funnene tyder på at Hvaler kommune har hatt god effekt av å kjøpe tjenester fra Fredrikstad kommune, særlig når det gjelder ressursbehovet. Videre har kommunen inkludert alle nivåer i informasjonssikkerhetsarbeidet, noe som anses som en styrke.

Funnene viser videre at Hvaler kommune har stilt kompetansekrav og lagt opp til opplæring innen temaet. Revisjonslaget vurderer at flere av kommunens ansatte viser interesse og prioriterer informasjonssikkerhets- og personvernarbeidet. Det er dermed grunn til å anta at ansatte har kompetanse innen temaet. Det er imidlertid avdekket forbedringspotensial knyttet til kompetanse og handlingsrom til å arbeide og etterleve informasjonssikkerhetsarbeidet. Revisjonslaget har avdekket at flere ansatte ikke har gjennomført opplæringen, samt har en opplevelse av at tiden ikke strekker til for å prioritere arbeidet. På bakgrunn av dette mener revisjonslaget at Hvaler kommune med fordel kan sikre handlingsrom til å arbeide med informasjonssikkerhet. Vi viser til våre vurderinger av opplæring og bevisstgjøringstiltak og medfølgende anbefaling redegjort for i problemstilling 2.

Hvaler kommune oppfyller ikke revisjonskriteriet om at de bør gjennomføre risikovurderinger for informasjonssikkerhet	Rød

Revisjonslaget vurderer at Hvaler kommune ikke oppfyller revisjonskriteriet. Hvaler kommune har utarbeidet retningslinje og et system for å utføre risikovurderinger. På bakgrunn av funn fra stikkprøver, vurderer revisjonslaget at Hvaler kommune i ikke har gjennomført risikovurderinger for informasjonssikkerhet fra 01.01.23. Revisjonslaget bemerker imidlertid at det er utført risikovurderinger for andre områder enn informasjonssikkerhet.

Hvaler kommune iverksetter i noen grad tiltak som blir identifisert etter gjennomføring av risikovurderinger, hendelser eller andre kontrollaktiviteter for å sikre kontinuerlig forbedring.	Gul

Revisjonslaget vurderer at Hvaler kommune i noen grad oppfyller revisjonskriteriet. Funnene viser at kommunen iverksetter tiltak etter avviksrapportering, og at Rådmannens IKT-sikkerhetsråd gir mulighet for å iverksette tiltak dersom alvorlige eller gjentakende avvik forekommer.

Revisjonslaget vurderer imidlertid at Hvaler kommune ikke har gjennomført risikovurderinger eller internrevisjoner (kontrollaktiviteter) i tilstrekkelig grad. Funn fra risikovurderinger og internrevisjoner ville synliggjort aktuelle tiltak som kommunen burde iverksette. På bakgrunn av manglende planlegging og gjennomføring av kontrollaktiviteter vurderer revisjonslaget dermed at Hvaler kommune i noen grad oppfyller revisjonskriteriet.

Det skal bemerkes at Rådmannens IKT-sikkerhetsråd, og internkontrollsystemet for øvrig, er i implementeringsfasen. Dette kan medføre at tiltak ikke har blitt iverksatt hittil.

Hvaler kommune oppfyller revisjonskriteriet med å fastsette ansvar og roller i styringsdokumenter for forebyggende sikkerhet. Disse skal være kjent i kommunen.	Grønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet om å fastsette ansvar og roller i styringsdokumentene. Rollene og ansvaret er kjent i kommunen.

Funnene viser imidlertid at ikke alle ansatte er kjent med alle styrende roller i kommunen. Revisjonslaget vurderer likevel at det ikke kan kreves at enhver ansatt er kjent med den øverste organiseringen innen sikkerhet og personvern og at det viktigste er at ansatte er kjent med eget og leders ansvar.

