Revisjon Øst IKS

FORVALTNINGSREVISJONSRAPPORT

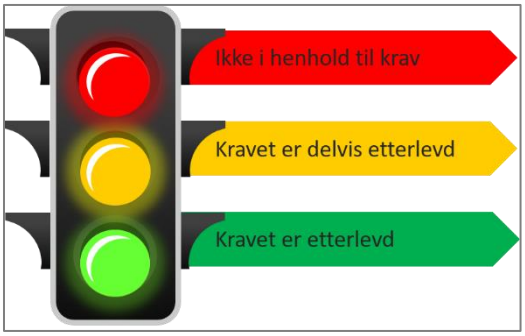
Informasjonssikkerhet

VÅLER KOMMUNE 2023

Postboks 84, 2341 Løten
Telefon: 62 43 58 00
https://www.revisjon-ost.no
E-post: post@rev-ost.no
Org. nr.: 974 644 576 MVA

Forord – om rapporten

Denne rapporten er bygget opp med et kort sammendrag som går gjennom hovedfunnene og konklusjonen i forvaltningsrevisjonsprosjektet i første kapittel.



Vi har valgt å benytte en «trafikklysmodell» for å illustrere hva vi mener er i henhold til krav på området, det som er godkjent med merknad, og det som ikke er i henhold til krav på området. Hver vurdering blir merket med henholdsvis grønt, gul/oransje og rødt.

Rapporten er utarbeidet med et digitalt tilsnitt og innehar lenker til ulike seksjoner av rapporten. Dette skal gjøre det enklere for leseren å navigere i rapportens innhold. Det er også lenket til de kilder som er digitalt tilgjengelige, for en mer interaktiv opplevelse av rapporten.

Rapporten er bygget opp etter NKRFs krav til sluttrapport i Standard for forvaltningsrevisjon (RSK 001). Dette innebærer minstekravene til

- sammendrag (kap. 1),
- informasjon om bestillingen (kap. 2 og 3),
- problemstillingene (kap. 6-8),
- valg av metoder og vurdering av datagrunnlag (kap. 5),
- revisjonskriterier (kap. 4 og vedlegg A),
- presentasjon av data (kap. 6-8),
- vurderinger (kap. 6-8),
- konklusjon (kap. 9),
- anbefalinger (kap. 10),
- referanser (kap. 12) og
- kommunedirektørens uttalelse (kap. 11).

I tråd med RSK 001, ønsker vi å fremheve at vi vektlegger at forvaltningsrevisjoner skal «bidra til et godt beslutningsgrunnlag for de folkevalgtes styring og kontroll, og å bidra til læring».

Vi vil takke kontrollutvalget for oppgaven, og administrasjonen for tilrettelegging for en best mulig og effektiv gjennomføring av forvaltningsrevisjonsprosjektet.

Vi håper at leseren finner nytte i rapporten og vil benytte denne videre i forbindelse med en trygg og god forvaltning av tjenesteområdet.

Løten, den 20. desember 2023

Magnus Michaelsen
Oppdragsansvarlig forvaltningsrevisor

Jo Erik Skjeggestad
Utøvende forvaltningsrevisor

Innholdsfortegnelse

1 Sammendrag 4
2 Bakgrunn for prosjektet 7
3 Aktualitet, formål og problemstillinger for forvaltningsrevisjonen 7
4 Revisjonskriterier 8
5 Metode for revisjonen 8
5.1 Dokumentstudier 8
5.2 Intervjuer 9
5.3 Spørreundersøkelse 9
6 Problemstilling 1 – Planverk, retningslinjer og rutiner 11
6.1 Revisjonskriterier for problemstilling 1 11
6.2 Innhentet data 12
6.3 Revisors vurdering 23
7 Problemstilling 2 – Implementering av sikkerhetstiltak 28
7.1 Revisjonskriterier for problemstilling 2 28
7.2 Innhentet data 29
7.3 Revisors vurdering 37
8 Problemstilling 3 – Praktisering av informasjonssikkerhet 42
8.1 Revisjonskriterier for problemstilling 3 42
8.2 Innhentet data 42
8.3 Revisors vurdering 47
9 Konklusjon 51
10 Anbefalinger 54
11 Kommunedirektørens uttalelse 56
12 Referanser 57
12.1 Internettreferanser 57
Vedlegg A: Utledning av revisjonskriterier 58

1 Sammendrag

Formålet med denne forvaltningsrevisjonen har vært å se etter om Våler kommune tilfredsstiller sentrale lovkrav og anbefalinger for informasjonssikkerhet. Formålet er belyst ved å besvare følgende problemstillinger:

1. Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte?
2. Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?
3. I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

I forbindelse med forvaltningsrevisjonen er det utledet revisjonskriterier fra lovverk, veiledere og anbefalinger fra KS, samt statlige myndigheter. Grunnlagsdata til forvaltningsrevisjonen er innhentet ved dokumentgjennomgang, intervjuer og en spørreundersøkelse rettet mot de ansatte i kommunen. I det følgende oppsummeres konklusjonene for den enkelte problemstilling.

Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte?

Vi konkluderer med at det i noen grad er etablert helhetlige planer og styringsdokumenter som skal ivareta helheten, og retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet.

Når det gjelder helhetlige planer og styringsdokumenter, har kommunen en del på plass. Hovedplanen for IKT-området, kommunens e-strategi, gjaldt imidlertid fra 2018-2021 og er ikke dekkende for dagens situasjon. Vi oppfatter videre at informasjonssikkerhet rundt om i kommunen i stor grad er noe som fortrinnsvis overlates til IKT-avdelingen. Systemet for internkontroll knyttet til informasjonssikkerhet er under planlegging. Viktige deler som systematiske risikovurderinger utarbeidelse av tiltaksplaner der risikoen er høy, kontroll og rapportering i tilknytning til oppfølging av internkontrolltiltakene, og jevnlige gjennomganger på området fra ledelsens side er etter hva vi kan se ikke iverksatt. Det er heller ikke klarlagt hva som kan aksepteres av risiko på området, noe som er en viktig forutsetning for systematiske risikovurderinger. Anbefalinger fra KS og statlige myndigheter tilsier at kommuneledelsen gjennomgår aktiviteten på IKT-området årlig. For helse- og omsorgstjenestene kreves det at ledelsens gjennomgang dokumenteres.

Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?

For denne problemstillingen kan vi konkludere med at kommunen stort sett har implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang. Forbedringspunkter i denne forbindelse kan knyttes til systematikk rundt risikovurderinger og at anbefalte sikkerhetstiltak, overvåkning og testing av IKT-systemene og håndtering av avvik gjennomføres mer planmessig enn i dag og rapporteres til kommunens ledelse. Vi mener videre at kommunen kan bli bedre på planlegging for håndtering av uønskede hendelser og å øve på slike.

Vi mener det er viktig at det gjennomføres systematiske risikovurderinger ute i kommunens enheter/virksomheter. Dette er blant annet basert på spørreundersøkelsen som viser at det er behov for større fokus knyttet til risiko innen informasjonssikkerhet. Selv om de ulike delene av IKT-området gjennomgås med hensyn til sikkerhet, mener vi at Nasjonal sikkerhetsmyndighet sine anbefalinger tilsier en mer planmessig gjennomgang, overvåkning og testing av de ulike deler av IKT-området enn hva Våler kommune gjennomfører i dag. Det at det ikke gjennomføres planmessig, øker risikoen for at faresignaler kan bli oversett. Vi kan heller ikke se at helse- og omsorgstjenestene planlegger og gjennomfører sikkerhetsrevisjoner for informasjonssikkerhet slik det er krav om, og at dette dokumenteres.

Kommunen har retningslinjer for utarbeidelse av katastrofeberedskap og en egen prosedyre for planlegging av utilsiktede avbrudd på IKT-området. Vi kan imidlertid ikke se at dette følges opp med lokale beredskapsplaner ute i enhetene/virksomhetene. Det øves heller ikke spesielt på håndtering av uønskede hendelser og krisehåndtering i tilknytning til informasjonssikkerhet, selv om alternativ drift har fungert der beredskapen er prøvd ut i praksis.

I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

Vår konklusjon er at kommunen har et forbedringspotensial med hensyn til systematisk oppfølging når det gjelder planer, rutiner og sikkerhetstiltak. Slik systematikk er viktig for å sikre at planer, rutiner og sikkerhetstiltak følges opp i kommunens enheter og av den enkelte ansatte.

Kommunen har rutiner for å sikre at de som ansettes i kommunen kjenner til de krav kommunen stiller når det gjelder informasjonssikkerhet. Det finnes imidlertid ingen fast rutine for å bekjentgjøre endringer i planer, rutiner og lignende til de som allerede er ansatt i kommunen, eller en plan for oppfriskning av kunnskap om informasjonssikkerhet. Resultatene fra spørreundersøkelsen til de ansatte tyder på at det er få ansatte som kjenner til kommunens strategi og regler for informasjonssikkerhet. Vi mener også at det er en litt for stor andel som oppgir at de ikke etterlever sentrale regler på området.

Planer, reglementer og rutiner oppbevares i kvalitetssystemet Compilo og det er fastsatt rutiner for ajourhold av dokumentene. Det er likevel tilfeldig hvordan denne rutinen etterleves. Vi kan ikke se at kommunen har rapporteringsrutiner som sikrer oppfølging og evaluering av planer, reglementer og rutiner knyttet til informasjonssikkerhet, selv om det foreligger planer om å innføre slik rapportering.

Spørreundersøkelsen til de ansatte viser at det er en ganske stor andel som oppgir at de ikke har fått opplæring innen informasjonssikkerhet. Stort sett er opplæringen relatert til den enkeltes arbeidsoppgaver, selv om opplæring/informasjon knyttet til informasjonssikkerhet ofte er basert på innspill fra eksterne samarbeidspartnere. Vi mener kommunen vil være tjent med å gjennomføre mer systematiske kartlegginger av opplæringsbehovet der en spør de ansatte direkte hva de har behov for. Videre at dette nedfelles i konkrete kompetanseplaner på de ulike nivåene i kommunens organisasjon. Kommunen har ikke kompetanseplaner som dekker informasjonssikkerhet i dag.

Anbefalinger

Ut fra de vurderinger og konklusjoner som er gjort, anbefaler vi kommunen å:

1. Oppdatere e-strategi for Våler kommune

2. Vurdere hvordan det generelt kan sikres større fokus på mål og strategi for informasjonssikkerhet i hele kommunens organisasjon. Både gjennom informasjon og opplæring, involvering og rapportering.
3. Få på plass et internkontrollsystem for informasjonssikkerhet som også omfatter:
   - Systematiske risikovurderinger.
   - Oppfølging og kontroll av at målsettinger på området og internkontrolltiltakene etterleves, og statusrapporteringer i tilknytning til dette.
   - Systematisk forbedringsarbeid.
   - Årlige gjennomganger på området fra ledelsens side som dokumenteres.
4. Fullføre kartleggingen av risiko i kommunens IKT-systemer og at en i den forbindelse i større grad tydeliggjøre hva som er akseptabel/uakseptabel risiko. Videre at det utarbeides handlingsplaner som beskriver hvordan risikoen skal reduseres til et akseptabelt nivå.
5. Gjennomfører sikkerhetsgjennomganger, sikkerhetsovervåkning og testing av IKT-systemene mer planmessig, og at planleggingen baseres på vurdering av risiko.
6. Sikre at kommunens interne retningslinjer for beredskap innen informasjonssikkerhet etterleves, og at en vurderer hvordan informasjonssikkerhet kan inkluderes i beredskapsøvelser.
7. At kommunen planlegger, gjennomfører, følger opp og dokumenterer sikkerhetsrevisjoner for informasjonssikkerhet i helse- og omsorgstjenestene slik det er anbefalt.
8. Sikrer opplæring i, og informerer om rutinene knyttet til avviksrapportering.
9. Innføre faste rutiner for hvordan kommunens ansatte skal informeres om endringer i planer, reglementer og rutiner. Det bør også innføres rutiner for å oppfriske de ansattes kjennskap til disse dokumentene.
10. Innskjerpe etterlevelse av rutinene for oppdatering av planer, reglementer og rutiner i Compilo.
11. Satse mer på opplæring innen informasjonssikkerhet, og å tilpasse opplæringen slik at den er relevant til den enkelte sine arbeidsoppgaver. Det vil i denne forbindelse være hensiktsmessig å gjennomføre mer systematiske kartlegginger av opplæringsbehovet i kommunen.
12. Utarbeide planer for hvordan kommunen skal sikre kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen. Planene kan med fordel knyttes til kommunens øvrige kompetanseplanlegging og system for forbedringsarbeid.

2 Bakgrunn for prosjektet

I henhold til kommuneloven § 23-2, punkt c, skal kontrollutvalget påse at det blir gjennomført forvaltningsrevisjon i kommunen. Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak (§ 23-3 første ledd).

I møte 16. mars 2022, sak 19/22, bestilte kontrollutvalget i Våler kommune en forvaltningsrevisjon rettet mot IKT-sikkerhet. I møtebehandlingen kom det innspill fra kontrollutvalget om at ledere i kommunen kan være mer utsatt for hackerangrep enn andre fordi de ofte har en større kontaktflate i jobbsammenheng enn andre ansatte. Utvalget var også opptatt av risikoen ved økt bruk av hjemmekontor. I Våler kommune er det videre nødvendig med fokus på de driftsmessige sikkerhetstiltakene, ettersom kommunen drifter sine IKT-systemer selv. Det var enighet om at disse innspillene passet inn under de problemstillingene som var satt opp i prosjektplanen, og at de tas hensyn til i arbeidet med forvaltningsrevisjonen.

3 Aktualitet, formål og problemstillinger for forvaltningsrevisjonen

Bestillingen av en forvaltningsrevisjon rettet mot IKT-sikkerhet har bakgrunn i «Plan for forvaltningsrevisjon for Våler kommune for 2021-2024» og prosjektplan for IKT-sikkerhet utarbeidet av Revisjon Øst IKS i 2022.

IKT-sikkerhet er i plan for forvaltningsrevisjon omtalt som et komplisert område hvor det kreves mye ressurser og kompetanse for å holde tritt med utviklingen. IKT-sikkerhet er også et område som det har vært avdekket mangler på i andre kommuner. I prosjektplanen vises det til ytterligere forhold som medfører økt risiko for IKT-sikkerheten. Det legges til grunn at de siste årene med omfattende bruk av hjemmekontor kan ha gitt spesielle utfordringer. Det antas videre at urolige tider i Europa øker risikoen for angrep på kommunens IKT-systemer. Av PST sin nasjonale trusselvurdering for 2022 fremgikk at en hadde hatt en markant økning i antall nettverksoperasjoner siste året. Disse operasjonene var rettet både mot både offentlige og privates virksomheter. En del av operasjonene er utført av trusselaktører som opererer på vegne av fremmede stater. Noe av hensikten kan være å så mistillit til offentlige myndigheter, informasjonen de gir, tjenestene de skal forvalte og sikkerheten/tryggheten de skal kunne garantere.

Som eksempel på risiko og vesentlighet på IKT-området ble det vist til tre eksempler der det gikk veldig galt, eller der det kunne gått mye verre. Disse eksemplene var e-post-angrep på HIKT i september 2022, datainnbrudd på Stortinget høsten 2020 og mars 2021 og hacking av Østre Toten kommune i 2021. Av disse eksemplene ser en at brukerne og brukervennlighet utgjør en vesentlig risiko med hensyn til IKT-sikkerhet. Holdninger og fokus i blant kommunens ledelse og ansatte kan utgjøre en avgjørende forskjell med hensyn til IKT-sikkerheten i kommunene.

Informasjons- og kommunikasjonsteknologi (IKT) er en samlebetegnelse for teknologi for innhenting, overføring, bearbeiding, lagring og presentasjon av informasjon. I prosjektplanen er det lagt til grunn at en forvaltningsrevisjon rettet mot IKT-sikkerhet kan være rettet mot sikring av selve informasjons- og kommunikasjonsteknologien. Hovedfokuset bør likevel rettes mot hvordan informasjonen i IKT-systemene sikres, og at det i den forstand er mer relevant å snakke om *informasjonssikkerhet*.

Formålet med forvaltningsrevisjonen har vært å se etter om Våler kommune tilfredsstiller sentrale lovkrav og anbefalinger for informasjonssikkerhet. Formålet belyses ved å besvare følgende problemstillinger:

1. Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte?
2. Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?
3. I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

4 Revisjonskriterier

På bakgrunn av problemstillingene i forvaltningsrevisjonen skal det etableres revisjonskriterier. Disse danner grunnlaget for hva innsamlede data skal vurderes opp mot. Kriteriene skal begrunnes i/utledes av autoritative kilder innenfor det reviderte området. Autoritative kilder kan være lover, forskrifter, forarbeider, rettspraksis, politiske vedtak/mål/føringer, administrative retningslinjer/mål/føringer, statlige føringer/veiledere, andre myndigheters praksis, teori og reelle hensyn som vurderinger av hva som er rimelig/formålstjenlig/effektivt. I dette prosjektet er revisjonskriteriene utledet fra følgende kilder:

- Kommuneloven
- eForvaltningsforskriften
- Digitaliseringsdirektoratet sine hjemmesider
- Datatilsynet sine hjemmesider
- Veiledere og anbefalinger fra KS, direktoratet for e-helse og Nasjonal sikkerhetsmyndighet

Fullstendig utledning av revisjonskriterier finnes i vedlegg A til rapporten.

5 Metode for revisjonen

Informasjon som belyser problemstillingene er innhentet gjennom dokumentstudier, intervjuer og spørreundersøkelse.

5.1 Dokumentstudier

Undersøkelsen har blant annet omfattet gjennomgang og vurdering av relevant dokumentasjon opp mot fastsatte revisjonskriterier, som i denne sammenheng er:

- Plan og strategidokumenter knyttet til informasjonssikkerhet
- Beskrivelse av styringssystemet
- Interne veiledere, retningslinjer og rutinebeskrivelser/prosedyrer
- Maler og skjema til bruk i forbindelse med personvern og informasjonssikkerhet
- Ulike oversikter over for eksempel IKT-systemer, behandlingsprotokoller o.l.
- Årshjul
- Rapportering på området

Vi har ellers hatt tilgang til kvalitetssystemet Compilo slik at vi selv har kunnet se hvordan dette systemet er bygget opp og skaffet oss en oversikt over hva slags dokument som finnes i dette systemet. Dokumenter som er grunnlag for våre vurderinger er omtalt i de relevante datakapitlene.

5.2 Intervjuer

Det ble innledningsvis gjennomført et oppstartsmøte (10.01.2023) der IKT-leder deltok fra kommunen. Formålet med møtet var, i tillegg til å informere kommuneadministrasjonen om forvaltningsrevisjonen, å innhente mer overordnet informasjon og sentrale dokumenter tilknyttet informasjonssikkerhet. Det er videre i perioden april til mai 2023, gjennomført kvalitative intervjuer med ledere og nøkkelpersonell i kommunen. Disse er:

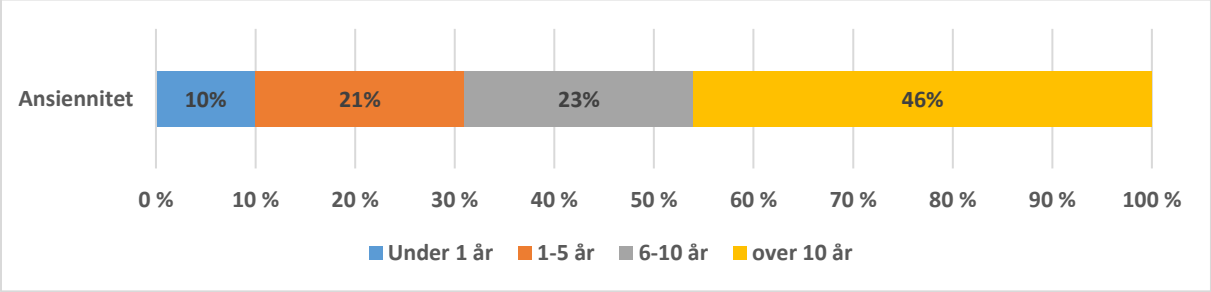
- Pleie- og omsorgssjef
- Leder tekniske tjenester
- Personvernombud
- IKT-leder
- Superbruker Visma profil
- Superbruker KOMTEK
- Kommunedirektør

Intervjuene er gjennomført enkeltvis på TEAMS og det er utarbeidet temalister som ble sendt de ulike respondentene før intervjuet. Det er også utarbeidet intervjuguider som er benyttet under selve intervjuene.

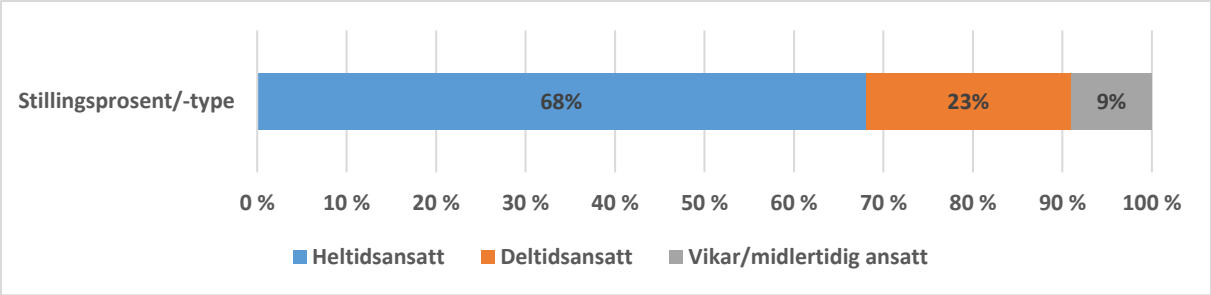
5.3 Spørreundersøkelse

I forbindelse med forvaltningsrevisjonen om informasjonssikkerhet i Våler kommune ble det i perioden 15. mai til 16. juni 2023 gjennomført en spørreundersøkelse rettet mot alle ansatte i kommunen. Det er foretatt fire løpende purringer i løpet av gjennomføringsperioden til de som ikke hadde besvart undersøkelsen.

Vi har fått e-postadresser til de ansatte fra kommunen og undersøkelsen ble sendt ut til 557 personer. Av årsrapporten til kommunen for 2023 fremgår det at kommunen hadde 362 faste ansatte ved utgangen av 2022. Dette betyr at 195 av de som har fått tilsendt undersøkelsen er tilknyttet kommunen i egenskap av vikariater eller engasjementer i ulike deler av kommunen. Det er til sammen 117 ansatte som har besvart undersøkelsen. Dette gir en svarprosent på 21 %. Vi har fått svar fra ansatte i alle kommunens virksomheter, selv om representasjonen her er noe variabel. Vi har fått svar både fra ansatte som har et kort arbeidsforhold i Våler kommune og ansatte som har arbeidet over 10 år i samme virksomhet. Ansatte som har besvart undersøkelsen har oppgitt følgende ansiennitet i virksomhetene de jobbet i på undersøkelsestidspunktet:



De som har besvart har oppgitt følgende stillingsprosent/-type for nåværende arbeidsforhold:



Undersøkelsen består av fem hovedtemaer med tilhørende spørsmål. Disse er:

1. Holdninger til digitalisering og digital sikkerhet
2. Synet på styring og kontroll
3. Risiko-oppfattelse
4. Sikkerhetsatferd, og
5. Kunnskap, læring og interesse

Vi har fordelt resultatene og analysen av svarene knyttet til de fem hovedtemaene i de ulike problemstillingene i rapporten. Noen av resultatene er likevel relevante for flere av problemstillingene i forvaltningsrevisjonen.

Ikke alle som har besvart spørreundersøkelsen har svart på alle spørsmålene. Dette har betydning for validiteten knyttet til det enkelte spørsmål. I presentasjonen under den enkelte problemstilling kommenteres dette for de spørsmålene der det er vesentlig forskjell på deltakere i undersøkelsen og antall svar på spørsmålet.

6 Problemstilling 1 – Planverk, retningslinjer og rutiner

Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte?

6.1 Revisjonskriterier for problemstilling 1

Følgende er en tabell med de kriterier vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A. Tabellen er interaktiv og leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriteriet. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor. Vi gjør derfor leseren oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

	Kriterium 1	Kommunen må ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi)
	Kriterium 2	Kommunen og kommunens øverste ledelse må ha en tilpasset og risikobasert internkontroll for informasjonssikkerhet. Internkontrollen inneholder både et strategisk og langsiktig perspektiv, og et operasjonelt perspektiv som omhandler daglig virksomhetsstyring.
	Kriterium 3	Kommunen må ha fastsatt hva som kan aksepteres av risiko og gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi. Der risikoen er over fastsatt grense for hva som er akseptabelt bør det utarbeides tydelige tiltaksplaner som viser hvem som er ansvarlig for ulike tiltak.
	Kriterium 4	Kommunen må ha rutiner og prosedyrer som sørger for at informasjon ikke blir kjent for uvedkommende.
	Kriterium 5	Kommunen må ha rutiner og prosedyrer som sørger for at informasjon ikke blir endret utilsiktet, eller av uvedkommende.
	Kriterium 6	Kommunen må ha rutiner og prosedyrer som sørger for at informasjon er tilgjengelig ut ifra tjenstlige behov.
	Kriterium 7	Kommunens ledelse må ha rutiner for å gjennomgå kommunens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året.
	Kriterium 8	Ledelsens årlige gjennomgang innen informasjonssikkerhet og personvern i helse- og omsorgstjenestene må dokumenteres, og dersom gjennomgangen har avdekket at virksomhetens risikonivå ikke er i henhold til akseptabelt risikonivå må det være vedtatt tiltaksplaner for å rette opp avviket.

6.2 Innhentet data

6.2.1 Data fra dokumenter

Våler kommune har en egen **«E-strategi for Våler kommune 2018-2021»**. E-strategien skal støtte opp under arbeidet med å nå de langsiktige og strategiske målene i kommuneplanens handlingsdel og økonomiplan. E-strategiens viktigste fokusområde er å utvikle Våler kommune som e-kommune, og bygger på følgende pilarer:

- Stabil drift
- Tjenesteutvikling og innovasjon
- Tilgjengelighet og mobilitet

Strategidokumentet har et eget kapittel som omhandler *Utvikling av infrastruktur*. Det legges her vekt på at en ved nyinnkjøp må ta hensyn til mulighetene og behovet for større mobilitet. Det skal fortrinnsvis anskaffes bærbare PC er som også kan brukes på hjemmekontor. Det tas videre sikte på å utvikle servermiljøet til å bli mer elastisk og behovsdrevet gjennom lokale skytjenester. Når det gjelder kommunikasjonsløsninger ellers er strategien å sikre bedre samordning mellom de ulike kanalene gjennom felles grensesnitt, og det legges opp til en standardisering av mobiltelefoner.

E-strategien omtaler videre *Forholdet til standarder og bruk av felleskomponenter*. Det er presisert at Våler kommunes strategi skal være konsistent med referansekatalogen for IT-standarder i offentlig sektor. Vi får ellers opplyst at Felleskomponenter som brukes av Våler kommune er DIFI[1] sine kvalitetskriterier, LOS [2] og ID-porten

Det finnes et eget kapittel som omhandler *Fagsystemer og fellessystemer.* Kommunens strategi på dette området er blant annet å legge til rette for bruk av digitale verktøy i forbindelse med innbyggertjenester. Det heter videre at ansattportalen (intranett) er den viktigste interne samhandlingsflaten i kommunen. Det er i denne forbindelse opplyst at portalen er rolle- og oppgavestyrt og skal prioriteres ved utvikling av interne tjenester. Ellers er helse, omsorg og velferd og utdanningsområdet prioriterte områder med hensyn til økt bruk av informasjonsteknologi.

Forvaltning og kompetanse er omtalt i egent kapittel, og det heter her at det er planer om å opprette en ordning med beredskapsvakt. Dette for å sikre høy oppetid og å understøtte organisasjonens behov for støtte utenom ordinær arbeidstid. Det fastslås at helhetlig styring og optimal ressursutnyttelse vektlegges med hensyn til IKT-drift. Behovet for kompetanseutvikling når det gjelder IKT skal innlemmes i kommunens kompetanseplaner. Ellers skal kompetansen økes ved bruk av e-læring. Opp mot kommunens ledere er planen å fokusere på strategisk IKT-ledelse og gevinstrealisering som følge av IKT-prosjekter. Det er ellers en målsetting at alle felles- og fagsystemer skal ha definerte systemeiere, systemansvarlige og vedlikeholdsansvarlige.

Strategidokumentet omtaler også regler for hvordan kommunen skal forholde seg med hensyn til innkjøp. Ved investering i nye systemer og/eller programvare må behovet og de tekniske løsningene drøftes med IKT-avdelingen. Det stilles enkelte krav til nye systemer/programvare, blant annet til integrasjon med andre IKT-systemer i kommunen og øvrig infrastruktur.

[1] Direktoratet for forvaltning og IKT (DIFI) ble fra 2020 en del av Digitaliseringsdirektoratet (Digdir)
[2] LOS er et felles vokabular som er temainndelt for å kategorisere og beskrive offentlige tjenester og ressurser (https://www.digdir.no/informasjonsforvaltning/los-felles-vokabular-klassifisering-av-offentlige-tjenester-og-ressurser/2434)

Det er lagt opp til at det utarbeides handlingsplaner som viser prioriterte tiltak for å nå kommunens strategi. For det enkelte prosjekt skal det dokumenteres gevinster i form av økonomiske besparelser, økt kvalitet eller andre relevante gevinster. Prosjektene skal videre legges inn i kommunens budsjetter.

Sikkerhetsmål og sikkerhetsstrategi for Våler kommune er i tillegg til e-strategien, kommunens overordnede og styrende dokument for informasjonssikkerhet. Det presiseres innledningsvis at det er kommunens ledelse som har ansvaret for all informasjonssikkerhet i kommunen. Det heter ellers at det er sikkerhetsleder som har ansvaret for å utarbeide mål og strategi for informasjonssikkerhet, utarbeidelse av rutiner samt kontroll med at rutinene følges. Følgende sikkerhetsmål er definert:

- Våler kommune skal sikre at informasjon behandles iht. krav i relevante lover og forskrifter.
- Sikkerheten i Våler kommune skal ha forankring i ledelsen ved Våler kommune.
- Sikkerheten skal ivaretas som en integrert del av hele Våler kommunes organisasjon.
- Den fysiske sikkerhet i Våler kommune skal hindre at uautoriserte får adgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles.
- Tilgang til systemer og informasjon gis kun til medarbeidere etter behov (need to know).
- Tilgang til systemer og informasjon for uvedkommende skal forhindres.
- Våler kommune skal sikre at informasjonsbehandling er korrekt og at informasjon ikke forandres uten lovlig tilgang.
- Våler kommune skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid for de personer som er autorisert.
- Det skal være mulig å spore uønskede hendelser.
- Det skal være tatt i bruk rutiner for å håndtere uønskede inkludert virksomhetskritiske hendelser.
- Det skal være tatt i bruk systematiske læreprosesser ved uønskede hendelser slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres.
- Forhindre at personer eller systemer hos Våler kommune bevisst eller ubevisst er årsak til sikkerhetsmessige uønskede hendelser mot egen eller andre virksomheter eller privatpersoner.
- Våler kommune skal sikre at medarbeidere som bruker Våler kommunes informasjonssystemer har en tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov/krav.

Strategidelen av dokumentet innledes med en oversikt over hvordan sikkerhetsarbeidet er tenkt organisert. Det er kommunens sikkerhetsleder som skal ha det overordnede utøvende ansvaret, men deler blir også delegert til personer i ulike avdelinger. Organiseringen skal fremgå av egen beskrivelse. Det nevnes ellers at kontrakter mellom Våler kommune og leverandører skal inkludere relevante sikkerhetskrav. Kommunen skal ha innsyn og kunne gjøre målinger av hvorvidt sikkerhetskravene etterleves. Egenkontroll skal gjennomføres regelmessig.

I kapitlet som omhandler personell og sikkerhet står det at alle skal underskrive en taushetserklæring og ansattretningslinjer for informasjonssikkerhet og personvern. De ansatte skal få tilstrekkelig

veiledning, opplæring og rutiner til å forvalte informasjon og systemer på en sikker måte. Fysisk sikring skal skje gjennom soneinndeling og adgangskontroll og forsøk på uautorisert adgang skal sikres med alarmsystemer. Det heter at tilgang til informasjonssystemer styres av linjeleder som skal kartlegge og autorisere ansattes behov, mens det er IKT-avdelingen som i praksis skal vedlikeholde tilgangsrettighetene og holde oversikt over gitte rettigheter.

Dokumenter og lagringsmedia med beskyttelsesverdig informasjon skal oppbevares, forsendes og destrueres slik at de ikke kommer uvedkommende i hende. Når det gjelder konfigurasjon skal IKT-avdelingen utarbeide og holde oversikt over utstyr, programvare og systemkonfigurasjon. Sikkerhetsleder har ansvaret for å utarbeide og vedlikeholde oversikt over sikkerhetsdokumentasjon.

Når det gjelder systemteknisk sikkerhet legger Våler kommune følgende verdier til grunn:

- Høy - gis bare systemer og informasjon med virksomhetskritisk beskyttelsesbehov.
- Middels - gis systemer og informasjon med beskyttelsesbehov.
- Lav - (lave krav til sikkerhet) kan gjelde alle systemer og informasjon med lite eller ingen beskyttelsesbehov.

Det stilles krav til dokumentasjon av beskyttelsesbehov. Både når det gjelder oversikt over de digitale verdiene i systemene og kriterier som legges til grunn i vurderingen.

Ansattretningslinjer for informasjonssikkerhet og personvern gir oversikt over hva den enkelte ansatte skal være kjent med når det gjelder informasjonssikkerhet og personvern. Dette er:

- Roller og ansvarsfordeling
- Sikkerhetsmål og strategier
- Sikkerhetstiltak en selv er pålagt å følge
- Kommunens rutiner for avvikshåndtering innen personvern og informasjonssikkerhet.

Med hensyn til roller og ansvarsfordeling fremkommer det at det er kommunedirektøren som er behandlingsansvarlig i kommunen. Virksomhetslederne har det daglige ansvaret inne det enkelte fagområde, mens det er IKT-sjefen som er ansvarlig for teknisk drift av hele dataanlegget. Sikkerhetsleder har som oppgave å koordinere sikkerhetsarbeidet. Det er videre presisert at man som ansatt må vite hvem som er systemansvarlig for de fagsystemene en benytter. Rollen som systemansvarlig innebærer vedlikehold og ajourhold av tilganger, og det er systemansvarlig man skal henvende seg til ved behov for mer opplæring i fagsystemet. Retningslinjene gir også en oversikt over ansvarsområdet/oppgavene til personvernombudet.

Det slås fast at alle medarbeidere skal være kjent med kommunens sikkerhetsmål og strategier. For sikkerhetstiltak som de ansatte er pålagt å kjenne til og etterleve i det daglige, er det henvist til kvalitetssystemet Compilo. Det heter at alle medarbeidere både har rett og plikt til å gjennomgå nødvendig opplæring før tilgang til de ulike datasystemene blir gitt.

Ansattretningslinjene inneholder videre regler for taushetsplikt. Det heter at alle har taushetsplikt i tjenestesaker, og skal alltid undertegne taushetspliktskjema ved ansettelsen. Denne plikten omfatter å hindre at informasjon som kan spores tilbake til en person, gjøres kjent for uvedkommende. Slik informasjon kan være opplysninger om brukere/klienter, ansatte, kommunens virksomhet, sikkerhetsmessige og organisatoriske forhold, både i muntlig, skriftlig og elektronisk format. Taushetsplikten gjelder ikke bare utad, men også overfor andre medarbeidere og kollegaer der

opplysningene må anses unødvendige. Taushetsplikten gjelder også etter at arbeidsforholdet er avsluttet.

Retningslinjene angir også regler for låserutiner og adgangskontroll, samt orden og ryddighet på kontoret. Det er den enkelte ansatte som har ansvaret for at personopplysninger på egen arbeidsplass er forsvarlig sikret. Det finnes videre egne regler for bruk av internett. Det er bare lov å koble seg til internett gjennom kommunens sikkerhetsløsning, og det er ikke tillatt å laste ned og installere programfiler. Medarbeidere har kun lov til å installere programvare på egen arbeidsstasjon etter autorisasjon av dataansvarlig. Dersom man trenger ekstra programvare må det tas kontakt med IKT-avdelingen. Retningslinjene inneholder også regler om endringer av rolle eller avslutning av arbeidsforholdet, og tilbakelevering av materiell til kommunen.

Når det gjelder regler for bruk av e-post heter det at private dokumenter må lagres i egne mapper som er merket privat. Det er kun lov å bruke arbeidstakers e-post til små og tidsbegrensede private gjøremål. Ansattretningslinjene angir videre regler for innsyn i arbeidstakers e-post eller i informasjon lagret lokalt på den enkeltes PC eller hjemmeområde. Det er presisert at sensitive personopplysninger ikke skal sendes med vanlig e-post. E-post som er lagrings- eller arkivverdige skal lagres i samsvar med kommunens regler for arkivering og journalføring. Det advares også mot å åpne ukjente vedlegg i e-poster.

Retningslinjene gir regler for bruk av passord. Det er ikke tillatt å dele passord, og passordet skal ikke skrives ned noen plass. Medarbeidere som er autorisert for tilgang til sensitive personopplysninger på sikret sone, er pålagt følgende begrensinger og kontroller:

- sperring slik at en ikke har samtidig tilgang til tjenester og informasjon utenfor sikret sone
- individuelle passord skal sørge for at brukere kun autoriseres for tilgang til informasjon og tjenester etter tjenstlige behov
- brukerkonti som ikke har vært benyttet de siste 6 uker blir sperret
- manglende skifte av passord innen fastsatt frist, fører til sperring av brukerkonto
- sikkerhetsrelevante hendelser logges og registreres i et hendelsesregister

Den enkelte ansatte må ellers, i møte med brukere/klienter og pasienter, kjenne til og kunne formidle informasjon om den registrertes rettigheter mht. samtykke, innsyn og retting/sletting av opplysninger. Retningslinjene informerer også om kommunens rutiner for avvikshåndtering og egenkontroll av sikkerhetsarbeid. Ved avvik skal man benytte avviksmodulen i Compilo. Egenkontroll går på hvordan sikkerhetstiltakene og internkontrollen er kjent, og som ansatt må en påregne å delta i spørreundersøkelser som kartlegger status.

Avslutningsvis gir retningslinjene informasjon om hvilke sanksjoner som brudd på retningslinjene kan føre til og at ansattretningslinjene er et kontraktsdokument mellom arbeidstaker og kommunen som arbeidsgiver. Dokumentet signeres i forbindelse med ansettelse og signering av taushetserklæringen. Ved å signere på dokumentet bekrefter den ansatte at ansattretningslinjene er lest og forstått og at den enkelte forplikter seg til å følge retningslinjene.

Vi har fått tilgang til notatet **«Styringssystem for informasjonssikkerhet og personvern»**. Dokumentet var på det tidspunktet vi avsluttet datainnsamling til denne forvaltningsrevisjonen oversendt kommuneledelsen for godkjenning. Innledningsvis i dokumentet defineres hva et styringssystem er,

formålet med styringssystemet, hvilke lovverk styringssystemet skal ivareta, samt definisjon på sentrale begreper. Styringssystemet er ellers inndelt i en styrende del, en gjennomførende del og en kontrollerende del. Det heter at arbeid med informasjonssikkerhet og personvern skal baseres på risikovurderinger.

For den styrende delen er «Ansattretningslinjer for informasjonssikkerhet og personvern», samt «Sikkerhetsmål og sikkerhetsstrategi – IKT» utgangspunktet. I tillegg kommer mer spesifikke retningslinjer og rutiner, avhengig av rolle og arbeidssted. I denne delen oppsummeres kommunens sikkerhetspolicy og policy for personvern og fordeling av myndighet, roller og ansvar.

For den gjennomførende delen gis det regler for innholdet i en årsplan for arbeid med informasjonssikkerhet og ledelsens årlige gjennomgang. Det fastsettes videre en inndeling når det gjelder kartlegging og klassifisering av informasjon. Det legges opp til å klassifisere informasjon som behandles i IKT-systemer som:

- åpen,
- intern/beskyttet,
- fortrolig og
- strengt fortrolig.

Behovet for sikring og hva som er akseptabel risiko er forskjellig for de ulike kategoriene.

Den kontrollerende delen inneholder bestemmelser om gjennomgang av IKT-sikkerhet og personvern, avvikshåndtering, egenrapportering og sikkerhetsrevisjon. Gjennomganger kan igangsettes av både kommunedirektør, kontrollutvalg, den som utøver databehandleransvar, personvernombudet, IT-sikkerhetsansvarlig og systemeier. Det er gitt eksempler på hva slike gjennomganger kan omfatte. De kan ellers igangsettes med bakgrunn i sikkerhetsavvik, utfordringer avdekket i årlig egenrapportering eller tekniske observasjoner. For registrering av avvik skal avviksmodulen i Compilo benyttes. Det er den enkelte medarbeider som er ansvarlig for å rapportere avvik, mens virksomhetens ledelse er ansvarlig for å behandle avvikene og iverksette tiltak. Det er avslutningsvis i notatet satt opp ett årshjul som viser tidspunkt for ulike aktiviteter, samt hvem som er ansvarlig for gjennomføringen.

I **personvernombudets årsrapport for 2022** etterlyses det større fokus på risikovurderinger i organisasjonen, og det etterlyses også flere ressurspersoner til å gjennomføre DPIA.

Kvalitetssystemet Compilo består av et dokumentbibliotek, en modul for melding av avvik, en modul for uttak av avviksstatistikk og en modul for administrasjon av egne oppdrag. Dokumentbiblioteket har innholdsfaner for det som defineres som ledelsesprosesser. Herunder kvalitetshåndbok (mål og system), lover/forskrifter og reglementer, overordnede planer, HMS og andre IK-systemer, beredskap og sikkerhet samt politisk styring. Ved vår gjennomgang var det ikke lagt inn noen dokumenter under fanen kvalitetshåndbok. Flest dokumenter ligger det under fanen for lover/forskrifter/reglementer. Dokumentbiblioteket har ellers egne områder for de ulike virksomhetsområdene i kommunen. Blant annet IKT. For IKT finnes det et:

- Eget område med dokumenter for sikkerhetsmål og sikkerhetsstrategi
- Eget område med maler og rutiner for behandling av helse- og personopplysninger
- Eget område med maler og rutiner for etablering og drift av informasjonssystemer
- Eget område med maler og rutiner for tilgangsstyring
- Eget område med maler og rutiner for avvikshåndtering

- Eget område med maler og rutiner for sikring av område og utstyr
- Eget område med maler og rutiner for telefoni
- Eget område med maler og rutiner for opplæring

Det kan her kommenteres at området med dokumenter for sikkerhetsmål og sikkerhetsstrategi inneholder retningslinjer for utarbeidelse av katastrofeberedskap. Området med maler og rutiner for etablering og drift av informasjonssystemer inneholder egne rutiner for planlegging av utilsiktet avbrudd – IKT. Både i retningslinjene for katastrofeberedskap og rutinen for planlegging av utilsiktet avbrudd er det fokus på å sikre nødvendig tilgang til IKT-systemene når uforutsette hendelser inntreffer. Under område med maler og rutiner for opplæring finnes en egen prosedyre for «Personellopplæring innen IKT». Prosedyren fokuserer blant annet på den enkelte ansatte sine plikter i forbindelse med forsvarlig sikring av personopplysninger og informasjon.