Hvaler kommune oppfyller revisjonskriteriet om å ha et system for rapportering og håndtering av hendelser, avvik og informasjonssikkerhetsbrudd	Grønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet om å ha et avvikssystem hvor rapportering og håndtering av informasjonssikkerhets- og personvernhendelser kan foregå. Systemet sikrer både ansvarliggjøring og håndtering. Dersom et avvik ikke blir lukket, sendes det videre i systemet. Dersom større avvik eller gjentakende avvik forekommer, tas det opp i ledergruppen.

Hvaler kommune har i stor grad et system for å evaluere internkontroll for informasjonssikkerhet for å sikre kontinuerlig forbedring av arbeidet	Lysegrønn

Revisjonslaget vurderer at Hvaler kommune i stor grad oppfyller revisjonskriteriet. Funnene viser at Hvaler kommune har et avvikssystem som de evaluerer både ved Rådmannens IKT-sikkerhetsråd, samt på lavere nivå når tiltak kan iverksettes. Det vurderes at Hvaler kommune har mål og delegert ansvar for kontinuerlig forbedring, samt utførelse av evalueringsaktiviteter i Rådmannens IKT-sikkerhetsråd. Revisjonslaget har identifisert mangler knyttet til kontrollaktiviteter, og at dette bør inngå i evalueringen.

Det må bemerkes at Hvaler kommune er i implementeringsfasen. Dette kan forklare hvorfor kontroll av etterlevelse mangler per i dag.

Hvaler kommune oppfyller ikke revisjonskriteriet om å gjennomføre beredskaps-øvelser for informasjonssikkerhet	Rød

Revisjonslaget vurderer at Hvaler kommune ikke oppfyller revisjonskriteriet. Kommunen mangler gjennomføring av beredskapsøvelser innen informasjonssikkerhet hvor Hvaler kommune håndterer og samarbeider med Fredrikstad. Mangel på gjennomføring av beredskapsøvelser kan ses i sammenheng med manglende identifisering av IKT-hendelser i overordnet risikovurdering.

4.4 Konklusjon og anbefalinger

Revisjonslaget konkluderer, basert på den gjennomførte revisjonen, med at Hvaler kommune har et internkontrollsystem som i stor grad inneholder forventede elementer etter anerkjente standarder og regulatoriske krav. Det er avdekket enkelte avvik som Hvaler kommune bør prioritere videre for å oppfylle regulatoriske krav.

Hvaler kommune jobber grundig med etablering av internkontrollsystem innen informasjonssikkerhet og personopplysningssikkerhet. Dokumentasjon i form av policyer, prosedyrer og rutiner, samt ansvarsfordeling og målsetning innen henholdsvis informasjonssikkerhet og personopplysningssikkerhet vurderes som tilfredsstillende.

Det er imidlertid avdekket funn som kan redusere kvaliteten av internkontrollsystemet, og fører til at systemet ikke inneholder alle forventede elementer etter anerkjente standarder og regulatoriske krav. Hvaler kommune har i liten grad gjennomført risikovurderinger innen informasjonssikkerhet, noe som kan medføre at risikoene ikke er kjent og ikke håndteres på riktig måte. Manglende risikovurderinger gjør det også vanskelig å konkludere med at internkontrollsystemet er tilstrekkelig. Videre er det avdekket manglende kontrollerende elementer, noe som medfører at kommunen ikke oppfyller krav i anerkjente standarder. Det skal imidlertid bemerkes at Hvaler kommune er i etableringsfasen av internkontrollsystemet, og at kontrollerende elementer kan tilkomme på et senere tidspunkt. Avslutningsvis er det avdekket mangler knyttet til beredskapsøvelser innen informasjonssikkerhet.

Anbefalinger

I revisjonsrapporten skilles det mellom *regulatoriske krav* og *beste praksis-krav* (viser til 3.2 om revisjonskriterier for ytterligere informasjon). De regulatoriske kravene formuleres som «Hvaler kommune bør», og beste praksis formuleres som «Hvaler kommune bør vurdere». Kravene skilles fra hverandre i tiltakene som listes opp.