I dokumentbiblioteket finnes også innholdsfaner for det som defineres som støtteprosesser. Herunder egne faner for felles skjemaer, kjøreregler for bruk av Compilo og GDPR-personvern. Under fanen GDPR – personvern finner vi blant annet:

- Avviksmelding til datatilsynet - mal
- Egenkontroll av informasjonssikkerhet – skjema
- Oversikt over behandlingsprotokoller – GDPR
- Rutiner ved brudd på personopplysningssikkerheten
- Rutiner for gjennomføring av risikovurderinger ved behandling av personopplysninger
- Kontroll med tilgang til særlige kategorier av personopplysninger (sensitive)
- Sjekkliste: Sjekk av innhold i databehandleravtaler
- Rutine for vurdering av personvernkonsekvenser – DPIA (Data Protection Impact Assessment)

6.2.2 Data fra intervjuer

6.2.2.1 Data fra intervju med kommunedirektør, IKT-leder og personvernombud

I intervju med **kommunedirektøren** har vi fått opplyst at kommunens E-strategi har vært lagt til grunn for IKT-satsningen de siste årene, og at det jobbes med å dokumentere styringssystemet for IKT-sikkerhet. Forberedelsene for overgang til Indigo IKT IKS var viktig for kommunen da intervjuet ble gjort, og både styring og infrastruktur på området skulle gjennomgås.

Når det gjelder internkontroll i kommunen så poengterer kommunedirektøren at det er mange områder som skal dekkes. Kvalitetssystemet Compilo er sentralt i og med at alt regelverk, retningslinjer og rutiner er lagt inn i dette systemet. Dersom det er brudd på reglene og rutinene som finnes i Compilo skal dette rapporteres som avvik i eget avvikssystem, som også ligger i Compilo. Kommunen har ellers fått vedtatt nytt delegeringsreglement for en tid tilbake, noe som har gjort at en får tydeliggjort ansvar og oppgaver i organisasjonen. Internkontrollen for informasjonssikkerhet organiseres på samme måte som på andre områder i kommunen, og regler og rutiner ligger i Compilo. Når det gjelder avviksregistrering for IKT og informasjonssikkerhet er det imidlertid sjelden at avvikssystemet i Compilo benyttes. Kommunedirektøren mener at dette sannsynligvis skyldes at slike saker ofte haster og at det er raskere å ta direkte kontakt med nærmeste leder eller IKT-avdelingen.

Da intervjuet ble gjennomført hadde det vært jobbet aktivt med styringsstrategi i kommunen en tid, og det var i denne forbindelse utarbeidet 11 punkter for styringsstrategi som var gjennomgått i virksomhetsledermøter. For punkt 5 i styringsstrategien, som handler om ansvar, er styring og struktur viktige stikkord. Dette gjelder også i forbindelse med internkontroll og det jobbes med å få til en mer

lik/enhetlig struktur for alle kommunens virksomheter. Det er den enkelte virksomhet som har ansvaret for rutiner for bruk av systemene i forhold til personvern etc. IKT-avdelingen har ansvaret for IKT-sikkerheten i alle systemene. IKT-avdelingen har et eget område for rutiner og andre dokumenter i Compilo.

Fra kommunedirektøren har vi fått opplyst at det jevnlig gjøres risikovurderinger i de fleste av kommunens virksomheter. Helse- og omsorgstjenestene blir trukket frem av kommunedirektøren som spesielt gode på dette, ettersom de har forholdt seg til «forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenestene» over mange år. Risikovurderingen gjennomføres både med hensyn til sikkerhet og kvalitet på tjenestene.

Når det gjelder personvern er personvernombudet en viktig ressurs, blant annet med hensyn til risikovurderinger. De ulike virksomhetene er godt kjent med at kommunen har et personvernombud og søker råd og veiledning dersom det er noe de lurer på. Det er kommunedirektøren sin oppfatning at hele organisasjonen har blitt mer oppmerksom på personvern etter at personvernombudet kom på plass.

Kommunen har ingen spesiell rapportering med hensyn til internkontroll eller informasjonssikkerhet, men dette kan gjerne være tema på virksomhetsledermøter og andre ledermøter. Det har blant annet kommet tilbakemeldinger på økt opplæringsbehov for enkelte av kommunens IKT-systemer.

Fra **IKT-leder** har vi fått opplyst at IKT-avdelingen har 2 ansatte og at den i stor grad er en utviklingsavdeling. Da intervjuene ble gjennomført fantes det superbrukere på noen av fagsystemene og programvareområdene. Ellers er det lederne i de enheter hvor systemene benyttes som var systemansvarlig (systemeiere). Ettersom Våler kommune er en relativt liten organisasjon, vil avdelingen være tettere involvert i en større del av den aktiviteten som skjer enn mange andre IKT-avdelinger. IKT-avdelingen kan for eksempel stille med prosjektledere når det tas i bruk nye IKT-systemer eller når det skal gjøres større endringer i systemene. Avdelingens oppgave er først og fremst å utvikle og effektivisere kommunen.

I forbindelse med styring og internkontroll følger kommunen de anbefalinger og veiledere som er kommet fra for eksempel KS og Nasjonal sikkerhetsmyndighet. Det er imidlertid ikke vedtatt å følge noen bestemt standard for styring av IKT sikkerhetsarbeidet. Våler kommune er medlem av Kommune-CSIRT. [3] Medlemskapet gir tilgang til ulike maler og verktøy, etterretningsinformasjon etc. som støtte til kommunens arbeid med IKT sikkerhet. Kommunen har også hatt dialog med Kommune-CSIRT vedrørende styringssystemet for IKT i kommunen og forholder seg til deres anbefalinger. De fleste IKT-systemene er etterhvert lagt ut i sky, og det har vært et målrettet arbeid med å få til dette de senere årene.

Da intervjuet ble gjennomført var kommunen i ferd med å utarbeide en oversikt og dokumentere styringssystemet for informasjonssikkerhet i kommunen. Selv om mye av dokumentasjonen vedrørende internkontroll er lagt inn i Compilo, mener IKT-leder at kommunen har noe igjen for å få til en god og oversiktlig struktur. Kommunen har til hensikt å tilpasse internkontrollen for informasjonssikkerhet bedre til kommunens øvrige internkontrollsystem. Dette vil en kunne oppnå når styringsdokumentet for informasjonssikkerhet legges til grunn og hvor dette da kan lenkes til

[3] CSIRT står for Computer Security Incident Response Team. Kommune-CSIRT er et interkommunalt selskap eid av Gjøvik og Lillehammer kommuner. Kilde: https://kommunecsirt.no/om-oss

Compilo. IKT-leder opplyser ellers å ha jobbet en god del med DPIA-er [4] og behandlingsprotokoller for de IKT-systemene hvor dette er påkrevd, sammen med personvernombudet. Oversikt/dokumentasjon på dette finnes i Compilo. Kommunen har foreløpig ingen dokumentert klassifisering av verdien på informasjonen i IKT-systemene, men prioriterer liv og helse først.

Når det gjelder rutiner for å sikre informasjonen i IKT-systemene finnes det noen felles rutiner ved skolene. IKT-leder mener likevel det er for få som kan IKT-systemene godt, også blant de som er systemansvarlige. Systemene brukes ofte for lite og ved nedbemanninger forsvinner kompetanse, eller at det blir for lite tid for de systemansvarlige til å utvikle og vedlikeholde rutiner for informasjonssikkerhet.

Rutinene for tilgangsstyring har alltid vært strenge, selv om det har vært mer fokus på dette de senere årene. En ansatt skal i utgangspunktet ikke ha flere tilganger enn hva denne må ha for å gjennomføre jobben sin. For noen systemer er det likevel umulig eller upraktisk å avgrense fullt ut. I for eksempel helse- og omsorgssystemene kan en bare avgrense i noen grad. Det finnes blant annet en «blålysfunksjon» for sykepleierne som sikrer at de kan bistå brukere de ikke har ansvaret for i det daglige.

I de fleste av IKT-systemene finnes det systemer for loggføring av hvem som er inne i hvilke deler av systemer, og hva de gjør av registreringer/endringer. Det foretas imidlertid ingen gjennomgang av loggene med mindre det har hendt noe spesielt.

Vi har ellers fått opplyst at gjennomgang og evaluering av aktivitetene for å sikre informasjon foregår fortløpende. En tar hensyn til eventuelle avvik eller risiko som oppstår og finner løsninger.

Fra **personvernombudet** har vi fått opplyst at ombudet ikke har vært involvert i utarbeidelse av gjeldende mål og strategi for informasjonssikkerheten i kommunen, men har kommet med forslag til nytt innhold som er bedre tilpasset GDPR. [5] Personvernombudet har også oppgitt å ha vært pådriver for å få innført risikovurderinger i forbindelse med innføring av nye IKT-systemer. Det er i denne forbindelse utarbeidet en ROS-modell i Excel-format som kommunen kan benytte, og hvor en kan vurdere ulike scenarioer ut fra sannsynlighet og konsekvens. Utskifting av nøkkelpersoner og ledelse i kommunen har vært en utfordring med hensyn til å få fart i arbeidet med interne rutiner for personvern og å få disse på plass. Personvernombudet har vært i ledergruppa i kommunen, blant annet for å presentere regler for databehandleravtaler og en sjekkliste i denne forbindelse. Det er imidlertid ikke noe fast opplegg med hensyn til å møte i ledergruppa. Personvernombudet har ellers bistått kommunen i forbindelse med utarbeidelse av behandlingsprotokoller. [6]

Vi har fått opplyst at det gjennomføres årlige undersøkelser i ledergruppa vedrørende sikring av personopplysninger. Denne består av en kort e-innledning med noe informasjon og spørsmål til slutt som må besvares. Personvernombudet videresender resultatene til kommunedirektøren. Resultatene

[4] DPIA står for Data Protection Impact Assessment og er en særskilt vurdering av personvernkonsekvenser når systemer og prosesser innebærer behandling av personopplysninger som kan ha innvirkning på personvernet til den som eier opplysningene.

[5] GDPR står for General Data Protection Regulation (personvernforordningen på norsk). GDPR er en EU-forordning som er gjeldende for EØS-statene, og er tatt inn i norsk lov ved ikrafttredelse av personopplysningsloven den 20.7.2018.

[6] En behandlingsprotokoll er en protokoll over alle behandlingsaktivitetene behandlende virksomhet er ansvarlig for ved behandling av personopplysninger. Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/

er også en del av grunnlaget når personvernombudet utarbeider sin årlige rapport om aktivitet og status for året som har gått.

Personvernombudet er opptatt av at det finnes gode rutiner når det gjelder personvern. Regler for dette er tatt inn i personalhåndbøker, der dette finnes, og det er opprettet egen GDPR-mappe i Compilo. Det finnes også skriftlige rutiner rundt om i enhetene som skal sikre at reglene rundt personvern overholdes.

I forbindelse med nytilsettinger er det også utarbeidet en egen ansattretningslinje for hva den ansatte skal ha oversikt over når det gjelder informasjonssikkerhet og personvern, og det må signeres for at regler og rutiner er lest og forstått. Det planlegges å innføre tilsvarende prosedyre for de ansatte ved endringer i regler og rutiner.

Når det gjelder tilganger er det personvernombudet sitt inntrykk at det er blitt en større bevissthet de senere år på hva som er tjenstlig behov for opplysninger. I helsetjenestene har det vært fokus på «snoking», og det føres logg på hvem og hvilket system man er inne i. Det er også andre systemer enn helsesystemene som har logg. For eksempel WebSak, Famac og Visma flyt. Ellers er trenden at nye IKT-systemer og nye versjoner av systemene stadig blir bedre og bedre tilpasset personvernbestemmelsene.

Det er særlig helse, HR og IKT-avdelingen i kommunen som har styring med de mest personvern-sensitive IKT-systemene i kommunen. Personvernombudet mener det er viktig å sette sikkerhetsmål og sikre et godt styringssystem som ivaretar målsettingene, og det er igangsatt et arbeid for å beskrive kommunens styringssystem.

6.2.2.2 Data fra intervju med virksomhetsledere

Det er gjennomført intervjuer med virksomhetslederne for tekniske tjenester og pleie- og omsorgstjenestene. Informasjon vi har fått i disse intervjuene oppsummeres i det følgende.

Vi har fått opplyst at dette er virksomheter der det er store forskjeller mellom de ansatte når det gjelder bruk av IKT-systemer. WebSak og Compilo er nevnt som viktige IKT-systemer for begge virksomheter. Foruten disse benytter virksomhetene ulike fagsystemer. Ved pleie- og omsorgstjenesten er Visma Profil et viktig IKT-system. Systemet er underlagt spesielle krav til sikkerhet, ettersom det er her pasientjournaler oppbevares. For de ulike virksomhetene i kommunen som bruker Visma profil er det opprettet en egen brukergruppe internt i kommunen.

Virksomhetslederne har oppgitt at de forholder seg til den overordnede strategien og planer for informasjonssikkerhet som finnes i kvalitetssystemet Compilo. Når det gjelder vurdering av risiko opplyser begge avdelinger at IKT-avdelingen er en viktig bidragsyter for dem med hensyn til å planlegge og gjennomføre oppgaver som har med IKT-sikkerhet å gjøre. Herfra får en også informasjon om aktuelle trusler og opplæring med hensyn til hvordan man skal forholde seg til disse.

I pleie- og omsorgstjenesten har det vært mye fokus på GDPR de senere årene, og de ansatte har fått opplæring i hvilke regler som gjelder. For pleie- og omsorgstjenesten er det pasientsystemene som er mest kritiske, og alle som skal ha tilgang i Visma Profil må signere for overholdelse av taushetsplikt. Det gis i utgangspunktet tilgang kun til de pasientene den enkelte skal ha ansvar for, og all bruk loggføres. Med hensyn til sikkerheten for brukere/pasienter er en likevel nødt til å ha en åpning for «nødvendig helsehjelp». Det er mulig å kjøre tester for å kontrollere om ansatte «snoker» i pasientjournalene. Dette gjøres i de tilfeller hvor det er mistanke om at snoking skjer.

Av aktuelle regler og rutiner, nevner virksomhetslederne rutiner for innføring av nytilsatte, som blant annet innebærer opplæring i de IKT-systemene som skal benyttes. Det benyttes her et eget skjema som krysses av og signeres når gjennomgangen er fullført. En har som fast rutine å slette alle tilganger når en ansatt slutter. Pleie- og omsorgstjenesten har videre opplyst at de har enkle regler for å hindre at uvedkommende ikke får tilgang til IKT-systemene; som for eksempel at en logger ut av systemene når en går fra datamaskinen, at man ikke låner bort brukernavn og passord andre, eller at en sikrer at det ikke ligger igjen informasjon på skriverne når en skanner papirdokumenter.

Tilbakemeldingen fra virksomhetene er at selv om man har strenge sikkerhetsrutiner for en del av IKT-systemene i kommunen, så gjør ikke dette at systemene blir tungvinte å bruke. Vi har ellers fått opplyst at virksomhetene har rollestyrt tilgang på de ulike systemene og at det holdes oversikt over hvem som har hvilke tilganger. De benytter ellers kun kommunalt IKT-utstyr.

Fra tekniske tjenester har vi fått opplyst at informasjonssikkerhet kan være tema på avdelingsmøter, men at det også er kultur for å ta opp ting mer uformelt i avdelingen. Fra pleie- og omsorgstjenesten har vi fått opplyst at det er igangsatt et arbeid for å innføre et internkontrollsystem som tilfredsstiller kravene i kommuneloven, og som også tilfredsstiller kravene i forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten.

6.2.2.3 Data fra intervju med superbrukere for Visma Profil og KOMTEK

For å se nærmere på hvordan informasjonssikkerhet praktiseres har vi valgt ut to IKT-systemer som brukes i kommunen, og innhentet ytterligere data i tilknytning til disse. Dette er KOMTEK som er et IKT-system for forvaltning av tekniske tjenester og Visma Profil som blant annet inneholder pasientjournaler for brukere i pleie- og omsorgstjenestene. Vi har blant annet hatt intervjuer med superbrukerne på disse systemene.

Superbruker på KOMTEK har opplyst at dette er et system som har svært få brukere i kommunen. Det er imidlertid lagret sensitive personopplysninger i systemet slik at det er viktig med gode sikkerhetsrutiner rundt systemet. Oppgaver som er tillagt superbruker er å holde kontakt med systemleverandøren med hensyn til endringer i systemet eller dersom det er noe i systemet som ikke fungerer. Superbruker har ikke oppgaver i forhold til de mer formelle tingene rundt personvern, som vurdering av personvernkonsekvenser (DPIA), behandlingsprotokoll og databehandleravtaler. Ellers er det slik at IKT-avdelingen bistår med oppdateringer og andre tekniske ting. Det er utarbeidet en brukerveiledning til systemet som skal kunne brukes ved eventuelt langtidssykefravær.

Superbruker for Visma Profil sine oppgaver er først og fremst å gi brukertilganger og sørge for å kjøre oppdateringer på systemet. Superbruker kan også bistå når det oppstår problemer, men avdelingene som benytter systemet har også direkte tilgang til support hos Visma. Visma Profil brukes av både pleie- og omsorg, psykisk helse- og rustjenesten og TIFU. De formelle tingene rundt informasjonssikkerhet og personvern i Visma Profil ivaretas av avdelingslederne, eventuelt i samarbeid med IKT-leder og/eller personvernombudet.

Det finnes en egen mappe for Visma Profil under administrative rutiner – felles for helse, pleie og omsorg. I denne mappen finnes det rutiner for bruk av systemet. De fleste dokumentene er ikke revidert det siste året.

6.2.3 Data fra spørreundersøkelsen

Under denne problemstillingen presenterer vi resultatene fra spørsmål knyttet til holdninger til digitalisering og digitalsikkerhet, og de ansattes syn på styring og kontroll.

I spørreundersøkelsen har vi spurt de ansatte om de opplever at kommunens ledelse er gode rollemodeller når det kommer til digital sikkerhet. De fleste, 54 % har svart at de i ganske stor grad eller i svært stor grad opplever at ledelsen er gode rollemodeller. 44 % har svart verken/eller. Det er videre 2 % som har svart at de i ganske liten grad opplever ledelsen som gode rollemodeller, og ingen som har svart at de i svært liten grad opplever dette. Tre fjerdedeler av deltakerne i undersøkelsen har besvart dette spørsmålet.

De ansatte er også blitt spurt om i hvilken grad de opplever at ledelsen har kommunisert tydelig hvilke forventninger de har til dem når det kommer til informasjonssikkerhet. Det er til sammen 58 % som har svart at de opplever dette i ganske stor grad eller i svært stor grad. Det er 27 % som har svart at de opplever dette i ganske liten grad, eller i svært liten grad. De øvrige 15 % har svart verken/eller på dette spørsmålet.

I spørreundersøkelsen har vi spurt de ansatte om virksomhetens regler for informasjonssikkerhet er til hinder for deres daglige gjøremål. 80 % mener reglene i svært lite grad eller i ganske liten grad har noe å si for deres daglige gjøremål. Det er 16 % som mener reglene verken/eller er til hinder. Det er videre 3 % som har svart at de i stor grad, eller i svært stor grad er til hinder for deres daglige gjøremål. Det er ca. tre fjerdedeler av de som har deltatt i undersøkelsen som har svart på dette spørsmålet.

På spørsmål om det hender at de ansatte bevisst bryter virksomhetens regler for informasjonssikkerhet, har de fleste, 97 %, svart at de er helt uenig eller delvis uenige i dette. 3 % har svart verken/eller på dette spørsmålet, mens det er ingen som har svart delvis enig eller helt enig. Også her er det er ca. tre fjerdedeler av de som har deltatt i undersøkelsen som har svart på dette spørsmålet

Avslutningsvis i spørreundersøkelsen har de ansatte fått et åpent spørsmål om hva de mener er hovedutfordringen med informasjonssikkerhet i deres virksomhet. Omtrent halvparten av de som har deltatt i undersøkelsen har besvart spørsmålet.

Av innspill som går igjen mange ganger er at en mangler opplæring og informasjon om informasjonssikkerhet. Det er i denne forbindelse ytret noe skepsis til e-læringskurs fordi de ikke er obligatoriske å gjennomføre, og at en da ikke vet om alle faktisk har den kunnskapen de har behov for. Det er også etterlyst opplæring som er relevant for den enkelte virksomhet, for eksempel innen helsesektoren. Et annet innspill som flere melder inn er virus som kommer gjennom e-post. Vi har også fått flere innspill på at stress og en hektisk hverdag øker risikoen for å gjøre feil.

Vi tar også med et utvalg av innspill som få eller bare en har kommet med. Disse mener at hovedutfordringen er:

- Manglende rutiner og at rutinene for informasjonssikkerhet gjør hverdagen mer tungvint.
- Økt risiko når informasjon skal deles med andre.
- At det ikke er nok fokus på informasjonssikkerhet i virksomhetene.
- At en er avhengig av å bruke private telefoner til jobboppgaver.
- At flere ansatte bruker samme PC eller at det er mange ansatte som jobber på samme arbeidsrom.
- At ansatte ikke logger seg ut ved dagens slutt.

- Deling av passord.
- Når man har med utstyr hjem og har hjemmekontor.