Basert på revisjonslagets vurderinger og konklusjon anbefaler revisjonslaget at Hvaler kommune bør:

- gjennomføre risikovurdering for å sikre at omfang og innretting av internkontrollen er tilpasset relevante personvern- og informasjonssikkerhetsrisikoer. Videre bør det gjennomføres oppdaterte risikovurderinger på personvernområdet for alle behandlingsaktiviteter i kommunen. Risikovurderingene bør fastsettes basert på en prioritert liste. Formålet med risikovurderingen bør være å:
    - vurdere hvorvidt eksisterende sikkerhetstiltak er tilstrekkelig, eller om det burde vært etablert ytterligere.
    - vurdere hvorvidt internkontrollsystemet er tilstrekkelig, eller om det burde ha vært etablert ytterligere rutiner. Hva som anses som tilstrekkelig er en kontinuerlig prosess og må bestemmes ut fra risikobildet.
    - vurdere tiltak i kommunens beredskapsplan.

Basert på revisjonslagets vurderinger og konklusjon anbefaler revisjonslaget at Hvaler kommune bør vurdere å:

- legge til telefonnummer til kontaktene i beredskapsplanen for IKT-hendelser.
- gjennomføre kontrollaktiviteter av internkontrollsystemet i sin helhet, samt aktiviteter som inngår. Dette sikrer at Hvaler kommune kan teste og vurdere sikkerhetstiltakenes effekt, samt etterlevelse av regulatoriske krav.

- implementere og øve på beredskapsplanen for IKT-hendelser. Hensikten er å kontrollere og teste beredskapsplanverket for å sikre at det fungerer som planlagt. Videre vil øvelser teste samarbeidet og kommunikasjonen mellom Hvaler og Fredrikstad i krisehendelser som omhandler informasjonssikkerhet. Dette vil bli et regulatorisk krav dersom Hvaler kommune identifiserer IKT-hendelser som en risiko ved utførelse av helhetlig risiko- og sårbarhetsanalyse (jf. § 2 forskrift om kommunal beredskapsplikt).

Revisjonslaget gjør oppmerksom på at dette ikke er ment som en fullstendig liste over nødvendige tiltak, men en vurdering av de mest vesentlige. Kommunen må selv vurdere hva som er nødvendige tiltak til enhver tid. Det er således ingen garanti at revisjonskriteriene etterleves 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 PROBLEMSTILLING 2

Har Hvaler kommune gjort internkontrollsystemer for informasjonssikkerhet og personopplysningssikkerhet kjent i kommunen og etterleves det?

5.1 Revisjonskriterier

Hvaler kommune bør:

- sikre at ansvar og myndighet innen informasjonssikkerhet er delegert og kommunisert (ISO/IEC 27001)
- ha opplæring og bevisstgjøringstiltak for å sikre at alle ansatte er bevisst eget ansvar for informasjonssikkerhet (ISO/IEC 27001, ISO/IEC 27701, Digdir: Internkontroll i praksis – kompetanse- og kulturutvikling)
- sikre at ansatte blir informert om eventuelle endringer i internkontroll for informasjonssikkerhet (Digdir: Internkontroll i praksis - Informasjonssikkerhet)
- sikre at ansatte kjenner til rutiner for varsling av informasjonssikkerhetshendelser (Digdir: Internkontroll i praksis - Informasjonssikkerhet).

5.1 Datagrunnlag

5.1.1 Hvaler kommune bør sikre at ansvar og myndighet innen informasjonssikkerhet er delegert og kommunisert

Viser til revisjonskriteriet 4.2.12 for ytterligere informasjon om roller og ansvar innen informasjonssikkerhet i Hvaler kommune.

Det fremgår *Styringsdokument for informasjonssikkerhet i Hvaler kommune* følgende ansvar og myndighetsfordeling:

- etatsleder/ virksomhetsleder skal sikre at de ansatte gjennomfører nødvendig opplæring og har kjennskap til regler og rutiner
- informasjonssikkerhetsansvarlig har ansvar for "å organisere faste møter for kompetanseheving og erfaringsdeling for alle som jobber med informasjonssikkerhet"
- personvernombudet "tilbyr (…) opplæring internt i kommunen", samt "driver holdningsskapende arbeid og gjøre ledelsen og ansatte kjent med sitt ansvar".