6.3 Revisors vurdering

6.3.1 Kommunens mål og strategi for informasjonssikkerhet

«E-strategi for Våler kommune 2018-2021» og «Sikkerhetsmål og sikkerhetsstrategi for Våler kommune» inneholder etter vår vurdering relevante sikkerhetsmål og strategi for arbeidet med informasjonssikkerhet i kommunen. Når det gjelder e-strategien er den imidlertid utgått på dato og situasjonen er en helt annen for kommunen i dag enn hva som var tilfelle da denne ble skrevet. Blant annet vil kommunens deltagelse i Indigo IKT IKS ha stor betydning. Kommunen bør, etter vår mening, få på plass en oppdatert plan for IKT-aktiviteten i kommunen. Vi mener også at det kan være hensiktsmessig å involvere personombudet i planleggingen, ettersom ombudet kan bidra med sin spesifikke kompetanse på personvern.

Ut ifra tilbakemeldinger vi har fått i intervjuer, er det vår vurdering at dokumenter som beskriver mål og strategi for informasjonssikkerhet er kjent for ledelsen i kommunen, og at de viktigste målene og strategiene for informasjonssikkerhet er kjent blant lederne i kommunen. Vårt inntrykk fra intervjuene er likevel at informasjonssikkerhet er noe som i stor grad overlates til andre. Fortrinnsvis IKT-avdelingen. Vi mener derfor at kommunen vil være tjent med å generelt ha større fokus på mål og strategi for informasjonssikkerhet. Både gjennom informasjon/opplæring, involvering og rapportering.

Vi mener likevel at revisjonskriterium 1 er etterlevd.

Kommunen må ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).

6.3.2 Kommunens internkontroll for informasjonssikkerhet

Fra intervjuer har vi fått informasjon om at kommuneledelsen jobber for å få på plass en mer lik/enhetlig struktur når det gjelder internkontroll, og at kvalitetssystemet Compilo er viktig med hensyn til dokumentasjon. Når det gjelder det strategiske perspektivet, er det utarbeidet et notat som beskriver kommunens styringssystem for informasjonssikkerhet og personvern. Det er lagt opp til at arbeidet med informasjonssikkerhet og personvern skal baseres på risikovurderinger.

Styringssystemet er etter hva vi kan forstå ikke iverksatt ennå. Det finnes etter hva vi kan se, ingen overordnet vurdering av risiko som er behandlet/diskutert i kommunens ledelse, og ledelsens årlige gjennomgang slik den er beskrevet i nevnte notat, er ikke gjennomført enda. Dette er sentrale deler av internkontrollsystemet som må være iverksatt før en kan si at en har et slik system. Notatet vedrørende styringssystem for informasjonssikkerhet og personvern er et godt utgangspunkt for det videre arbeidet på området, men det er viktig at en i startfasen er åpen for å vurdere justeringer og tilpasninger. Dette vil være en del av det å tilpasse systemet til egen organisasjon og de endringer som er i ferd med å innføres for IKT-området.

Sett i forhold til det generelle internkontrollsystemet i kommunen, er det ingenting som tilsier at internkontrollsystemet for informasjonssikkerhet og personvern ikke er tilpasset og integrert i kommunens helhetlige internkontrollsystem. Her må vi imidlertid basere oss på det vi har fått opplyst i intervjuer, ettersom det ikke finnes noen beskrivelse av et helhetlig internkontrollsystem for Våler kommune og hvordan dette er tenkt å fungere. En slik beskrivelse ville ha vært til hjelp for oss i våre

vurderinger. Større nytte vil imidlertid en slik beskrivelse ha for ledelse og ansatte i kommunen i forbindelse med å sikre integrering av det helhetlige internkontrollsystemet i kommunen.

Når det gjelder den mer operative tilnærmingen, så har vi sett at det utarbeides rutiner både for IKT-avdelingen, informasjonssikkerhet og personvern, samt rutiner for bruk av det enkelte IKT-system. Det registreres og håndteres avvik på området. Dette selv om det er veldig få avvik på IKT-området som rapporteres i avviksmodulen i Compilo, slik det er lagt opp til. Vi kan imidlertid ikke se at det gjennomføres systematiske risikovurderinger og at det utarbeides tiltaksplaner der det er høyere risiko enn hva som kan aksepteres, slik det er anbefalt.

Vi kan heller ikke se at det gjøres egne kontroller av at innførte internkontrolltiltak/rutiner følges opp/fungerer. Dette gjelder også helse- og omsorgstjenestene, der internkontroll for systemene er underlagt «Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren» og skal kunne dokumenteres. Vi har ikke sett dokumentasjon som tilsier at helse- og omsorgstjenestene i Våler kommune gjennomfører egne risikovurderinger, og planlegger og følger opp internkontrolltiltak for informasjonssikkerhet. At ledelsen går foran som gode forbilder er viktig i tilknytning til internkontrollen i kommunen. I spørreundersøkelsen til de ansatte i kommunen svarer de fleste at de opplever ledelsen som gode rollemodeller når det kommer til digital sikkerhet. Et flertall opplever videre at ledelsen har kommunisert tydelig hvilke forventninger de har til de ansatte når det kommer til informasjonssikkerhet. Det er likevel ca. en fjerdedel som ikke opplever dette i særlig grad.

Selv om vi mener at kommunen har en del å ta tak i når det gjelder internkontrollsystemet for informasjonssikkerhet, er det igangsatt et arbeid som kan få dette på plass. Vi mener derfor at revisjonskriterium 2 delvis er etterlevd.

Kommunen og kommunens øverste ledelse må ha en tilpasset og risikobasert internkontroll for informasjonssikkerhet. Internkontrollen inneholder både et strategisk og langsiktig perspektiv, og et operasjonelt perspektiv som omhandler daglig virksomhetsstyring.

6.3.3 Klargjøring av hva som kan aksepteres av risiko og oppfølging av risiko-områder

Når det gjelder å fastsette hva som kan aksepteres av risiko, beskriver notatet styringssystem for informasjonssikkerhet og personvern en måte å klassifisere informasjon i IKT-systemene (åpen, intern, fortrolig og strengt fortrolig). Slik vi har forstått det, er det tenkt at alle IKT-systemene i kommunen skal vurderes i henhold til denne klassifiseringen, og at hva som er akseptabel risiko og behovet for sikring skal vurderes for det enkelte system. Styringssystemet har ikke trådt i kraft ennå, og det gjenstår en del kartleggingsjobb som må på plass før ledelsen kan ta stilling til hva som kan aksepteres av risiko.

Vi har likevel mottatt risikovurderinger fra kommunen på enkelte systemer som er vurdert på tilsvarende måte når det gjelder personvern, og som er utarbeidet av IKT-leder og personvernombudet. I personvernombudets årsrapport etterlyses det større fokus på risikovurderinger i organisasjonen, og det etterlyses også flere ressurspersoner til å gjennomføre DPIA. Fra den gjennomførte spørreundersøkelsen til de ansatte ser vi at manglende opplæring og informasjon, virus som spres via e-post og risiko for å gjøre feil i en stressende og hektisk hverdag, er det som de ansatte i kommunen mener utgjør den største utfordringen med hensyn til informasjonssikkerhet.

Fra intervjuene er det likevel vårt inntrykk at ledelsen har oversikt over IKT-systemene i kommunen, og hvilke systemer som inneholder informasjon av kritisk verdi. Det er imidlertid lite systematikk og

planmessig oppfølging av risiko på IKT området, foreløpig. Vi mener derfor at revisjonskriterium 3 er delvis etterlevd.

Kommunen må ha fastsatt hva som kan aksepteres av risiko og gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi. Der risikoen er over fastsatt grense for hva som er akseptabelt bør det utarbeides tydelige tiltaksplaner som viser hvem som er ansvarlig for ulike tiltak.

6.3.4 Rutiner for å sikre konfidensialitet i informasjonssystemene

Sikkerhetsmålene for Våler kommune omhandler mål for sikring av IKT-systemene, fysisk sikring av lokaler og sporing av uønskede hendelser. Kommunen har rutinebeskrivelser som gir bestemmelser om tilgangen til IKT-systemene, og ut fra tilbakemeldingene i intervjuer er det vårt inntrykk at det vektlegges at den enkelte ansatte skal ha tjenstlig behov når de får tilgang til de ulike IKT-systemene. Den enkelte ansatte gjøres oppmerksom på, og ansvarlig-gjøres for sin rolle ved at de gjennomgår og bekrefter ansattretningslinjer for informasjonssikkerhet og personvern. I ansattretningslinjene redegjøres det for regler om taushetsplikt, fysisk sikring av personopplysninger og sikkerhet rundt IKT-systemene i kommunen. Med hensyn til sikkerhet rundt IKT-systemene fastsettes det blant annet regler for bruk av internett, installasjon av programvare, passordregler og regler for bruk av e-post.

Fra intervjuer har vi fått opplyst at det er mulig å ta ut logger fra systemene for å se hvem som har vært inne på hva i kommunens IKT-systemer, men at slike gjennomganger kun foretas dersom det er mistanke om «snoking». Vi mener en planmessig gjennomgang av denne typen logger kan være en effektiv måte for kommunen å kontrollere om rutinene på området følges. Omfanget må selvsagt vurderes og begrunnes ut fra risiko.

Vi mener at revisjonskriterium 4 er etterlevd.

Kommunen må ha rutiner og prosedyrer som sørger for at informasjon ikke blir kjent for uvedkommende.

6.3.5 Rutiner for å sikre integritet i informasjonssystemene

Som nevnt i vurderingen for revisjonskriterium 4 har kommunen rutinebeskrivelser som gir bestemmelser for tilgang til kommunens IKT-systemer, og et ansattreglement som gir oversikt over hva den enkelte ansatte skal være kjent med når det gjelder informasjonssikkerhet og personvern. Det at kommunen virker å ha god oversikt over hvem som har tilgang til kommunens IKT-systemer reduserer risikoen for at uvedkommende gis mulighet til å endre eller slette informasjon.

Det å ha god kunnskap om riktig bruk av IKT-systemene er viktig for å redusere risikoen for at informasjon registreres, endres eller slettes slik at det oppstår feil. Det er klarlagt i strategi- og rutinedokumenter at det er enhetslederne som skal sikre at ansatte får den opplæringen de har behov for. Det finnes en generell rutinebeskrivelse for opplæring av personell innen IKT. Både denne og ansattreglementet fokuserer på den enkelte ansatte sine plikter i forbindelse med forsvarlig sikring av personopplysninger og informasjon. Det at lederne i kommunen følges spesielt opp med hensyn til kjennskap til personvern og informasjonssikkerhet, med en årlig gjennomgang, er etter vår mening et viktig tiltak med hensyn til å sikre oppfølging i den enkelte virksomhet/enhet.

Vi har fra tekniske tjenester og pleie- og omsorgstjenestene fått tilbakemeldinger på at en også på virksomhets-/enhetsnivå har som rutine å lære opp nye ansatte i bruk av IKT-systemene og å gi påfyll

når det er behov for det, uten at det finnes noe skriftlig rutine på dette. Rutinebeskrivelsene for bruk av IKT-systemene ute i virksomhetene/enhetene vil imidlertid også være til hjelp for de som skal benytte de, og vil redusere risikoen knyttet til integritet. Loggføring av hvem som registrerer, endrer og sletter informasjon vil videre kunne gi nyttig informasjon i tilknytning til eventuelle avvik som oppstår, selv om en ikke bruker denne muligheten systematisk for å kontrollere at IKT-systemene brukes slik de skal.

Vi mener at revisjonskriterium 5 er etterlevd.

Kommunen må ha rutiner og prosedyrer som sørger for at informasjon ikke blir endret utilsiktet, eller av uvedkommende.

6.3.6 Rutiner for å sikre tilgjengelighet i informasjonssystemene

Våler kommunen har en e-strategi som legger vekt på tilgjengelighet, blant annet ved at det ved nyanskaffelser skal vektlegges økt mobilitet. Planen er videre å satse på skytjenester i større grad og felles grensesnitt for IKT-verktøyene. Det benyttes også autentiseringsmekanismer i nettverk, operativsystem og annen programvare som legger til rette for et begrenset antall passord for den enkelte. For å ivareta pasientsikkerheten planlegges det slik at personell på vakt har nødtilganger i IKT-systemene for helse- og omsorgssektoren. Dette er tiltak for å sikre god tilgjengelighet, uten at det nødvendigvis øker risikoen for at uvedkommende skal få tilgang til informasjon eller at informasjon endres eller slettes utilsiktet. Tilbakemeldingen fra intervjuer og fra spørreundersøkelsen til de ansatte er da også at de, med noen få unntak, ikke opplever at tiltakene for informasjonssikkerhet vanskeliggjør tilgangen til informasjon de har behov for i jobbsammenheng. I spørreundersøkelsen har videre de aller fleste svart at de ikke bryter reglene for informasjonssikkerhet bevisst.

Kommunen har egne rutinebeskrivelser for planlegging av utilsiktet avbrudd og avviksbehandling på IKT-området. Det finnes også en egen retningslinje for utarbeidelse av katastrofeberedskap. Disse dokumentene er utarbeidet med tanke om å sikre tilgjengeligheten til IKT-systemene. Tilbakemeldingene fra intervjuer er også at kommunen har lite «nedetid» i sine IKT-systemer, og tilbakemeldingen med hensyn til de beredskapsplaner som finnes, er at de har fungert når det har vært behov for å ta de i bruk. Behandling av uønskede hendelser, beredskap og systemgjenoppretting kommer vi imidlertid nærmere inn på under problemstilling 2.

Ut fra dette mener vi at revisjonskriterium 6 er etterlevd.

Kommunen må ha rutiner og prosedyrer som sørger for at informasjon er tilgjengelig ut ifra tjenstlige behov.

6.3.7 Ledelsens gjennomgang av aktivitetene på IKT-området

Tilbakemeldingene fra intervjuer er at det ikke finnes faste rutiner for ledelsen, når det gjelder å gå gjennom aktivitetene på IKT-området. IKT og informasjonssikkerhet kan likevel være tema i ulike møter på ledernivå. Vi mener det er viktig at kommunens ledelse med jevne mellomrom har gjennomganger der det kan tas stilling til eventuelle endringer i regelverk og endringer i risiko- og trusselbildet, slik det er anbefalt både fra KS og statlige myndigheter. En slik gjennomgang bør også oppsummere vesentlige og/eller alvorlige avvikssaker og hvordan disse er håndtert og fulgt opp, status på behandlingsaktivitetene, endringer i risikovurderinger og internkontrolltiltak, oppfølging av leverandører etc.

At ledelsen har en systematisk gjennomgang av aktiviteten er viktig uansett hvordan kommunen har organisert IKT-området, og vi mener en slik gjennomgang bør gjennomføres årlig. KS anbefaler i sin veileder for personvern og informasjonssikkerhet årlig gjennomgang. Den kan gjerne gjennomføres i forbindelse med gjennomgang av internkontroll på andre områder i kommunen. Vi mener videre at gjennomgangen bør dokumenteres. Dette for å ivareta det organisatoriske minne, men et referat eller en kort rapport vil også kunne forenkle formidling av informasjon ut i organisasjonen.

Vi registrerer at det i notatet «Styringssystem for informasjonssikkerhet og personvern» legges opp til egenrapportering på informasjonssikkerhet og personvern fra de ulike virksomheter/enheter og en årlig gjennomgang fra kommuneledelsen. Dette er foreløpig ikke trådt i kraft. Det er heller ikke, etter hva vi har oppfattet, bestemt hva en slik årlig gjennomgang skal omfatte. KS sin veileder har forslag til agenda for slike gjennomganger.

Vi mener at revisjonskriterium 7 foreløpig ikke er etterlevd.

- Kommunens ledelse må ha rutiner for å gjennomgå kommunens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året.

6.3.8 Dokumentasjon av ledelsens gjennomgang, og utarbeidelse av tiltaksplaner

I motsetning til øvrig virksomhet i kommunen har helse- og omsorgstjenestene i henhold til «Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren» et krav om at ledelsens gjennomgang, slik den er beskrevet under kriteriepunkt 7, dokumenteres. Fra pleie- og omsorgstjenesten har vi fått opplyst at det er igangsatt et arbeid for å endre kommunens internkontrollsystem slik at systemet både tilfredsstiller kravene i kommuneloven og kravene i forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten. Et sentralt krav i nevnte forskrift er at ledelsen for helse- og omsorgstjenestene har en systematisk gjennomgang av aktivitetene og internkontrollsystemet årlig. Vi mener ledelsens gjennomgang på IKT-området kan samkjøres med den årlige gjennomgangen av internkontrollsystemet i helse- og omsorgstjenestene. I denne forbindelse må kommunen også sikre at dokumentasjonskravet blir ivaretatt.

Norm for informasjonssikkerhet og personvern legger også opp til at helse- og omsorgstjenesten utarbeider tiltaksplaner for å rette opp avvik. Vi kan ikke se at tjenesten utarbeider slike planer i dag. tiltaksplanene skal det spesifiseres hvem som har ansvaret for gjennomføringen og hva slags tidsfrist en har for gjennomføringen.

Vi mener at revisjonskriterium 8 ikke er etterlevd.

- Ledelsens årlige gjennomgang innen informasjonssikkerhet og personvern i helse- og omsorgstjenestene må dokumenteres, og dersom gjennomgangen har avdekket at virksomhetens risikonivå ikke er i henhold til akseptabelt risikonivå må det være vedtatt tiltaksplaner for å rette opp avviket.

7 Problemstilling 2 – Implementering av sikkerhetstiltak

Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?

7.1 Revisjonskriterier for problemstilling 2

Følgende er en tabell med de kriterier vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A. Tabellen er interaktiv og leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriteriet. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor. Vi gjør derfor leseren oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

Kriterium 9	Kommunen må gjennomføre systematiske risikovurderinger på informasjonssikkerhetsområdet.
Kriterium 10	Kommuneledelsen må ha oversikt over og et bevisst forhold til: a. Styringsstrukturer, leveranser og understøttende systemer b. Enheter og programvare c. Brukere og behov for tilganger
Kriterium 11	Det må sikres jevnlig gjennomgang og vurdering av risiko når det gjelder: a. IKT-arkitektur b. Konfigurasjon av maskin- og programvare c. Nettverk d. Dataflyt, brukertilganger og behov for kryptering e. E-post og nettlesere
Kriterium 12	Kommunen må ta hensyn til informasjonssikkerheten i forbindelse med anskaffelser og utviklingsprosesser.
Kriterium 13	Kommunen må gjennomføre planmessig sikkerhetsovervåkning og testing på området.
Kriterium 14	Det må planlegges hvordan uønskede hendelser skal behandles, hvordan systemer og nettverk kan gjenopprettes og det gjennomføres øvelser på området.
Kriterium 15	For helse- og omsorgstjenestene må det planlegges og gjennomføres sikkerhetsrevisjoner. Resultatene fra sikkerhetsrevisjonene må følges opp og dokumenteres.
Kriterium 16	Kommunen må ha klare rutiner for avviksrapportering og -håndtering.

7.2 Innhentet data

7.2.1 Data fra dokumenter

E-strategi for Våler kommune gir noe informasjon om hvordan en tenker å tilrettelegge for sikkerhetstiltak i kommunen. Når det gjelder arkitektur legger e-strategien opp til en to-sone-modell med en intern og en sikret sone. For alle systemer skal det automatisk tas sikkerhetskopier som oppbevares i en katastrofelokasjon. Brukere av kommunens nettverk skal autentiseres på personnivå ved hjelp av katalogtjenesten i nettverket, mens autorisasjon administreres i det enkelte fagsystem. Det heter ellers at kommunen skal følge det arbeidet som skjer gjennom KS og KommIT [7] når det gjelder standardisering av arkitektur og felleskomponenter. Det opplyses i e-strategien om at kommunen har eget trådløst gjestenett tilgengelig.

I dokumentet «**Sikkerhetsmål og sikkerhetsstrategi for Våler kommune»** er det presisert at sikkerhetstiltak for Våler kommunes nettverk og systemer aldri skal baseres på at andre har en sikker infrastruktur. For datakommunikasjon skal kommunens nett deles inn i begrensede soner og brannmurer/sikkerhetsbarrierer skal skille mellom kommunen og eksternt nett. Det heter at all ekstern kommunikasjon skal rutes via sikkerhetsbarrierer som filtrerer ulovlige tjenester, uønsket informasjon, adresser og trafikkretning. Sikret sone sikres med to sikkerhetsbarrierer, og det skal være elektronisk overvåkning av ekstern nettverkstrafikk/kommunikasjon mot virksomhetskritiske systemer og nettverk i kommunen.

Autentiseringsmekanismer i nettverkskomponenter, operativsystem og annen programvare skal videre sikre at brukere har tilgang til relevant informasjon. Dette skal også redusere antall passord som en bruker må kunne. Det skal benyttes automatisk passord beskyttet skjermsparer. Systemene skal ellers oppdateres jevnlig med hensyn til sikkerhet. Servere og klienter skal være herdet mot innbrudd og nedetid, og det skal benyttes to-nivå automatisk viruskontroll. Strategien inneholder ellers regler for konfigurering av kommunens utstyr, kryptering og regler for tilkobling av IKT-utstyr som ikke eies av kommunen. Det er lagt vekt på at IKT-avdelingen skal ha oversikt over kommunens infrastruktur. Informasjonssystemene skal videre være konfigurert til å logge forsøk på uautorisert tilgang. Tilgang relatert til brukere skal være sporbart til brukernavn. Det heter ellers at det skal benyttes standardisert programvare- og maskinvare-plattformer i kommunens informasjonssystem. Strategien inneholder avslutningsvis kjøreregler for applikasjoner som utvikles spesielt for Våler kommune.