Det ble opplyst i intervju at informantene kjenner til eget ansvar og myndighet innen informasjonssikkerhet og personopplysningssikkerhet. I enkelte intervju fremkom det at informantene ikke var kjent med roller og ansvar utover ens egen enhet. Det ble videre opplyst om at ansvaret hovedsakelig ligger hos rådmannen som delegerer til kommunalsjefer, som igjen delegerer til enhetsledere. Enhetsledere har igjen et ansvar for å videreformidle budskapet til de ansatte. Det fremkom videre at enhetslederne har enhetsledermøter med personvernombudet, og at dette bidrar til at ansvar og myndighet blir kjent for dem.

5.1.2 Hvaler kommune bør ha opplæring og bevisstgjøringstiltak for å sikre at alle ansatte er bevisst eget ansvar for informasjonssikkerhet

Det fremgår av *Adgang til utstyr* at alle nye brukere av kommunens datasystem må utføre obligatorisk opplæring om datasystemene. Det fremkom i intervju at nyansatte får tilsendt opplæringsmateriell når de tiltrer i stillingen. Det fremkom i intervju at enkelte ansatte ikke hadde fått tilsendt kurset ved ansettelse. Et av områdene de ansatte må gjennomgå er personvern og informasjonssikkerhet. Det ble i intervjuet gjennomført stikkprøver av opplæringsmateriellet innen områdene. Det fremgår videre av dokumentet *Adgang til utstyr* at leder mottar en månedlig rapport av antall personer som har gjennomført opplæringen. Det fremkom videre at ledere ikke mottar oversikt over navn på ansatte som mangler gjennomføring av opplæringen. Det er sektorene selv som er ansvarlige for at nyansatte gjennomfører opplæringen.

Videre fremkom det av intervju at ansatte skal signere ulike erklæringer ved tiltredelse i stillingen. Det fremgår av *Signering av GDPR- og IKT-retningslinjer for ansatte* at ansatte skal ha lest og forstått innholdet i *IKT-reglement i Hvaler kommune* og forplikter seg til å etterleve reglene i arbeidet i kommunen (Viser til revisjonskriteriet 4.2.1 for ytterligere informasjon om innhold i dokumentet).

Videre fremkom det i intervju at Hvaler kommune gjennomførte opplæring om informasjonssikkerhet og personvern i form av e-læring høsten 2023. De ansatte fikk tilsendt ett tema innen området i 12 uker. Revisjonslaget gjennomførte stikkprøver av statistikk for gjennomføring av opplæringen om informasjonssikkerhet og personvern, hvor det fremkom at 30-40% hadde startet på opplæringen. Innen opplæringen «personvern» og «grunnleggende om personvern» hadde 65-66% påbegynt opplæringen. Det fremkom videre i intervju at enhetsledere også får opplæring om personvern fra personvernombudet i kommunen.

Det fremkom i intervju at informantene var kjent med viktigheten av å verne om informasjon og overholde taushetsplikten. Det fremkom videre en oppfatning av at ansatte viser en interesse for feltet ettersom de ofte diskuterer hvem som har *behov* for kjennskap til ulik informasjon i det daglige. Informantene ga eksempler på hvordan vern om personopplysninger overholdes i praksis. Det fremkom i intervju at ansatte kan oppleve utfordringer knyttet til overholdelse av personvernreglene da Hvaler kommune er liten av størrelse. Videre at det kan forekomme situasjoner der informasjon blir delt dersom en person hører til flere instanser.

Enkelte informanter opplyste om at det er ikke er avsatt tilstrekkelig ressurser for å prioritere opplæringsarbeidet. Det ble videre informert om at enkelte savner et system knyttet til opplæringsarbeidet. Andre informanter la vekt på at det har vært mindre fokus på kompetansehevende arbeid i kommunen, og at de ønsker kurs i informasjonssikkerhet og personvern. Informantene opplyste videre at det er mangler knyttet til informasjonsdeling over digitale plattformer, samt hva som inngår som «de mest sensitive personopplysningene». Enkelte formidlet at noen ledere er opptatt av temaet, mens andre ikke har et like stort fokus på dette.