Strategidokumentet har et eget kapittel som omhandler regler for endringskontroll. Det heter her at beskyttelsesbehovet alltid skal vurderes ved endringer som berører informasjonssystemene. Endringer som kan ha betydning for informasjonssikkerheten skal godkjennes av sikkerhetsleder, og IKT-avdelingen skal, som grunnlag, utarbeide en risikovurdering med forslag til tiltak. Sikkerhet skal være et vurderingspunkt i eventuelle forprosjekter og gjennom alle faser av endringen. Sikkerhetsnivået skal ellers verifiseres før endringer drifts-settes.

Sikkerhetsstrategien har også egne kapitler om beredskap og avvikshåndtering. Det kan i denne forbindelse nevnes at sikkerhetsleder skal involveres i alle alvorlige hendelser. Dersom personvernopplysninger er kommet på avveie skal Datatilsynet varsles og personvernombudet involveres.

[7] KommIT er et rådgivende organ i KS innen digitalisering og smart bruk av teknologi. Kilde: https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/samstyringsstruktur/kommit-radet/

Våler har en egen **rutine for risikovurderinger knyttet til personopplysninger**. Formålet med rutinen er å sikre at den risikoen som avdekkes ved behandling av personopplysninger er innenfor de akseptkriterier kommunen har fastlagt. Rutinen skal identifisere trusler, angi sannsynlighet og konsekvens av en uønsket hendelse, gi oversikt over restrisiko og fastsette en plan for videre håndtering av uakseptabel risiko. Risikovurderinger knyttet til personopplysninger skal gjennomføres årlig, og også vurderes i forbindelse med organisasjonsendringer og ekstern overføring av nye typer opplysninger eller til nye partnere. Det er den som er daglig ansvarlig etter personopplysningsloven som har ansvaret for å igangsette risikovurderinger. Rutinen beskriver hvilke elementer som skal inngå i en risikovurdering. Blant annet skal vurderingen knyttes til konfidensialitet, tilgjengelighet og integritet/kvalitet. Restrisiko skal vurderes, håndteres og dokumenteres og resultatet fra vurderingen skal rapporteres til IT-ansvarlig, sikkerhetsansvarlig og i årlige ledelsesgjennomganger.

Veileder for anskaffelser i Våler kommune består av to deler der del I er et reglement mens del II er en beskrivelse av faser, rutiner og verktøy som skal hjelpe brukerne i anskaffelsesprosessen. Veilederen er generell og gjelder for alle typer innkjøp. Hensikten med veilederen er å sikre at lovverket om offentlige anskaffelser overholdes. Nyttig i forhold til IKT-anskaffelser er at innkjøpere må tenke tverrfaglig og gjøre en grundig gjennomgang av hvilke enheter og ledere som må involveres, allerede i behovsverifikasjonen. Ellers er spesifikasjonsfasen sentral, der både interne og eksterne rammebetingelser må tas hensyn til.

Retningslinjer ved utarbeiding av katastrofeberedskap må karakteriseres som et hjelpedokument for utarbeidelse av beredskapsplaner på IKT-området. Retningslinjene sier noe om hva en katastrofe kan være og hva som bør sikres. Dokumentet fokuserer spesielt på sensitive personopplysninger og kritiske systemer. En katastrofeplan skal i følge retningslinjene omhandle planlegging av katastrofehåndtering, kontinuitet, midlertidig drift og reetablering. Det gis videre en oversikt over hva som bør testes og det presiseres at katastrofeplanene må oppdateres jevnlig slik at de dekker den situasjonen som kommunen til enhver tid befinner seg i.

Det er utarbeidet en **prosedyre for planlegging av utilsiktet avbrudd – IKT**. Formålet med en slik plan er å sikre nødvendig behandling av personopplysninger ved avbrudd i normal drift, og at alternativ drift utføres planmessig. Det er IT-ansvarlig som har ansvaret for at det utarbeides planer. Planen skal inneholde identifisering og vurdering av kritisk avbrudd og virkningen på informasjonssikkerheten og informasjonssystemet. Den skal beskrive alternativ behandling og drift, metode for gjenskaping av normal drift etter korreksjon og beredskapsplaner. Endringer av prosedyren gjøres årlig i tilknytning til ledelsen gjennomgang.

I **prosedyre for avviksbehandling innen informasjonssikkerhet** heter det at avviksbehandling skal iverksettes ved sikkerhetsbrudd og/eller når oppgaver er gjennomført i strid med de rutiner som er besluttet. Formålet er å forbedre kvaliteten og sikkerheten i informasjonsbehandlingen i kommunen. Det er sikkehetsansvarlig som er ansvarlig for avvikssystemet. Avvik skal meldes i avviksmodulen i Compilo, og de skal behandles av nærmeste leder. Systemteknisk og korrigerende tekniske tiltak delegeres til IT- ansvarlig. Det er i prosedyren gitt eksempler på situasjoner som gjør det nødvendig å iverksette avvikshåndtering. All e-post med mistenkte og sikre virusalarmer skal varsles til IT-ansvarlig. Enhetsledere rapporterer til sikkerhetsansvarlig og IT-ansvarlig om avvik i egen enhet. I uthevet skrift i prosedyren står det at; ved brudd på informasjonssikkerheten som har medført uautorisert utlevering av sensitive personopplysninger, eller ved mistanke om slik utlevering skal avviket meldes til Datatilsynet. Det finnes en egen rutine for dette.

HelseCERTs [8] tilbakeblikk for Våler kommune i Hedmark for 2022 oppsummerer oversikt over trusler, anbefalinger og tiltak som er spesielt anbefalt for Våler kommune. Verdikjedeangrep, utpressing, svindel, spionasje og sabotasje er nevnt som aktuelle trusler overfor IKT-systemene for helse. Det opplyses at HelseCERT kan tilby hurtigtester, sikkerhetsskanning, og at det i 2023 vil fokuseres på loggføring. Alle medlemmer i HelseCERT anbefales å kjøre hurtigtest. Resultater fra gjennomførte inntrengningstester viser en positiv trend, men at en opplever mindre modenhet hos små virksomheter enn hos de store. Risikoområder som er avdekket i inntrengningstestene og som det anbefales at kommunen tar tak i, er svake passord, internt utviklede systemer som ikke følger beste praksis, sensitiv informasjon på delte filområder, dårlig sikring av interne systemer, svak sikring av terminalserver og feilkonfigurert tilgangsstyring for sertifikater (AD CS [9]). Av hendelser siste periode er det videre fokusert på skadevare via minnepinner og fakturasvindel. Fakturasvindel er en form for svindel hvor svindlerne forsøker å skaffe tilgang til legitime fakturaer og endre kontonummer på disse. Rapporten viser en generell utvikling i sårbarheter mot internett og e-postsikkerhet. HelseCERT har ikke observert sårbarheter for Våler i 2022, og det er heller ikke gitt spesielle anbefalinger til kommunen.

Vi har mottatt **skjematiske risikovurderinger** for enkelte av kommunens IKT-systemer vedrørende personvern der en vurderer sannsynligheten for at konkrete uønskede hendelser skal inntreffe, hva slags konsekvens dette kan få, og hva slags tiltak som må gjøres for å redusere risikoen.

Andre dokumenter og rutinebeskrivelser fra Compilo som er aktuelle i tilknytning til sikkerhetstiltak for å hindre dataangrep og uautorisert tilgang til informasjon:

- IKT organisering
- Ansvar og myndighet for daglig ansvar innen hver enhet – IKT
- IT-ansvarlig sitt ansvar og myndighetsområde
- Systemansvarlig ansvars og myndighetsområde - IKT
- Rutine for bruk av internett
- Prosedyre for bruk av bærbart utstyr
- Låserutiner og adgangskontroll – IKT
- Rutine for melding til Datatilsynet
- Rutine for kontroll og tilgang lukket sone
- Rutine for hjemmekontor

7.2.2 Data fra intervjuer

Fra **kommunedirektøren** har vi fått opplyst at en har vurdert at risiko og sårbarhet i tilknytning til IKT-drift er for høy i dag, og at løsningen er å knytte seg til et større fagmiljø gjennom det interkommunale samarbeidet Indigo IKT IKS. Måten trusler og endringer i risiko fanges opp er ellers at eksterne samarbeidspartnere kommer med innspill via IKT-avdelingen.

Når det gjelder drift av kommunens IKT-systemer er det virksomhetslederne som står som systemeier for fagsystemene i egen virksomhet. Deretter oppnevnes det gjerne superbrukere i virksomhetene

[8] HelseCERT er helse- og omsorgssektorens nasjonale senter for cybersikkerhet. CERT står for Computer Emergency Response Team. Kilde: https://www.nhn.no/tjenester/helsecert

[9] AD CS står for Active Directory Certificate Services, og er en Microsoft Windows Server-rolle for utstedelse og forvaltning av digitale sertifikater over datanettverk – såkalte PKI (Public Key Infrastructure). Kilde https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview og https://no.wikipedia.org/wiki/Public_key_infrastructure

som kjenner godt til fagområdet som systemet skal dekke. På den mer tekniske delen må i mange tilfeller IKT-avdelingen bistå som superbrukere, blant annet når det gjelder programvare-oppdateringer, tilganger etc. Kommunen har regler for bruk av kommunens PC-er og telefoner for å sikre informasjon i IKT-systemene. Kommunen har også regler for hjemmekontor. Det brukes ellers ikke private PC-er og telefoner på kommunens IKT-systemer. IKT-avdelingen er sentral med hensyn til å holde i orden utstyr, servere og annen infrastruktur, ta backup etc. Med hensyn til informasjonssikkerheten er det mye som løses fortløpende når det er tid til det, eller det oppstår en situasjon. Det er ikke så mye langsiktig planlegging når det gjelder sikkerhetstiltak og vedlikehold.

Kommunedirektøren har opplyst om at informasjonssikkerhet er en del av kravspesifikasjonen i forbindelse med anskaffelse av IKT-systemer og utstyr, og er omtalt i eget kapittel når det legges ut anbud. Informasjonssikkerhet og andre IKT-utfordringer kan også være tema i forbindelse med endringsprosesser i kommunen. Som eksempel ble det nevnt samling av tekniske tjenester i Våler og Åsnes, der de ulike tjenestestedene benytter forskjellige IT-løsninger. Slike ting må kartlegges og det må klargjøres hvilke systemer en kan ha felles, og hvilke som fortsatt må brukes separat. Kommunedirektøren fremholder ellers at det er viktig å involvere fagpersoner både i anskaffelses- og endringsprosesser på IKT-området.

Når det gjelder beredskap på IKT-området er kommunen i prosess med å utarbeide ny ROS-analyse. NOU-en «Nå er det alvor» tar til orde for økte krav til beredskap i kommunene med hensyn til strøm, IT og vann. Kommunens gjeldende beredskapsplan vil være for kortsiktig med hensyn til nye krav som stilles, og bevisstheten rundt beredskap i kommunen vil generelt måtte høynes. Kommunedirektøren opplyser at IKT-leder sitter i beredskapsutvalget, noe som er hensiktsmessig med hensyn til å få dekket IKT-området på en god måte. Det er ikke gjennomført øvelser i Våler som har berørt IKT-området mens nåværende kommunedirektør har vært i kommunen.

Fra **IKT-leder** har vi fått opplyst at vurderinger knyttet til risiko for dataangrep og uautorisert tilgang til systemene gjøres daglig. NSMs [10] anbefalinger for IKT-sikkerhet er implementert i organisasjonen. Det er lite innspill med hensyn til IKT-sikkerhet fra egen organisasjon. Når det gjelder avvikssystemet i Compilo er dette generelt lite brukt i forbindelse med IKT-sikkerhet, og det brukes heller ikke i forbindelse med risikovurderinger. Det er først og fremst HelseCERT, Kommune-CSIRT og de store IT-leverandørene som er de viktige kildene med hensyn til aktuell risiko. Kommunen kjøper også IKT-bistand fra andre der det er behov. IKT-leder tilkjennegir at kommunen i stor grad lener seg på Visma og de andre store og seriøse leverandørene når det gjelder informasjonssikkerhet. Det holdes ellers jevnlige webinarer om IKT-sikkerhet, som IKT-avdelingen i kommunen deltar på.

De ulike IKT-systemene har egne superbrukere. På noen områder fines det også brukergrupper internt i kommunen. Eksempelvis Visma Profil der en har en brukergruppe med representanter for hver avdeling som bruker systemet. For KOMTEK finnes en brukergruppe for flere av kommunene i nærområdet. IKT-leder kunne ønske seg superbrukere med større teknisk kunnskap om systemene. Slik det er i dag bøtes dette på ved at IKT-avdelingen er involvert på den tekniske siden i mange av IKT-systemene.

Med hensyn til bruk av kommunale telefoner har IKT-leder opplyst om at det finnes egne telefoni-avtaler som gir regler for nedlasting av programvare etc. Kommunen har videre eget reglement for

[10] Nasjonal sikkerhetsmyndighet.

bruk av kommunens PC-er på hjemmekontor. Alle PC-er har for øvrig to-faktor-pålogging på VPN. [11] All kommunikasjon i kommunens IKT-systemer er kryptert, inkludert informasjon som ligger i kommunens PC-er. Mal for telefoni-avtaler og regler for hjemmekontor ligger i Compilo. Alle IKT-systemene i kommunen ligger bak brannmurer, og kommunen har få gamle utdaterte IKT-systemer. IKT-leder mener ut fra dette at kommunen skal være rimelig trygg for forsøk på inntrengning fra utsiden.

IKT-avdelingen holder fortløpende oversikt over IKT-systemene i kommunen. Pleie- og omsorgssystemene ligger i eget lukket nett, beskyttet av egne brannmurer. Kommunen har ellers eget elevnett og gjestenett. Dette med IKT-arkitektur er noe IKT-leder mener at kommunen kunne utviklet mer, men det vil uansett i stor grad handle om hvem som har tilgang til hvilke IKT-systemer. Når det gjelder konfigurering har kommunen interne regelsett for dette. For Office365 og brannmurer benyttes eksterne konsulenter i forbindelse med konfigurering. Deler av nettverk leases fra TietoEvery og oppdateringer med hensyn til nettverkssikkerhet er inkludert i avtalen.

IKT-avdelingen deltar vanligvis som rådgivere på det tekniske i utviklingsprosesser eller i forbindelse med anskaffelser. Når det gjelder anskaffelse av IKT-systemer og utstyr kjører IKT-avdelingen prosessen selv. Kommunen kjøper fra store anerkjente IKT-leverandører som kommunesektoren har hatt gode erfaringer med gjennom mange år, og som en vet jobber seriøst med sikkerheten i sine systemer. IKT-leder trakk her frem Acos som samarbeider med Kommune-CSIRT. Dette samarbeidet har blant annet ført til at en har avdekket og fått sikret en sårbarhet i Acos sin skyløsning. Dette kommer da alle Acos sine kunder til gode. Våler kommune utvikler ikke egne informasjonssystemer.

IKT-leder har opplyst om at kommunen har egne kontaktpersoner hos IKT-leverandørene. I en innføringsperiode for et IKT-system er det jevnlig kontakt. Kontakten blir mer sporadisk når systemene er implementert. Dersom en er misfornøyd med noe eller det er noe man lurer på, og IKT-leder opplever at det fungerer godt å ta kontakt med leverandørene.

Når det gjelder sikkerhetsovervåkning og testing av IKT-systemene, så gjøres dette kontinuerlig gjennom automatisk sikkerhets- og sårbarhetstest (scanning) av servere mot internett. Det er flere instanser som gjør dette: KommuneCSIRT, HelseCERT og AllvisNOR (NSM). Kommunen får rapporter fra HelseCERT hver måned. AllvisNOR skanner målrettet etter åpninger og kommunen får beskjed hvis de finner noe.

Sikkerhetsrevisjoner i pleie- og omsorgssystemene er, ifølge IKT-leder, en del av den generelle og løpende gjennomgangen av IKT-systemene. Kommunen får videre en årsrapport fra HelseCERT som sier noe om aktiviteten gjennom året og som gir anbefalinger mht. sikkerhetstiltak. Årsrapport fra HelseCERT inneholder også testresultater for Våler kommune spesielt. Rapportene blir gjennomgått og anbefalinger blir fulgt opp. Som minimum blir det gjort en risikovurdering av anbefalingene. IKT-leder fortalte ellers at det i disse dager er viktig med de geografiske sperrene som vanskeliggjør forsøk på å komme inn i systemene fra utlandet.

IKT-leder sitter i kommunens beredskapsutvalg og er således tett på med hensyn til å planlegge hva som skal gjøres dersom det oppstår uønskede hendelser på IKT-området. Det har ikke vært noen egne øvelser der IT-sikkerheten har vært tema. Det er imidlertid behov for å gjenopprette IKT-systemer innimellom, slik at en uansett har en viss øvelse i dette. Strømbrudd er også noe kommunen er utsatt

[11] VPN står for Virtual Private Network, eller virtuelt privat nettverk. Kilde: https://no.wikipedia.org/wiki/Virtuelt_privat_nettverk

for fra tid til annen, og beredskapen har i slike tilfeller fungert godt. Det tas backup av systemene hver natt, som oppbevares i hvelv. Som tidligere nevnt brukes ikke avvikssystemet i Compilo i særlig grad for interne avvik som gjelder IKT. Avvikene meldes heller inn via e-post/supportmeldinger, fordi dette er raskere. Meldingene følges opp fortløpende, og problemene løses der og da.

7.2.2.1 Data fra intervjuer med virksomhetsledere

I det følgende oppsummeres informasjon vi har fått i intervju med virksomhetslederne for tekniske tjenester og pleie- og omsorgstjenestene.

Når det gjelder risikovurderinger knyttet til IKT og informasjonssikkerhet har vi fått opplyst at virksomhetene i stor grad støtter seg på IKT-avdelingen. Hit melder de fra om avvik og de får også informasjon om risikoforhold de bør fokusere på. Det er ikke så ofte virksomhetene gjør anskaffelser og/eller omstillinger med betydning for informasjonssikkerheten. Dersom det er aktuelt støtter en seg også her på IKT-avdelingen og RIIK [12] dersom det gjelder anskaffelser. I pleie- og omsorgstjenesten har en videre hatt et samarbeid med kommunene i Sør-Østerdal om velferdsteknologi. En har da blant annet vært opptatt av oppbevaring av data i systemene.

Virksomhetene er ikke direkte involvert i sikkerhetsovervåkning og testing av IKT-systemene. IKT-avdelingen er sentral her. Ellers stoler en i stor grad på at leverandørene av IKT-systemene ivaretar sikkerheten. Det blir ikke gjort noen egen gjennomgang av IKT-systemene fra pleie- og omsorgstjenesten sin side.

Når det gjelder håndtering av uønskede hendelser, gjenoppretting av systemer og beredskapsøvelser, så har tekniske tjenester opplyst at IKT er en del av kommunens beredskapsplan. Kommunen hadde en bordøvelse som berørte IKT-systemene for noen år siden, og en har også hatt lengre strømbrudd der rutinene for beredskap har vært prøvd ut i praksis. Dette har fungert slik det var planlagt. Pleie- og omsorgstjenestene har informert oss om at de har egen beredskapsplan. De har fått prøvd ut beredskapsplanene, for eksempel i forbindelse med strømbrudd, noe som opplyses å ha fungert godt.

I tilknytning til rapportering og håndtering av avvik oppgir pleie- og omsorgstjenesten at de bruker avvikssystemet i Compilo. Registrerte avvik kan være tema på personalmøter, men avvikene som diskuteres i personalmøtene er vanligvis andre typer avvik en avvik knyttet til IKT-systemene og personvern. Fra tekniske tjenester har vi fått opplyst at avvik innen IKT og informasjonssikkerhet som regel haster, og at man da tar direkte kontakt med IKT-avdelingen.

7.2.2.2 Data fra intervju med superbrukere for Visma profil og KOMTEK

Superbruker KOMTEK har opplyst at ikke er involvert i vurdering av risiko rundt systemet. Systemet oppdateres imidlertid jevnlig, og oppdateringene kan ha med sikkerheten å gjøre. Det er ellers veldig få i kommunen som har tilgang til systemet, noe som i seg selv reduserer risikoen. Systemet er ellers lite sårbart for nedetid, slik at strømbrudd og brudd i nettforbindelsen utgjør liten risiko. Superbruker oppgir å ha fått opplæring i bruk av avviksmodulen i Compilo, men bruker denne svært sjelden.

Fra superbruker for Visma Profil har vi fått opplyst at IKT-avdelingen holder oversikt over risiko som vedrører kommunens servere, mens Visma gir informasjon med hensyn til deres spesifikke IKT-systemer. Ellers får kommunen informasjon om trusler og endringer i risikobildet fra HelseCERT når det gjelder IKT-systemene innen helse- og omsorgstjenestene, og fra KommuneCSIRT. Oppdatering og vedlikehold av Visma Profil er det Norsk helsenett som står for. Det være seg å rette opp i feil som

[12] Regionalt innkjøp i Kongsvingerregionen.

oppstår, avdekke og følge opp svakheter og ivareta sikkerheten. Visma Profil planlegges å bli skybasert fra 2025, noe som vil redusere risikoen ytterligere.

Alt som gjøres i systemet loggføres, slik at det er mulig for avdelingslederne å sjekke for eksempel om ansatte har vært inne på brukere de ikke har oppgaver i forhold til. Det foretas sikkerhetskopiering av opplysningene i Visma Profil hver kveld, og backup oppbevares sikkert. Visma Profil sikres også ved de mer generelle tiltakene som IKT-avdelingen gjør. For eksempel ved at det følges med på brannmuren med hensyn til forsøk på å omgå denne, og på e-poster med mistenkelig innhold. Eventuelle risikovurderinger knyttet til informasjonssikkerhet og personvern når det gjennomføres endringsprosesser eller investeres i nytt IKT-utstyr eller nye IKT-systemer, gjennomføres av avdelingslederne og IKT-leder.

Kommunen har fått prøvd ut sin beredskap på IKT-siden i forbindelse med strømbrudd og/eller at internett har vært nede. Når det gjelder helse- og omsorgstjenestene har sykehjemmet eget nødstrømsaggregat som sikrer strømforsyning. En er heller ikke avhengig av kommunens nett for å ha tilgang til Visma. Har man tilgang på mobilnett så skal det være mulig for sykehjemmet å få tilgang, selv om kommunens nett er nede. Rapportering om feil til IKT-avdelingen meldes vanligvis på e-post, og det er ikke så ofte at avvikssystemet i Compilo benyttes i forhold til IKT-saker.

7.2.3 Data fra spørreundersøkelsen

Under denne problemstillingen presenterer vi resultatene fra spørsmål knyttet til risikooppfattelse og sikkerhetsatferd blant de ansatte.

Med hensyn til **hvordan de ansatte oppfatter risiko** har de tatt stilling til et utvalg av hendelser som kan utgjøre en sikkerhetsrisiko, og hvor bekymret den enkelte er for at disse hendelsen skal ramme en selv på en skala fra 1 til 5, der 1 tilsier at en i svært liten grad er bekymret, mens 5 tilsier at en i svært stor grad er bekymret. For alle de beskrevne hendelsene ligger gjennomsnittssvarene rundt midtverdien 3. Svarene for den enkelte hendelse fordeler seg som følger:

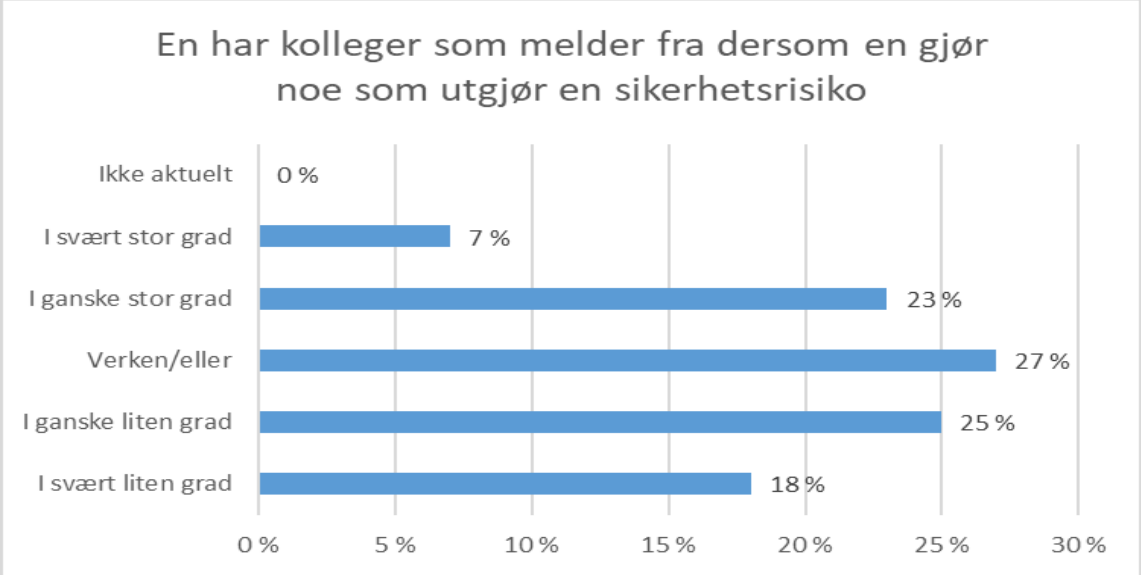
Hvor bekymret er du for at følgende hendelser skal ramme dag (poengskala fra 1-5)	**1** Svært liten grad	**2** Ganske liten grad	**3** Verken/ eller	**4** Ganske stor grad	**5** Svært stor grad	**Vet ikke**
At jeg skal få virus el. på arbeidsgivers datautstyr	19%	30%	10%	27%	14%	0%
At jeg skal bli lurt til å gi fra meg informasjon	22%	20%	13%	25%	9%	1%
At min virksomhet skal bli utsatt for svikt i digitale systemer på bakgrunn av utilsiktede feil	8%	26%	18%	30%	16%	2%
At jeg mister egne/arbeidsgivers data	10%	26%	16%	24%	23%	1%

De ansatte har også tatt stilling til hvilken risiko de forbinder med et utvalg av aktiviteter på en skala fra 1 til 5, der 1 er i svært liten grad, mens 5 er i svært stor grad. Flest mener det er høy risiko ved å dele jobb-passord med andre (gjennomsnittssvaret her er på 4,3). Bruk av e-post scorer lavest (gjennomsnittssvaret er her på 2,6). Svarene for den enkelte aktivitet fordeler seg som følger:

I hvilken grad forbinder du følgende aktiviteter med høy risiko (poengskala fra 1-5)	1 Svært liten grad	2 Ganske liten grad	3 Verken/ eller	4 Ganske stor grad	5 Svært stor grad	Vet ikke
Bruke e-post	14%	41%	18%	21%	5%	1%
Dele jobb-passord med andre	4%	8%	7%	14%	66%	1%
Bruke sosiale medier	7%	15%	26%	34%	16%	2%
Bruke digitale assistenter (som smart høytalere, Siri/Bixby ol)	9%	14%	38%	16%	11%	12%
Bruk av minnepinner og lignende	9%	20%	26%	24%	11%	10%
Bruk av sky-tjenester	10%	29%	33%	14%	5%	9%
Mottak av SMS-er med lenke	8%	6%	15%	32%	33%	6%

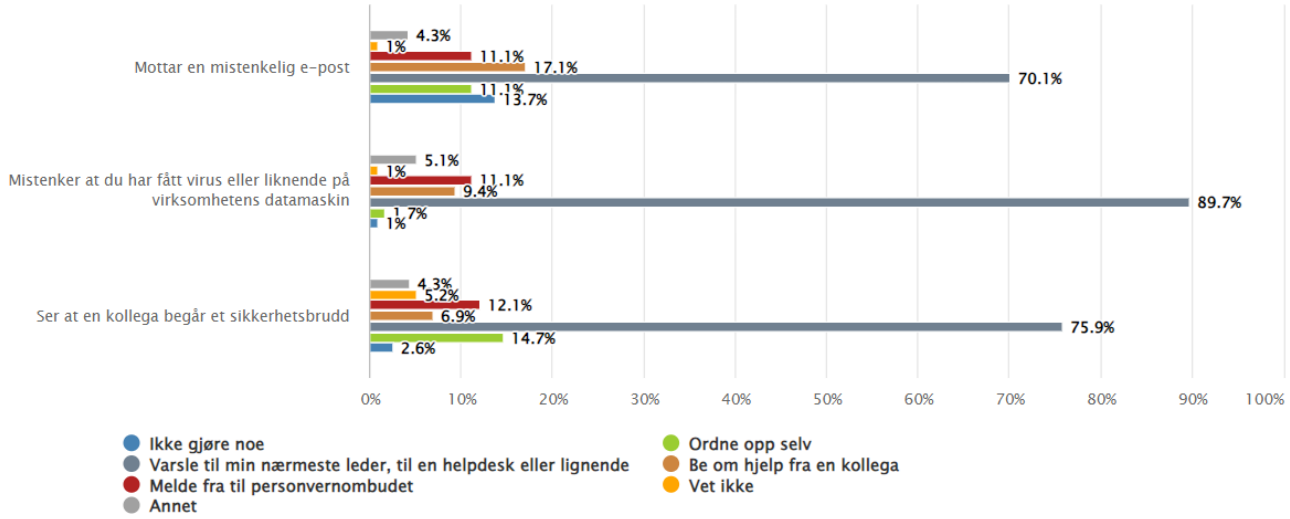
De fleste mener det er større risiko for at andre skal gjøre noe mot arbeidsgivers digitale tjenester eller enheter, en at de selv skal gjøre en feil som går utover de digitale tjenestene eller enheter. Det er 53 % som har svart at det er andre som utgjør størst risiko, mens 25 % har svart at de selv utgjør en risiko. Det er 22 % som har svart «vet ikke» på dette spørsmålet.

Når det gjelder **atferd knyttet til informasjonssikkerhet** har vi spurt de ansatte om deres kolleger sier ifra til dem om de gjør noe som utgjør en risiko for informasjonssikkerheten i virksomheten. Svarene fordeler seg som følger:



De fleste, 44 %, mener i motsatt fall at det er ganske lett å si ifra til en kollega dersom en ser at denne gjør noe som kan utgjøre en risiko for informasjonssikkerheten. Det er 24 % som har svart verken/eller og 17 % som har svart at det er svært lett å si fra til en kollega. Det er videre 12 % som har svart at det er ganske vanskelig å si fra og 3 % som har svart at det er svært vanskelig å si fra dersom en ser at en kollega gjør noe som kan utgjøre en risiko for informasjonssikkerheten i virksomheten.

Som en oppsummering av spørsmål knyttet til sikkerhetsatferd, er de ansatte blitt spurt om hva de vil gjøre dersom de opplever å motta en mistenkelig e-post, mistenker at de har fått virus eller lignende på kommunens datamaskin eller ser at en kollega begår et sikkerhetsbrudd. Det ble gitt syv forskjellige svaralternativer på hvert spørsmål og man kunne velge to alternativer på hvert spørsmål. Svarene kan oppsummeres i følgende figur:



I spørreundersøkelsen har de ansatte også svart på om de vet hvem de skal melde fra til dersom det oppstår en digital sikkerhetshendelse. 87 % svarer at de vet hvem de skal melde fra til, mens de øvrige 13 % ikke vet det. De som har svart at de vet hvem de skal melde fra til har vi fulgt opp ved at de har fått angi hvem de ville meldt fra til. Det er mange som ville meldt fra til flere instanser. De aller fleste ville meldt fra til IKT-avdelingen, men også til nærmeste ledere/kommunens ledelse. 10 av de 95 som har svart på spørsmålet ville meldt fra til personvernombudet, mens 9 av de 95 ville rapportert avvik i Compilo. Det er også noen som ville meldt fra til IT-ansvarlig (her vet vi ikke om det er IKT-avdelingen de mener, eller om det er IT-ansvarlig for et bestemt IKT-system), verneombud, Datatilsynet, beredskapssjef og/eller personalsjef.

7.3 Revisors vurdering

7.3.1 Systematiske risikovurderinger på området

Vi kan ikke se at det gjennomføres systematiske risikovurderinger når det gjelder informasjonssikkerhet, utover at det er gjennomført risikovurderinger for enkelte av IKT-systemene når det gjelder personvern. I det daglige er IKT-avdelingen sentral med hensyn til å fange opp trusler og avvik, og å holde seg orientert om risikobildet generelt. Andre virksomheter henviser også til IKT-avdelingen eller IKT-leverandørene, både når det gjelder informasjonssikkerhet generelt og når det gjelder sikkerhet i tilknytning til deres egne fagsystemer. Kommunens IKT-avdeling har til nå bestått av to personer, noe som tilsier at kommunen er svært sårbar ved sykdom eller utskifting av personell Sårbarheten når det gjelder IKT-systemene vil sannsynligvis reduseres når kommunen nå går inn i samarbeidet Indigo IKT. Vi mener likevel at en viktig del av risikovurderingene med hensyn til informasjonssikkerhet må foregå ute i enhetene/virksomhetene ettersom organisering av virksomheten, internkontroll og holdninger er like viktige som de tekniske sikkerhetstiltakene. Hva som kan aksepteres av risiko på området er videre noe kommunens ledelse må ta stilling til. Vi merker oss for øvrig at kommunen har utarbeidet rutiner som skal ivareta informasjonssikkerheten i forbindelse

med mer bruk av bærbare enheter og hjemmekontor. Vi er enige med personvernombudet her, som i sin årsrapport for 2022 påpeker at det bør kurses og veiledes i risikovurderinger i kommunen.

Kommunen har likevel et visst grunnlag for å få på plass systematiske risikovurderinger. Det er utarbeidet en egen rutine for risikovurderinger knyttet til personvern som skal gjennomføres årlig. I notatet «Styringssystem for informasjonssikkerhet og personvern» finnes forslag til hvordan verdien av informasjonen i IKT-systemene skal kategoriseres, og hvordan risiko på området skal håndteres. Rutiner for risikovurderinger og styringssystem for informasjonssikkerhet og personvern er foreløpig ikke tatt i bruk.

I spørreundersøkelsen har vi stilt de ansatte i kommunen noen spørsmål knyttet til hvordan de oppfatter risiko knyttet til informasjonssikkerhet. De ansatte er ganske delt når det gjelder bekymring for å få virus e.l. på arbeidsgivers datautstyr. De er mer bekymret for at virksomheten som sådan skal bli utsatt for svikt i digitale systemer på bakgrunn av en utilsiktet feil eller at de mister egne/arbeidsgivers data, enn at de skal bli lurt til å gi fra seg informasjon. De fleste mener videre det er større risiko for at andre skal gjøre noe mot IKT-systemene enn at de selv skal gjøre en feil som rammer IKT-systemene.

De fleste er enige i at det er høy risiko ved å dele passord med andre, SMS-er med lenke og bruk av sosiale medier. Det er mer varierende hvordan de ansatte vurderer risikoen ved bruk av digitale assistenter, minnepinner og lignende. Minnepinner var et av de risikoområdene som HelseCERT tok opp i sin årsrapport for 2022. Minst risiko mener de ansatte det er forbundet med bruk av sky-tjenester og e-post. Dataangrep via e-post-systemer er måten som for eksempel Østre-Toten kommune fikk satt sine IKT-systemer ut av spill på. Vi mener at svarene understøtter behovet for opplæring og informasjon om risiko ut til enheter/virksomheter.

Ut fra dette mener vi at revisjonskriterium 9 ikke er etterlevd.

Kommunen må gjennomføre systematiske risikovurderinger på informasjonssikkerhetsområdet.

7.3.2 Kommuneledelsens oversikt over sentrale deler av IKT-området

IKT-avdelingen er sentral når det gjelder å holde oversikt over den interne infrastrukturen for IKT, enheter, programvare og sikkerheten rundt dette. Ut fra de oversikter som avdelingen opererer med, og tilbakemeldinger vi har fått gjennom intervjuer, er det vårt inntrykk at avdelingen har en tilfredsstillende oversikt over sitt område.

IKT-avdelingen er en del av kommunedirektørens stab, og det synes å være tett kontakt mellom IKT-avdelingen og kommunedirektør. Vi mener likevel at arbeidet med informasjonssikkerhet kunne vært mer planmessig og strukturert, og at kommuneledelsen minst bør ha en årlig gjennomgang/oppsummering av tiltakene og hva som er gjort. Dette inkludert risikovurderinger, avvikshåndtering og hvordan internkontrollsystemet har fungert på området. Dette er etter vår mening viktig for å sikre kommuneledelsen tilstrekkelig oversikt på området.

Systemeiere og superbrukere har ellers, sammen med IKT-avdelingen, ansvar for å holde oversikt over hvem som har hvilke tilganger. Kommunens policy for tilgang til IKT-systemene er tydelig på at en ikke skal ha flere tilganger enn nødvendig. Ut fra hva vi kan forstå, følges dette opp på en god måte.

Vi mener at revisjonskriterium 10 er delvis etterlevd.

Kommuneledelsen må ha oversikt over og et bevisst forhold til:
a. Styringsstrukturer, leveranser og understøttende systemer
b. Enheter og programvare
c. Brukere og behov for tilganger

7.3.3 Gjennomgang av risiko på sentrale deler av IKT-området

Det er vår oppfatning at det ikke gjennomføres planmessige gjennomganger av sentrale deler av IKT-området. Tilbakemeldingen vi har fått er at dette gjennomføres fortløpende når det er behov for det, eller når en har tid til å gjøre det. Nasjonal sikkerhetsmyndighet anbefaler at dette gjennomføres planmessig og vi mener planleggingen av denne typen gjennomganger bør ses i forbindelse med vurdering av risiko. Så må kommunen selvsagt også være rustet til å ta hånd om mer fortløpende hendelser, som for eksempel når de får innspill på risikoforhold fra IKT-leverandørene eller de andre samarbeidspartnerne på IKT-sikkerhet.

Ellers registrer vi at kommunen i sine strategidokumenter, rutinebeskrivelser etc. legger opp til å følge Nasjonal sikkerhetsmyndighet sine grunnprinsipper for IKT-sikkerhet for områdene a-e i kriteriepunktet under. En plan for gjennomgang av IKT-sikkerheten må omfatte alle disse områdene.

Gjennomgang og vurdering av risiko blir etter vår mening for tilfeldig, noe som øker risikoen for at faresignaler kan bli oversett. Ut fra dette mener vi at revisjonskriterium 11 bare delvis er etterlevd.

Det må sikres jevnlig gjennomgang og vurdering av risiko når det gjelder:
a. IKT-arkitektur
b. Konfigurasjon av maskin- og programvare
c. Nettverk
d. Dataflyt, brukertilganger og behov for kryptering
e. E-post og nettlesere

7.3.4 Informasjonssikkerhet ved anskaffelser og i utviklingsprosesser

Kommunens strategidokumenter på området og kommunens innkjøpsveileder legger opp til at informasjonssikkerhet skal tas hensyn til i forbindelse med utviklingsprosesser og i forbindelse med anskaffelser. Fra intervjuer er det vårt inntrykk at IKT-avdelingen alltid involveres i de IKT-faglige vurderingene som må gjøres i endringsprosesser eller anskaffelser som kan innvirke på informasjonssikkerheten. I henhold til den dokumentasjon vi har mottatt er dette slik disse prosessene er ment å fungere.

Vi mener at revisjonskriterium 12 er etterlevd.

Kommunen må ta hensyn til informasjonssikkerheten i forbindelse med anskaffelser og i utviklingsprosesser.

7.3.5 Planmessig sikkerhetsovervåkning og testing

Vi kan ikke se at det finnes noen egen plan for sikkerhetsovervåkning og testing av IKT-systemene. Fra intervjuer har vi fått opplyst at den løpende sikkerhetsovervåkningen og testingen av IKT-systemene som blir gjort av kommunens samarbeidspartnere på området er viktig for Våler kommune. Det er IKT-avdelingen som får tilbakemeldinger fra samarbeidspartnerne på risikoforhold som kommunen bør ta tak i. Det gjøres ellers en risikovurdering i tilknytning til rapporter på informasjonssikkerheten som

kommunen får fra, for eksempel, HelseCERT. Kommunen har etter hva vi kjenner til ikke tatt initiativ til for eksempel inntrengningstester spesifikt rettet mot egne IKT-systemer de senere årene.

I kommunens sikkerhetsmål og sikkerhetsstrategi er det nedfelt et krav om at IKT-systemene skal være konfigurert til å logge forsøk på uautorisert tilgang. Vi har ikke opplysninger som tilsier at denne typen logger brukes aktivt i overvåkning av IKT-systemene utover at IKT-avdelingen har opplyst at de følger med på brannmurene med hensyn til forsøk på å omgå denne. De følger også med på e-poster med mistenkelig innhold, og tar tak i forhold som har med informasjonssikkerhet å gjøre når de oppstår.

Vi mener kommunen vil være tjent med å gjennomføre sikkerhetsovervåkning og testing mer planmessig enn i dag. En plan for dette kan ta utgangspunkt i en oversikt over hva eksterne samarbeidspartnere gjør av sikkerhetsovervåkning og testing, men det er også viktig at kommuneledelsen tar stilling til hva kommunen har behov for samlet sett, ut fra en vurdering av risiko.

Vi mener at revisjonskriterium 13 er delvis etterlevd.

Kommunen må gjennomføre planmessig sikkerhetsovervåkning og testing på området.

7.3.6 Planlegging for håndtering av uønskede hendelser

IKT-leder utgjør en del av krisestaben i kommunen, og er tett på med hensyn til det arbeidet som gjøres der. Det er videre utarbeidet egne retningslinjer for utarbeidelse av katastrofeberedskap og en egen prosedyre for planlegging av utilsiktede avbrudd – IKT som skal sikre at de ulike enheter/virksomheter planlegger for sine egne IKT-systemer. Beredskapsplanene skal i henhold til prosedyren, i tillegg til å beskrive alternativ drift, også beskrive gjenoppretting. Vi kan imidlertid ikke se at det i særlig grad er utarbeidet egne beredskapsplaner med bakgrunn i denne prosedyren eller retningslinjene for utarbeidelse av katastrofeberedskap, ute i de enkelte enheter/virksomheter. Vi kan heller ikke se at det øves spesielt på håndtering av uønskede hendelser og krisehåndtering.

Kommunen har imidlertid fått prøvd ut beredskapen i enkelte tilfeller ved strømbrudd eller at nettet har vært nede, og det rapporteres at beredskapen har fungert godt. Så vil det, som kommunedirektøren påpeker, komme strengere krav til kommunens beredskap slik at kommunen utvilsomt vil ha en jobb å gjøre på dette området.

Når det gjelder roller og ansvarsforhold i forbindelse med krisehåndtering, er det vår vurdering at dette er tilstrekkelig beskrevet i systembeskrivelsen for informasjonssikkerhet og i de rutiner som er utarbeidet. Kommunen har etter vår vurdering også tilfredsstillende rutiner for sikkerhetskopiering.

Vi mener at revisjonskriterium 14 er delvis etterlevd.

Det må planlegges hvordan uønskede hendelser skal behandles, hvordan systemer og nettverk kan gjenopprettes og det gjennomføres øvelser på området.

7.3.7 Sikkerhetsrevisjoner i helse og omsorg

Vi kan ikke se at det planlegges sikkerhetsrevisjoner knyttet til informasjonssikkerhet i helse- og omsorgssektoren slik «Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren» legger opp til. Vi kan heller ikke se at det gjøres kontroller på at etablerte sikkerhetstiltak og rutiner følges opp, eller at det gjøres spesielle evalueringer av disse.