Flere informanter opplyste om at systemene de benytter er lagt opp på en måte som gjør det naturlig for ansatte å ta hensyn til informasjonssikkerhet og personvern. En informant beskrev dette som en styrke i de tilfellene der opplæringen eventuelt ikke har nådd ut til alle ansatte.

Det ble opplyst i intervju at Digitaliseringsrådet jobber med å opprette et tettere samarbeid med Fredrikstad kommune for å sikre kompetanseoverføring av IKT-sikkerhet.

5.1.3 Hvaler kommune bør sikre at ansatte blir informert om eventuelle endringer i internkontroll for informasjonssikkerhet

Viser til revisjonskriteriet 4.2.15 for beskrivelse av hvordan ansatte blir informert ved endringer i systemet i etterkant av avviksrapportering.

Det fremkom av intervju at hver enkelt tjenesteleder står ansvarlig for lokale rutiner, og skal informere ansatte ved endringer. Som beskrevet i revisjonskriteriet 4.2.1, bistår kvalitetskoordinator i Hvaler kommune med å sikre at rutinene gjennomgås jevnlig. Det fremkom i enkelte intervjuer at informantene opplever manglende informasjon om endringer i rutinene.

Flere av retningslinjene og prosedyrene har versjonsnummer 1.0 og godkjenningsdato fra våren 2024. Det fremkom i intervju at versjonsnummer 1.0 betyr at dette er første versjon i Hvaler kommune av de gjeldende dokumentene.

5.1.4 Hvaler kommune bør sikre at ansatte kjenner til rutiner for varsling av informasjonssikkerhetshendelser

Viser til revisjonskriteriet 5.2.1 for informasjon om tiltak som bidrar til kjennskap av rutiner i Hvaler kommune.

Det fremkom i intervju at ansatte har fått fysisk og elektronisk opplæring om avvikshåndtering. Samtlige informanter opplyste om at de visste hvordan avvik skulle rapporteres. Gjennom stikkprøver fikk revisjonslaget innsikt i hvordan ansatte kan gjennomføre dette. Videre fremkom det at enhetsledere er ansvarlige for at ansatte innen tjenesteområdet har nødvendig kunnskap om rutine for varsling om informasjonssikkerhetshendelser.

Det fremkom i intervju at det trolig rapporteres inn for lite avvik innen informasjonssikkerhet og personvern. Det fremgår av *Referat fra møte i rådmannens IKT-sikkerhetsråd* at det har vært åtte avvik innen informasjonssikkerhet og personvern, hvorav det første av de innmeldte avvikene var datert til 17.08.2023. Det fremkom videre i intervju at det er behov for å etablere en avvikskultur i kommunen.

5.2 Vurderinger

Hvaler kommune har sikret at ansvar og myndighet innen informasjonssikkerhet er delegert og kommunisert	Grønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet. Kommunen har fordelt roller og ansvar, samt kommunisert forventninger til ansatte og ledere. Vurderingen forsterkes av funnene som viser at samtlige informanter kjenner til sin egen rolle.

Det er imidlertid funn som viser at enkelte informantene opplever lite synlighet fra kommunens ledelse innen informasjonssikkerhetsarbeidet.

Hvaler kommune har i stor grad opplærings- og bevisstgjøringstiltak for å sikre at alle ansatte er bevisst eget ansvar for informasjonssikkerhet	Lysegrønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet. Kommunen har etablert et opplæringsprogram av god kvalitet, særlig ved bruk av e-læringsprogrammet fra høsten 2023. Funnene viser at de fleste har mottatt opplæringsmateriell ved ansettelse, og andre ikke. Det fremstår videre som det er noe varierende gjennomføring av opplæring, og revisjonslaget argumenterer for at kommunen bør sikre at dette gjennomføres og blir satt i system. Her tillegges særlig leders ansvar for å sikre at ansatte gjennomfører obligatorisk opplæring. Funnene viser at enkelte ansatte savner ytterligere opplæring innen temaet, særlig da det stilles spørsmål ved enkelte områder. Funnene viser videre at ledere ikke mottar oversikt over hvilke ansatte som mangler gjennomføring, noe som kan påvirke lederes mulighet til å identifisere manglende gjennomføring. Det må bemerkes at noe av opplæringsmateriellet nylig har kommet på plass.