Tilbakemeldingene, spesielt fra HelseCERT gir innspill til risikoområder som kommunen bør følge opp på generelt grunnlag, eller spesielt i forhold til Våler kommune. Fra intervjuer har vi fått opplyst at

dette blir gjort. Vi kan imidlertid ikke se at dette dokumenteres, noe som er et krav i henhold til den nevnte normen.

Vi mener at revisjonskriterium 15 ikke er etterlevd.

For helse- og omsorgstjenestene må det planlegges og gjennomføres sikkerhetsrevisjoner. Resultatene fra sikkerhetsrevisjonene må følges opp og dokumenteres.

7.3.8 Rutiner for rapportering og håndtering av avvik

Kommunens styringsdokumenter på IKT- området legger opp til at avviksmodulen i Compilo skal benyttes til rapportering av avvik. Denne strategien følges opp med egen prosedyre for avviksbehandling innen informasjonssikkerhet, som også angir hvem som er ansvarlig for å følge opp meldte avvik. Det er også opprettet en egen kategori for avvik knyttet til personvern i kommunens avvikssystem. Så har vi fra intervjuer fått opplyst at Compilo brukes lite til dette formålet, og at en heller tar direkte kontakt med nærmeste leder eller IKT-avdelingen. Vi antar at det ofte kan være slik at avvikene må tas tak i for at en skal komme videre i arbeidet og at direkte kontakt da er mest effektivt. At en har denne muligheten er derfor viktig. Vi mener likevel at avvikene bør registreres i kommunens avvikssystem slik at de kan systematiseres og benyttes til systematisk forbedringsarbeid. Avvik er en viktig kilde til slik arbeid, og vi kan ikke se at avvikene benyttes til systematisk forbedringsarbeid på IKT-området i dag.

I spørreundersøkelsen har vi kartlagt om de ansatte i kommunen oppfatter at avviksrapporteringen fungerer. Undersøkelsen viser at de ansatte ikke har særlig stor tiltro til at en kollega melder ifra dersom de gjør noe som utgjør enn sikkerhetsrisiko. Et flertall mener derimot at det er lett å si fra til en kollega dersom de selv ser at noen gjør noe som medfører risiko for informasjonssikkerheten. Det er viktig at de ansatte opplever at det er aksept for å si ifra når de oppdager brudd på informasjonssikkerheten, noe undersøkelsen tyder på at det er. Vi har også stilt de ansatte spørsmål knyttet til om de har fått opplæring i/blitt informert om hvordan de skal rapportere avvik. En stor andel av de ansatte sier de vet hvem de skal melde fra til dersom det oppstår en digital sikkerhetshendelse, og mange ville ha meldt fra til flere instanser. Undersøkelsen viser at de aller fleste ville ha meldt fra til nærmeste leder, til helpdesk (dvs. IKT-avdelingen) eller lignende, dersom de mottar en mistenkelig e-post, ser en kollega begå sikkerhetsbrudd, eller dersom de mistenker at de har fått virus eller lignende på kommunens datamaskiner.

Vi bemerker at det er en andel på 13 prosent som ikke vet hvem de skal melde fra til. Det er videre bare en liten andel som ville ha rapportert denne typen hendelser i avvikssystemet Compilo. Ut fra dette mener vi at det fortsatt er behov for å drive opplæring og å informere om rutinene knyttet til avvik.

Vi mener at revisjonskriterium 16 er delvis etterlevd.

Kommunen må ha klare rutiner for avviksrapportering og –håndtering.

8 Problemstilling 3 – Praktisering av informasjonssikkerhet

I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

8.1 Revisjonskriterier for problemstilling 3

Følgende er en tabell med de kriterier vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A. Tabellen er interaktiv og leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriteriet. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor. Vi gjør derfor leseren oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

	Kriterium 17	Kommunen må ha rutiner for bekjentgjøring, oppbevaring og ajourhold som sikrer at gjeldende planer, reglementer og rutiner knyttet til informasjonssikkerhet er kjent og tilgjengelig.
	Kriterium 18	Kommunen må ha rapporteringsrutiner som sikrer oppfølging og evaluering av planer, reglementer og rutiner knyttet til informasjonssikkerhet.
	Kriterium 19	Kommunen må sikre oversikt over kompetansebehovet og sørge for at den enkelte ansatte både får generell og tilpasset opplæring i hvordan informasjonssikkerheten kan ivaretas.
	Kriterium 20	Det bør planlegges hvordan kommunen skal sikre kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen.

8.2 Innhentet data

8.2.1 Data fra dokumenter

I **sikkerhetsmål og sikkerhetsstrategi for Våler kommune** fastslås at kommuneledelsen har ansvar for å kontrollere at rutinene for informasjonssikkerhet følges. Det heter også at det skal gjennomføres egenkontroll/måling av sikkerhetsnivå ved Våler kommune regelmessig i henhold til systematiserte rutiner.

I notat om **styringssystem for informasjonssikkerhet og personvern** finnes et eget avsnitt om ledelsens årlige gjennomgang av personvern og informasjonssikkerhet. Av forhold det er aktuelt å inkludere i en slik gjennomgang er:

- Endringer i eksterne krav innen informasjonssikkerhet og personvern.
- Orientering om risiko- og trusselbildet for personvern og informasjonssikkerhet.
- Gjennomgang av vesentlige og/eller alvorlige avviksaker i kommunen siden forrige ledelsens gjennomgang, herunder hvordan disse er håndtert og fulgt opp.
- Resultat fra risikovurderinger og personvernkonsekvensvurderinger.
- Gjennomgang av behandlingsaktivitetene (behandlingsprotokoll).
- Overordnet gjennomgang av endringer i risikovurderinger og tiltak som er innført.
- Gjennomgang av oppfølgingen av leverandører.

- Muligheter for forbedring av styringssystemene.

Dersom gjennomgangen avdekker at kommunens risikonivå ikke er akseptabelt skal det vedtas tiltaksplaner for dette, med tidsfrister og plassering av ansvar. Tiltaksplanene bør inngå i budsjettprosessen til kommunen. Det heter videre at alle systemeiere skal gjennomføre årlig egenrapportering av IKT-sikkerhet for sine IKT-systemer og etterlevelse av bestemmelsen i «Styringssystemet for informasjonssikkerhet og personvern».

IKT-avdelingen har en egen **prosedyre for personellopplæring - IKT** hvor formålet er å formidle den enkelte medarbeider sine plikter i forbindelse med forsvarlig sikring av personopplysninger og informasjon. Prosedyren gjelder ved nytilsettinger, stillingsendringer, endring i konfigurasjon eller offentlige krav. Aktivitetene kan knyttes til taushetsplikt, krav til kompetanse, sikkerhetsopplæring og personellforvaltning. Det heter at alle medarbeidere som er brukere av informasjonssystemene i kommunen skal gjennomgå opplæring og trening i informasjonssikkerhetsprosedyrer, i tillegg til nødvendig opplæring i eget fagsystem før de blir gitt tilgang til systemene. Det er den enkelte selv, enhetsleder og sikkerhetsleder som er ansvarlig for at opplæringen gjennomføres.

Ansattretningslinjer for informasjonssikkerhet og personvern beskriver hva den enkelte ansatte skal være kjent med når det gjelder informasjonssikkerhet og personvern. Dette inkludert roller og ansvarsfordeling, sikkerhetsmål og strategier, sikkerhetstiltak en selv er pålagt å følge og kommunens rutiner for avvikshåndtering. Dokumentet er nærmere beskrevet i datadelen til problemstilling 1.

I **årsrapport personvern 2022** rapporteres det kort om hva som er gjort i året som er gått med hensyn til nye rutiner, risikovurderinger, utarbeidelse av DPIA-personvernkonsekvenser, personvernerklæringer og opplærings/informasjonsarbeid. Videre er det kort redegjort for gjennomført veiledning, oppfølging av databehandleravtaler og behandlingsprotokoller. Det er opplyst om at det er gjennomført en årlig personvernundersøkelse overfor virksomhetslederne. Når det gjelder tanker om hva som bør gjøres i 2023 er følgende nevnt:

- Det bør kurses og veiledes i risikovurderinger slik at dette alltid gjennomføres før en ny behandling av personopplysninger går i gang.
- Det trengs flere ressurspersoner på utførelse av DPIA.
- En plan for opplæring i personvern og informasjonssikkerhet som sikrer at alle medarbeidere i kommunen får nødvendig opplæring.
- Et årshjul for internkontroll innen personvern.

Når det gjelder opplæring i personvern og informasjonssikkerhet er det foreslått å bruke nanolæringprogram [13] som også kan benyttes i forbindelse med onboarding av nye medarbeidere. I forbindelse med årshjul for internkontroll innen personvern er det presisert at dette bør samkjøres med kommunens internkontroll for øvrig og at ledelsens gjennomgang er et konsept som kan bidra til mer systematikk i arbeidet.

I **kvalitetssystemet Compilo** oppbevarer kommunen planer, reglementer og rutiner som gjelder samlet for hele kommunen eller for den enkelte virksomhet/enhet. Det legges inn tidsfrister for når det enkelte dokument skal gjennomgås og vurderes med hensyn til endringer. Vanligvis skal dette gjøres årlig. I forbindelse med gjennomføringen av forvaltningsrevisjonen har vi hatt tilgang til Compilo, og vi

[13] Nanolæring er en læringsmetode med fokus på repetisjon, refleksjon og forsterkning, gjennom mange, små leksjoner som hver for seg kan gjennomføres på kort tid.

har sett etter om dokumentene oppdateres når de skal. I forbindelse med vår gjennomgang har vi sett at det er ganske mange dokumenter hvor dato for revisjon er overskredet.

8.2.2 Data fra intervjuer

Fra **kommunedirektøren** har vi fått opplyst at de ansatte i kommunen har enkel tilgang til dokumenter som planer, reglementer og rutiner i Compilo. Regelen er at retningslinjer og rutiner som legges inn i systemet vurderes med hensyn til revisjon en gang i året. Det er likevel ikke sikkert at dette blir gjort. Overordnet oppfølging av Compilo har ellers vært tillagt HR-leder. Kommunen hadde da intervjuet ble gjennomført vært uten HR-leder en periode og kommunedirektøren mener man på grunn av dette er kommet noe på etterskudd både med innholdet i systemet og opplæring i bruken av systemet. Ny HR-leder kom på plass i april i 2023 og det er å anta at en vil komme à jour etter hvert.

Fravær av HR-leder har også hatt betydning for kartlegging og oversikt over kompetansebehovet for kommunen samlet. Det finnes ikke oppdaterte kompetanseplaner for kommunen, og ingen egen kompetanseplan for informasjonssikkerhet. Det blir likevel gjennomført opplæring, kurs og ulike kompetansehevende tiltak på IKT-området. Dette er mest aktuelt når det innføres nye systemer, men kan også være aktuelt i forbindelse med programvareoppdateringer. Kommunedirektøren ser ellers at det er behov for oppfriskningskurs på ulike IKT-systemer.

Dersom det oppstår uønskede hendelser eller ting som kan medføre risiko i tilknytning til IKT-systemene, skal disse rapporteres til nærmeste leder straks. Deretter må det tas stilling til om for eksempel IKT-avdelingen og/eller personvernombudet skal involveres. Det er kommunedirektøren sin oppfatning at de ansatte i kommunen har gode holdninger med hensyn til informasjonssikkerhet og bruk av IKT-systemene. IKT-avdelingen sender ut informasjons-e-poster med påminnelser om hvordan den enkelte skal forholde seg når det gjelder bruk av IKT-utstyr. Disse kan inneholde korte e-kurs/informasjonsvideoer. Det sendes også ut varsler dersom det er mye mistenkelige e-poster i omløp e.l. IKT-avdelingen har et årshjul som omhandler sin virksomhet gjennom året.

Når det gjelder behovet for kompetanse på IKT-området i tiden fremover, opplyser kommunedirektøren at dette vil endres som følge av at kommunen går inn i Indigo IKT IKS. Hva kommunen skal ha og hva Indigo IKT skal bidra med vil bli klarlagt utover høsten 2023. Når det gjelder de ansatte og ledelsen i kommunen, vil kompetansebehovet på IKT-området og kompetanse med hensyn til informasjonssikkerhet bli en del av en større plan. Det er som tidligere nevnt behov for opplæring i enkelte av kommunens IKT-systemer, men det er også viktig med mer planlagt oppfriskning på området.

Fra **IKT-leder** har vi fått opplyst at planer, reglementer og rutiner/prosedyrer ligger i kvalitetssystemet Compilo. Alle har tilgang og det er den enkelte tjeneste som har ansvar for å legge inn og vedlikeholde dokumenter i systemet. Hvor ofte systemet brukes vil nok variere mye, og det er ansatte i kommunen som bruker IKT-utstyr veldig sjelden i sin jobb. Når det innføres nye IKT-systemer eller gjøres endringer i disse vurderes behovet for opplæring. Ofte er det superbrukerne som står for opplæring/informasjon, men det kan også gå ut meldinger fra IKT-avdelingen om spesielle ting. Ellers finnes det nettkurs som kan brukes. Kommunen bruker e-kurs både til nytilsatte og til andre ansatte når det er behov for det. IKT-avdelingen gjennomfører for øvrig årlige nettkurs med hensyn til IKT-sikkerhet. Det er IKT-leder sitt inntrykk at dette bidrar til at kommunens ansatte blir mer oppmerksomme, og sier ifra dersom de ser noe mistenkelig. For eksempel når de får mistenkelige e-poster.

IKT-planer, reglementer og rutiner følges opp av ledelsen i tilknytning til andre ting som omhandler internkontroll. Når det gjelder kompetansebehovet finnes det ingen spesiell kompetanseplan for IKT og informasjonssikkerhet. IKT-avdelingen har ikke fått noe innspill fra enhetene med hensyn til kompetansebehov og IKT-leder mener at det må antas at disse enhetene da har den kompetansen de mener de har behov for. IKT-avdelingen får ellers de kurs og kompetansetiltakene de melder inn behov for. Ut fra størrelsen på kommunen og IKT-avdelingen er det ikke mulig å ha spisskompetanse i kommunen, og strategien er derfor å kjøpe dette fra eksterne. Generell IKT-kompetanse og bestiller-kompetanse er viktig å ha for kommunen.

Med bakgrunn i strategien om innkjøp av spisskompetanse, og det at kommunen har en målsetting om å gå over på skyløsninger for alle IKT-systemene, har gjort at IKT-avdelingen er redusert fra 3 til 2 ansatte. Skyløsninger fordrer i mindre grad driftspersonell i kommunen. Kommunen har ikke noe eget system for forbedringsarbeid i forbindelse med IKT-sikkerhet. Dette gjøres daglig når en ser (eller får innspill på) at det er ting som må tas tak i.

8.2.2.1 Data fra intervju med virksomhetsledere

I det følgende oppsummeres informasjon vi har fått i intervju med virksomhetslederne for tekniske tjenester og pleie- og omsorgstjenestene.

Virksomhetene viser til Compilo når det gjelder planer, reglementer og rutiner som gjelder i virksomheten. Fra pleie- og omsorgstjenesten har vi fått opplyst at det legges inn frister for ajourhold i dette systemet som en får en påminnelse om. Det opplyses imidlertid også å være krevende å få gjennomgått alt, og å ta stilling til eventuelle endringer innen fastsatte frister. Ingen av virksomhetene har faste rapporteringsrutiner når det gjelder IKT og/eller informasjonssikkerhet. Dette kan likevel være tema i planleggingsmøter på ulike nivå i kommunen.

Når det gjelder opplæring/kompetanseutvikling oppgir pleie og omsorgstjenesten at de har egen opplæringsplan for virksomheten, mens tekniske tjenester bruker medarbeidersamtalene som grunnlag for kompetanseplanlegging. Virksomhetene melder også inn opplæringsbehov til kommuneledelsen, blant annet behov for opplæring innen IKT og informasjonssikkerhet.

8.2.2.2 Data fra superbrukere for Visma profil og KOMTEK

Fra intervju med superbruker for KOMTEK har vi fått opplyst at de som bruker systemet har lang erfaring med det, og at det i sin tid ble gitt opplæring i bruk av systemet. Systemleverandøren avholder egne fagdager hvert år. Det er også utnevnt såkalte «nøtteknekkere» som er kommuneansatte med inngående kjennskap til KOMTEK, og som en kan få hjelp av dersom en har problemer. Det finnes ellers en lokal samlingsgruppe for KOMTEK med representanter fra Våler, Åsnes, Grue, Elverum og SØIR IKS som en kan støtte seg på. Superbruker har ingen spesiell rapportering i tilknytning til informasjonssikkerhet for KOMTEK.

Fra superbruker for Visma Profil har vi fått opplyst at det er avdelingene som står for opplæring av nye ansatte, eller opplæring i forbindelse med endringer i systemet. Superbrukerfunksjonen medfører ingen spesiell rapportering utover det å si fra, eksempelvis til avdelingslederne eller IKT-leder dersom det oppstår feil. Det som vanligvis fører til problemer i Visma Profil er brukerfeil eller at en ikke har nett-tilgang.

8.2.3 Data fra spørreundersøkelsen

Under denne problemstillingen presenterer vi resultatene fra spørsmål knyttet til kjennskap til strategi og interne regler knyttet til informasjonssikkerhet, sikkerhetsatferd samt opplæring på området.

Når det gjelder kjennskap til **strategi, regler og rutiner innen informasjonssikkerhet** har vi spurt om de ansatte opplever at kommunen har en tydelig strategi når det gjelder digital sikkerhet. På dette spørsmålet har de fleste, 78 %, svart at de i ganske stor grad eller svært stor grad er enige i dette. 18 % har svart verken/eller, og 4 % har svart at de i ganske liten grad er enige i dette. Det er ingen som har svart at de i svært liten grad opplever at kommunen har en tydelig strategi når det gjelder digital sikkerhet. Det var imidlertid bare en femtedel av de som har deltatt i undersøkelsen som svarte på dette spørsmålet. De ansatte har i spørreundersøkelsen blitt spurt om deres virksomhet har regler for informasjonssikkerhet. Her har 73 % svart ja, 2 % nei mens 25 % ikke vet om deres virksomhet har regler.

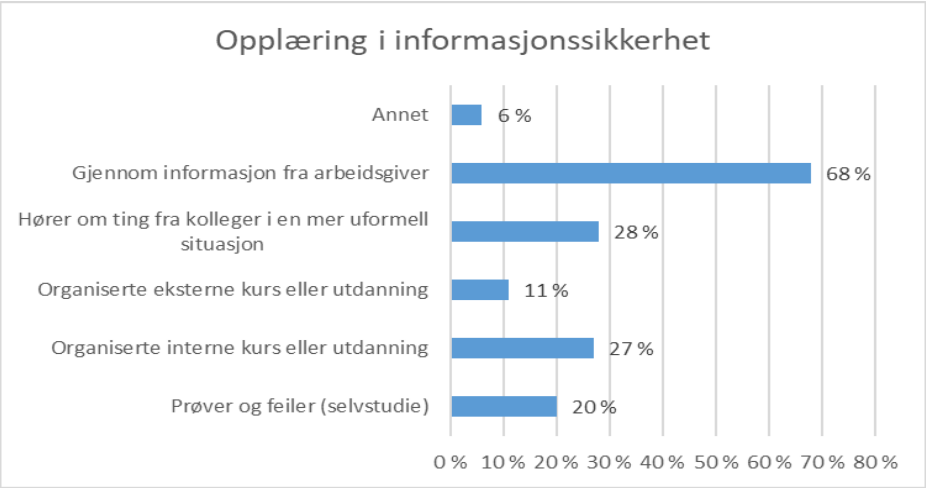
I undersøkelsen var det også **spørsmål rettet mer konkret mot atferd** når det gjelder bruk av digitale verktøy, og som kan si noe om hvordan de ansatte etterlever regler for informasjonssikkerhet. De ansatte er spurt om de undersøker om en nettside er sikker før de bruker den. Flest, 59 %, har svart at de gjør dette av og til, mens 31 % har svart at de alltid gjør dette. 7 % har svart at de aldri undersøker om nettsider er sikre før de bruker de, mens 3 % har svart at dette ikke er aktuelt for dem. Når det gjelder passordbruk, har 88 % svart at de ikke bruker samme passord hjemme og på jobb. 11 % bruker de samme passordene hjemme og på jobb, mens 1 % har svart at dette ikke er aktuelt for dem. På spørsmål om en benytter de samme passordene i flere av systemene på jobb svarte 60 % «nei» og 40 % «ja».

59 % låser alltid skjermen når de forlater datamaskinen sin, 34 % gjør det av og til mens det er 7 % som aldri gjør dette. 49 % oppgir at de alltid undersøker om lenker og vedlegg de mottar i e-post er sikre før de åpner dem. 41 % gjør dette av og til, mens 9 % aldri gjør det. Her er det 1 % som har svart at dette ikke er aktuelt for dem. Det er ellers ikke vanlig å poste/dele informasjon om arbeidet sitt i sosiale medier blant ansatte i Våler kommunen. 82 % har svart at dette gjøres i svært liten grad, 12 % har svart i ganske liten grad, mens 4 % har svart av og til. Det er 2 % som har svart at de poster/deler i ganske stor grad og ingen som har svart at de gjør dette i svært stor grad.