Personvernombudet opplyser til revisjonslaget i møte 12. september 2024 om presentasjon av forvaltningsrapporten for Hvaler kommune at mangler knyttet til å filtrere hvilke ansatte som har gjennomført opplæring er rettet opp i.

Hvaler kommune har sikret at ansatte blir informert om eventuelle endringer i internkontroll for informasjonssikkerhet	Grønn

Revisjonslaget vurderer at Hvaler kommune tilfredsstiller revisjonskriteriet. Hvaler kommune har et velfungerende system for å oppdatere ansatte om endringer ved bruk av oppsummeringsmail, meldinger på intranett og informasjon fra ledere/ansvarlige. Det må bemerkes at kommunen må videre arbeide med andre områder hvor det kan forekomme endringer etter arbeidet (eksempelvis risikovurderinger), og at dette bør utbedres i takt med internkontrollsystemets implementering.

Hvaler kommune har i stor grad sikret at ansatte kjenner til rutiner for varsling av informasjonssikkerhetshendelser	Lysegrønn

Revisjonslaget vurderer at Hvaler kommune i stor grad oppfyller revisjonskriteriet. Kommunen har gjort de ansatte kjent med rutiner for varsling ettersom det fremgår av samtlige intervju at informantene har kjennskap til dette. Det er imidlertid funn som viser at det er rapportert relativt få avvik innen informasjonssikkerhet og personvern, noe som tyder på at arbeidet bør prioriteres videre.

5.3 Konklusjon og anbefalinger

Revisjonslaget konkluderer, basert på den gjennomførte revisjonen, med at Hvaler kommune har etablert et internkontrollsystem for informasjonssikkerhet og personvern som er kjent i kommunen. Det er ikke avdekket alvorlige avvik knyttet til problemstilling 2. Revisjonens funn viser at både ansatte og ledere i stor grad kjenner til sin rolle og sitt ansvar. Kommunen har de siste årene kommet godt i gang med etablering av internkontrollsystemet, men er fremdeles i en implementeringsfase. Det gjenstår arbeid for å sikre at internkontrollarbeidet og ansvarsrollene etterleves, men ut fra revisjonslagets forståelse etterlever en stor del av ansatte og ledere det som forventes av dem.

Anbefalinger

I revisjonsrapporten skilles det mellom *regulatoriske krav* og *beste praksis-krav* (viser til 3.2 om revisjonskriterier for ytterligere informasjon). De regulatoriske kravene formuleres som «Hvaler kommune bør», og beste praksis formuleres som «Hvaler kommune bør vurdere». Listen nedenfor inneholder kun formuleringer som sistnevnte («bør vurdere»).

Basert på revisjonslagets vurderinger og konklusjon anbefaler revisjonslaget at Hvaler kommune bør vurdere å:

- strukturere opplæring innen informasjonssikkerhet ved å:
    - innføre obligatorisk opplæring for nye og nåværende ansatte som gjentas jevnlig.
    - sørge for at gjennomført opplæring blir dokumentert.
- styrke kulturen for rapportering av personvern- og informasjonssikkerhetsavvik samt øke ansattes bevissthet og kompetanse på området. Dette kan omfatte utvikling og gjennomføring av opplæringsprogrammer eller workshops som øker ansattes forståelse av hva som utgjør et personvern- og informasjonssikkerhetsavvik, samt viktigheten av å rapportere alle typer avvik, inkludert mindre alvorlige hendelser. Det kan også inkludere etablering av enkle og tydelige sjekklister for identifisering og rapportering av avvik, slik at alle ansatte enkelt kan følge opp og handle riktig.

Revisjonslaget gjør oppmerksom på at dette ikke er ment som en fullstendig liste over nødvendige tiltak, men etter revisjonslaget vurdering de mest vesentlige. Kommunen må selv vurdere hva som er nødvendige tiltak til enhver tid. Det er således ingen garanti at revisjonskriteriene etterleves 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 Hvaler kommune

- Beredskapsplan Hvaler kommune
- Rutiner for kriseledelse og krisestab
- Adgang til utstyr
- Antivirus
- Avvik informasjonssikkerhet og personvern
- Behandlingsprotokoll fra liste
- Beredskapsplan IKT
- Databehandleravtale
- Digitale sport og taushetsplikt
- Digitalt fjernarbeid
- DPIA – Personvernkonsekvensvurdering
- Gjennomføring av DPIA – personvernkonsekvensutredning
- IKT-reglement Hvaler kommune
- Informasjonssikkerhetspolicy
- Innsyn i elektroniske spor
- Ivaretakelse av informasjonsplikten
- Konfigurasjonskontroll
- Lagring av data i kommunens O365
- Lagring av filer i eksterne skyløsninger
- Låserutiner og adgangskontroll
- Oppgradering og vedlikehold av programvare
- Organisasjonskart Hvaler kommune
- Oversikt avvik
- Passord
- Personvernombud
- Rådmannens IKT-sikkerhetsråd
- Referat fra møte i rådmannens IKT-sikkerhetsråd 21.05.24
- Retningslinje for gjennomføring av risiko og sårbarhetsanalyser
- Retningslinje for informasjon til berørte av sikkerhetsbrudd
- Retting og sletting av personopplysninger
- Riktig bruk av e-post
- Signering av GDPR – og IKT-retningslinjer for ansatte
- Styringsdokument for informasjonssikkerhet i Hvaler kommune
- Styringsdokument internkontroll personvern
- Styringssystem Hvaler kommune
- Taushetsplikt
- Teams videomøter

Informanter

- Rune Willy Antonsen – Rådmann
- Ketil Bjørge Johansen – Digitaliseringssjef
- Synnøve Zynne Tilrem – Personvernombud
- Anne-Kari Haakenstuen – Stabssjef
- Lise Krogstad – Kvalitetskoordinator
- Øystein Myksvoll Lande – Rektor
- Amund Bjørke – Kommunalsjef helse og friskliv
- Martin Ludvig Lund – Ansatt i skole, oppvekst og kultur
- Kristine Kirkenes – Ansatt i helse og friskliv

Stikkprøver

- Stikkprøve av risikovurderingssystemet
- Stikkprøve av tiltak etter risikovurderinger
- Stikkprøve av opplæringsmaterialet
- Stikkprøve av statistikk for gjennomført opplæring
- Stikkprøve av registrering av avvik

Referanser

- Forskrift om kommunal beredskapsplikt (2011) *Forskrift om kommunal beredskapsplikt* (FOR-2011-08-22-894). Lovdata. https://lovdata.no/dokument/LTI/forskrift/2011-08-22-894
- Standard Norge. (2022) *Ledelsessystemer for informasjonssikkerhet* (NS-ISO/IEC 27001:2023). https://online.standard.no/nb/ns-en-isoiec-27001-2023
- Nasjonal sikkerhetsmyndighet (2020, 01. juli) *Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester.* Nasjonal sikkerhetsmyndighet. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/
- Personopplysningsloven (2018) *Lov om behandling av personopplysninger* (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysning
- Personopplysningsloven (2018) EUs generelle personvernforordning 2016/679 av 27. april 2016 (GDPR). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr#KAPITTEL_gdpr
- Datatilsynet (2018) *Informasjonssikkerhet og internkontroll.* https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/
- Nasjonal sikkerhetsmyndighet (2020) *Grunnprinsipper for IKT-sikkerhet*. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/introduksjon/
- Digitaliseringsdirektoratet (u.å) Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet. https://www.digdir.no/informasjonssikkerhet/kompetansebeskrivelser-roller-innen-styring-og-kontroll-av-informasjonssikkerhet/1107