Når det gjelder **opplæring**, så er det 58 % av de ansatte som har svart at de har fått opplæring i informasjonssikkerhet, og da 42 % som oppgir at de ikke har fått dette. De som har bekreftet å ha fått opplæring har videre blitt spurt om hvem som tilbød opplæringen, og hvordan den ble gjennomført. Det var ca. halvparten av de som deltok i undersøkelsen som ga oss tilbakemelding på dette. De fleste har fått opplæring internt i kommunen ved hjelp av e-læringskurs. En god del sier de har fått intern opplæring, uten at det fremgår om dette er internt ved deres virksomhet eller for kommunen samlet. Noen få nevner ellers personvernombudet og at kommunen har en sikkerhetsmåned der det sendes ut mye informasjon og opplæringsmateriell.

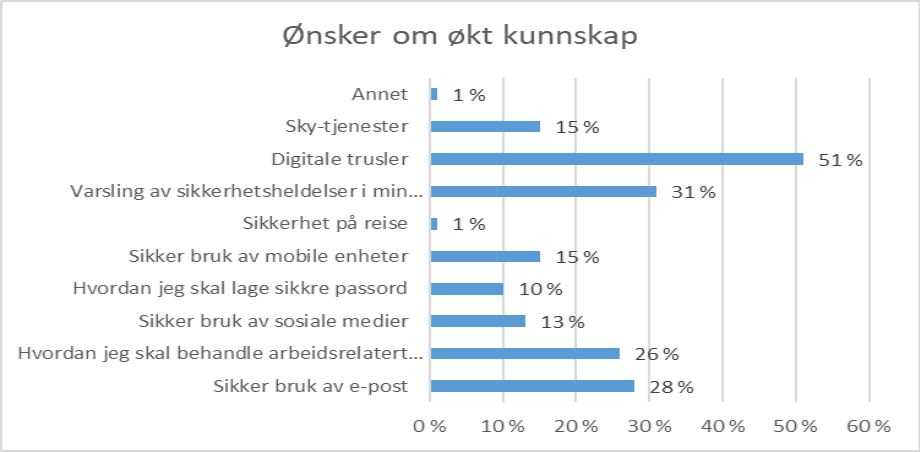
De som har svart at de har fått opplæring har også fått spørsmål om opplæringen var relatert til de arbeidsoppgavene den enkelte har. Her svarte 68 % at opplæringen i ganske eller svært stor grad var relatert til deres arbeidsoppgaver. 14 % har svart at opplæringen i ganske liten eller i svært liten grad var relatert til arbeidsoppgavene, mens de øvrige 18 % har svart verken/eller på dette spørsmålet. Det var ca. halvparten av det totale antallet deltakerne i spørreundersøkelsen som besvarte dette spørsmålet.

Vi har i spørreundersøkelsen spurt de ansatte om hvordan de vanligvis lærer om informasjonssikkerhet. Svarene fordelers seg slik:



Hver enkelt kunne krysse av for de to viktigste kategoriene på dette spørsmålet.

På spørsmål om det er ønske om mer kunnskap om informasjonssikkerhet på jobb har 79 % svart «ja» og 21% har svart «nei». De alle fleste av de som ønsker mer kunnskap om informasjonssikkerhet på jobb har videre spesifisert hva de ønsker mer kunnskap om. Svarene kan illustreres i følgende tabell:



Også her har den enkelte kunnet krysse av for de to viktigste kategoriene, og det var ca. tre fjerdedeler av deltakerne i undersøkelsen som svarte på dette spørsmålet.

8.3 Revisors vurdering

8.3.1 Rutiner for bekjentgjøring av planer, reglementer og rutiner på området

Kommunens planer, reglementer og rutiner oppbevares i kvalitetssystemet Compilo. Vi har fått opplyst at alle ansatte skal ha tilgang til dette systemet. Vi vet at det er en del ansatte i kommunen som sjelden eller aldri er inne i kommunens IKT-systemer, men muligheten skal likevel finnes. Vi har forstått det slik at det jevnlig må tas stilling til om dokumentene må endres, og at de ansvarlige får automatisk beskjed om dette fra Compilo. Vanligvis skal rutiner vurderes med hensyn til revisjon minst en gang i året. Vi har i forbindelse med at vi har hatt tilgang til Compilo sett at det er ganske mange dokumenter som ikke er revidert når de skal.

Kommunen har i forbindelse med ansettelser et ansattreglement hvor mange forhold knyttet til informasjonssikkerhet gjennomgås. Vi har ikke inntrykk av at kommunen har spesielle rutiner for å bekjentgjøre endringer i planer, reglementer eller rutiner utover at dette kan tas opp i ulike møter. Vi mener det er behov for en fast rutine for hvordan dette gjøres slik at en sikrer at alle ansatte får informasjon. Det kan også være hensiktsmessig å planlegge oppfriskning av kunnskapen på området. IKT-avdelingen informerer og kurser de ansatte om IKT-sikkerhet, blant annet ut fra sikkerhetstips fra eksterne samarbeidspartnere. I spørreundersøkelsen til de ansatte har vi stilt spørsmål om de opplever at kommunen har en tydelig strategi når det gjelder digital sikkerhet. De fleste som har svart på dette spørsmålet mener at kommunen har en tydelig strategi, men ettersom det bare er en femtedel av deltakerne i undersøkelsen som har svart på spørsmålet, mener vi det kan stilles spørsmålstegn ved om kommunens strategi er kjent. Når det gjelder spørsmål om virksomheten de jobber ved har regler for informasjonssikkerhet, så har flertallet svart bekreftende på dette. Det er likevel en fjerdedel av de ansatte som ikke vet om det finnes regler. Ut fra dette mener vi at kommunen bør ha større fokus på å bekjentgjøre planer/strategi og rutiner for informasjonssikkerhet. Vi mener kommunen bør innføre faste rutiner for oppfriskning og informasjon om endringer i planer, reglementer og rutiner.

I spørreundersøkelsen til de ansatte i kommunen finnes det også spørsmål knyttet til atferd når det gjelder bruk av passord, orden på arbeidsplassen og sikkerhet rundt e-post. Dette er områder hvor kommunen har stilt krav til de ansatte. Resultatene viser at de fleste bruker forskjellige passord hjemme og på jobb. Vi merker oss likevel at det er ca. 10 % som ikke bruker forskjellige passord. Det er også langt mer vanlig å bruke de samme passordene på flere av IKT-systemene på jobb, selv om de fleste også her bruker forskjellige passord. Hele 40 % oppgir å ikke være så nøye med om de går fra en ulåst datamaskin, og det er bare halvparten av de ansatte som alltid undersøker at lenker og vedlegg de mottar i e-post er sikre før de åpner dem. Andre resultater fra undersøkelsen er at de fleste undersøker om nettsider er sikre før de tar de i bruk, og at det bare er en liten andel av de ansatte i kommunen som poster/deler informasjon om arbeidet sitt i sosiale medier. Det er etter vår vurdering enkelte avvik mellom kommunens krav til informasjonssikkerhet og hvordan det praktiseres.

Vi mener at revisjonskriterium 17 er delvis etterlevd.

Kommunen må ha rutiner for bekjentgjøring, oppbevaring og ajourhold som sikrer at gjeldende planer, reglementer og rutiner knyttet til informasjonssikkerhet er kjent og tilgjengelig.

8.3.2 Rapporteringsrutiner for informasjonssikkerhet

Vi har tidligere kommentert at kommunen i tilknytning til planer for styringssystem for informasjonssikkerhet og personvern mener å innføre at kommuneledelsen har en gjennomgang av området årlig. En gjennomgang som beskrevet i notat om «Styringssystem for informasjonssikkerhet og personvern» vil gi kommuneledelsen et godt grunnlag for å planlegge utviklingen på området. En slik gjennomgang er imidlertid avhengig av at det rapporteres fra kommunens enheter/virksomhet i større grad enn hva som gjøres i dag. I det planlagte styringssystemet vil enhetslederne ha en nøkkelrolle med hensyn til å sørge for at det gjennomføres risikovurderinger på området og egenkontroller der resultatene skal vurderes og danne grunnlag for sikkerhetstiltak. Enhetslederne skal også gjennomgå og eventuelt revidere rutiner o.l. som legges inn i kvalitetssystemet Compilo. Etterlevelsen av dette fremsto i undersøkelsen som variabelt. Det som gjøres på enhets-/virksomhetsnivå er informasjon som er relevant for kommuneledelsen å ha tilgang til i forbindelse med deres gjennomgang. Rapportering for informasjonssikkerhet kan både gjøres separat eller i

tilknytning til annen type rapportering. Vi forstår det imidlertid slik at kommunen planlegger å ha egen rapportering spesielt for informasjonssikkerhet.

Oppsummering av avvik som er meldt/håndtert er også en kilde for evaluering. Her vil kommunen være avhengig av at avvikene for informasjonssikkerhet også registreres i avvikssystemet i Compilo, noe som i liten grad skjer i dag. Etter hva vi har fått opplyst kan status for informasjonssikkerhet være tema i møter på ulike nivå i kommunen. IKT-leder informerer også om status for arbeidet i sin avdeling til kommuneledelsen og oppfølging og evaluering av planer, reglementer og rutiner kan være tema i denne forbindelse. Vi merker oss også at personvernombudet utarbeider en årsrapport for sitt arbeid som kan ha nytteverdi i forhold til arbeidet med informasjonssikkerhet i kommunen.

Vi vurderer likevel at rapporteringsrutinene, foreløpig bærer preg av å være tilfeldige og ustrukturert.

Vi mener at revisjonskriterium 18 ikke er etterlevd.

Kommunen må ha rapporteringsrutiner som sikrer oppfølging og evaluering av planer, reglementer og rutiner knyttet til informasjonssikkerhet.

8.3.3 Oversikt over kompetansebehovet/ generell og tilpasset opplæring

Fra ledelsen i kommunen har vi fått innspill på at det er behov for opplæring i enkelte av kommunens IKT-systemer, men også mer planlagt oppfriskning i bruk av ulike systemer. Enhetene/virksomhetene melder inn behov for opplæringstiltak til kommuneledelsen, og pleie- og omsorgstjenestene har egen opplæringsplan. Det fantes ingen egen oppdatert opplæringsplan for kommunen samlet da vi gjennomføre denne forvaltningsrevisjonen, men det var planlagt å starte et slik arbeid. Vi oppfatter videre at superbrukere, brukergrupper og andre typer samarbeid for de ulike IKT-systemene kan være nyttige med hensyn til opplæring i systemene og problemløsing. IKT-avdelingen oppdaterer videre de ansatte i kommunen på informasjonssikkerhet ved å sende ut e-postmeldinger og lenker til e-kurs etc. Ledere i kommunen får årlig en egen gjennomgang/kartlegging når det gjelder informasjonssikkerhet og personvern. Oppdatering/opplæring fra IKT-avdelingen er etter hva vi har forstått basert på tips og råd fra eksterne samarbeidspartnere, og i liten grad etter innspill fra interne. Vi mener det av og til kan være hensiktsmessig å gjennomføre mer systematiske kartlegginger av opplæringsbehovet. I forbindelse med spørreundersøkelsen til de ansatte har vi derfor også hatt med en del spørsmål som går på opplæring.

Resultatene fra undersøkelsen viser at det er et lite flertall som oppgir å ha fått opplæring i informasjonssikkerhet. Det er likevel hele 42 % som ikke har fått dette. De fleste som har oppgitt hvor de har fått opplæring fra, har vist til intern opplæring i kommunen. Med hensyn til om de ansatte har fått opplæring som er relatert til deres arbeidsoppgaver, har ca. to tredjedeler bekreftet at opplæringen var relatert til arbeidsoppgavene deres. Vi mener det bør være en målsetting at alle ansatte får opplæring innen informasjonssikkerhet som oppleves relevant i forhold til den enkelte sine arbeidsoppgaver. Kommunen har med andre ord fortsatt noe å gå på her. Generelt er det informasjon fra arbeidsgiver som er den viktigste kilden til økt kunnskap om informasjonssikkerhet, selv om en også får opplæring ved tips fra kolleger eller gjennom interne opplæringstiltak i kommunen. Et flertall ønsker mer kunnskap om informasjonssikkerhet, og det er kunnskap om digitale trusler de fleste ønsker mer kunnskap om. Vi mener resultatene fra spørreundersøkelsen viser at kommunen bør fokusere mer på opplæring innen informasjonssikkerhet, og å tilpasse opplæringen slik at den er relevant til den enkelte sine arbeidsoppgaver.

Vi mener at revisjonskriterium 19 er delvis etterlevd.

Kommunen må sikre oversikt over kompetansebehovet og sørge for at den enkelte ansatte både får generell og tilpasset opplæring i hvordan informasjonssikkerheten kan ivaretas.

8.3.4 Kompetanseplanlegging

Våler kommune har ingen egen kompetanseplan for informasjonssikkerhet. Kommunen har heller ingen overordnet kompetanseplan for kommunen samlet. Vi har likevel forstått det slik at en er i ferd med å utarbeide en slik plan. Vi har også fått opplyst at enheter/virksomheter i kommunen kan ha egne kompetanseplaner for sin virksomhet, eller planlegger kompetanseutvikling for sin virksomhet på annen måte. Noe av utfordringen med at en ikke har en overordnet kompetanseplan vil være at planleggingen på enhets-/virksomhetsnivå fort kan bli mindre målrettet. Vi mener kompetanseplanlegging med hensyn til informasjonssikkerhet med fordel kan inkluderes i øvrige kompetanseplaner. Det er imidlertid viktig at kompetanseplanene samlet sikrer kompetansebehovet både for nøkkelpersonell innen IKT, ansatte generelt og kommunens ledelse.

Kommunen har en strategi om å kjøpe spesialkompetanse, ettersom fagmiljøet i kommunen på IKT er lite. I tillegg har en knyttet til seg en del samarbeidspartnere som utfører oppgaver med sikring av IKT-systemene. Dette ved at kommunen benytter spesielle IKT-systemer som Visma Profil som testes med hensyn til sikkerhet av HelseCERT, eller at en har knyttet til seg fagmiljøer gjennom for eksempel KommuneCSIRT. Kommunen er videre i ferd med å gå inn i Indigo IKT IKS. Vi mener at måten den eksterne kompetansen skal benyttes på, også bør inkluderes i kommunens kompetanseplaner.

Kommunen har etter hva vi kan se ikke noe eget system for forbedringsarbeid på området. Et slikt system vil være nært knyttet til internkontrollsystemet for øvrig og innebære læring og utvikling med basis i for eksempel risikovurderinger, registrerte avvik og endringer i kravene til informasjonssikkerhet. Også her vil det være hensiktsmessig å knytte informasjonssikkerhet til systematisk forbedringsarbeid for tjenestene for øvrig. I helse- og omsorgstjenestene er det et forskriftskrav at virksomheten driver med systematisk forbedringsarbeid. Systematisk forbedringsarbeid er imidlertid også en av intensjonene i bestemmelsene om internkontroll i kommuneloven, og er således gjeldende for all kommunal virksomhet.

Vi mener at revisjonskriterium 20 er delvis etterlevd.

Det bør planlegges hvordan kommunen skal sikre kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen

9 Konklusjon

Vi har gjennom denne forvaltningsrevisjonen sett etter om Våler kommune tilfredsstiller sentrale lovkrav og anbefalinger for informasjonssikkerhet. En generell konklusjon er at kommunen har igangsatt en del viktig utviklingsarbeid når det gjelder planlegging, retningslinjer og rutiner for å ivareta informasjonssikkerheten i kommunen. Kommunen har også på plass en god del av sikkerhetstiltakene som er anbefalt for kommunene for å sikre seg mot dataangrep og uautorisert tilgang til informasjon. Når det gjelder systemer som sikrer at planer, rutiner og sikkerhetstiltak følges opp rundt om i enhetene/virksomhetene og av den enkelte ansatte, mener vi at kommunen har en vei å gå.

I tilknytning til de risiko-områdene som kontrollutvalget var opptatt av i forbindelse med bestillingen av denne forvaltningsrevisjonen kan vi ikke se at ledere er underlagt andre sikkerhetsbestemmelser enn andre ansatte i kommunen. De følges likevel spesielt opp med hensyn til opplæring/informasjon og kartlegging av kunnskap. Når det gjelder hjemmekontor dekkes sikkerheten gjennom opprettede rutiner som de ansatte skal forholde seg til, og de tekniske løsningene er opplyst å være sikkerhetstilpasset for slike løsninger.

I det følgende presenteres konklusjoner for den enkelte problemstilling.

Planer, retningslinjer og rutiner som kan ivareta informasjonssikkerheten

Det er i noen grad etablert helhetlige planer og styringsdokumenter som skal ivareta helheten, og retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte. Vi mener likevel at det er rom for forbedring både når det gjelder planlegging og internkontroll. Dette basert på følgende:

- Våler kommune har overordnede styringsdokumenter som beskriver sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerheten i kommunen. E-strategi for Våler kommune er utarbeidet for perioden 2018-2021 og dagens situasjon krever at strategien oppdateres. Vi har inntrykk av at informasjonssikkerhet rundt om i kommunen i stor grad er noe som fortrinnsvis overlates til IKT-avdelingen. Av den grunn mener vi at kommunen vil være tjent med å ha større fokus på mål og strategi for informasjonssikkerhet gjennom informasjon/opplæring, involvering og rapportering.
- Når det gjelder internkontroll for informasjonssikkerhet er det lagt planer for et styringssystem som er basert på anbefalinger fra KS og sentrale myndigheter. Deler av styringssystemet er operativt, men det er også sentrale deler som ikke er iverksatt ennå. Kommunen har utarbeidet rutiner for informasjonssikkerhet som både skal sikre konfidensialitet, integritet og tilgjengelighet i IKT-systemene. Det er likevel viktig å få på plass systematiske risikovurderinger og utarbeidelse av tiltaksplaner der risikoen er høy, kontroll og rapportering i tilknytning til oppfølging av internkontrolltiltakene, og jevnlige gjennomganger på området fra ledelsens side. Internkontrollsystemet for informasjonssikkerhet bør ellers integreres i et helhetlig internkontrollsystem for kommunen.
- Et godt internkontrollsystem for informasjonssikkerhet krever også at det det er klarlagt hva som kan aksepteres av risiko på området. Det planlagte styringssystemet for informasjonssikkerhet beskriver hvordan informasjon i IKT-systemene skal klassifiseres. Planen er at risiko skal vurderes for det enkelte IKT-system i henhold til klassifiseringen og at det skal utarbeides handlingsplaner der risikoen er for høy. Dette arbeidet er igangsatt, men det gjenstår en god del kartleggingsarbeid

her før en kan si at kommunen er i mål. I spørreundersøkelsen til de ansatte i kommunen er manglende opplæring og informasjon, virus som spres via e-post og risiko for å gjøre feil i en stressende og hektisk hverdag, oppgitt som de største utfordringene knyttet til informasjonssikkerhet.

- Ledelsen i kommunen har ingen fast rutine for gjennomgang av aktivitetene innen informasjonssikkerhet i dag. Det som er anbefalt er en årlig gjennomgang, og vi mener at det er hensiktsmessig at ledelsens gjennomgang dokumenteres. Innen helse- og omsorgstjenestene er det et normkrav om at ledelsens årlige gjennomgang av aktiviteten innen informasjonssikkerhet og personvern dokumenteres. For at en slik gjennomgang skal være hensiktsmessig må imidlertid kommunen få på plass et system for vurdering og rapportering av status ute i kommunens enheter/virksomheter. Det finnes planer i kommunen, både for egenvurdering og rapportering fra enheter/virksomheter og en årlig ledelsens gjennomgang. Dette er imidlertid ikke iverksatt.

Implementerte sikkerhetstiltak mot dataangrep og uautorisert tilgang

Kommunen har stort sett implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang. Vi mener likevel kommunen har et forbedringspotensial knyttet til systematiske risikovurderinger, planmessig gjennomgang av IKT-systemene og rapportering i tilknytning til informasjonssikkerhet. Dette basert på at:

- Vi kan ikke se at det gjennomføres systematiske risikovurderinger når det gjelder informasjonssikkerhet i kommunen. Kommunens enheter/virksomheter henviser i stor grad til IKT-avdelingen når det gjelder informasjonssikkerhet. Vi mener at en viktig del av risikovurderingene med hensyn til informasjonssikkerhet må foregå ute i enhetene/virksomhetene ettersom organisering av virksomheten, internkontroll og holdninger er like viktige som de tekniske sikkerhetstiltakene. Det er heller ikke tatt stilling til hva som kan aksepteres av risiko i kommunen. Resultatene fra spørreundersøkelsen til de ansatte viser også at risiko knyttet til informasjonssikkerhet er et tema som bør vies mer oppmerksomhet i kommunens enheter/virksomheter. Kommunen har likevel et godt grunnlag til å få på plass systematiske risikovurderinger og en beskrivelse av risikoaksept, ettersom det allerede er utarbeidet rutiner for risikovurderinger, forslag til kategorisering av verdien av informasjonen i IKT-systemene og beskrivelse av hvordan risiko skal håndteres.
- IKT-avdelingen har etter vår vurdering tilfredsstillende oversikt over den interne infrastrukturen for IKT, enheter, programvare og sikkerhet rundt dette. For å sikre at kommuneledelsen samlet får tilstrekkelig oversikt mener vi imidlertid at arbeidet med informasjonssikkerhet bør gjennomføres mer planmessig og strukturert, og at kommuneledelsen jevnlig bør ha en gjennomgang av status.
- Selv om IKT-avdelingen i noen grad gjennomgår risiko for de ulike deler av IKT-området mener vi at gjennomgangen ikke er planmessig slik Nasjonal sikkerhetsmyndighet anbefaler. Gjennomgang og vurdering av risiko blir noe tilfeldig og dette øker risikoen for at faresignaler kan bli oversett. Kommunen har heller ingen egen plan for sikkerhetsovervåkning og testing på området, og her baserer kommunen seg i stor grad på eksterne samarbeidspartnere. Vi mener kommunen bør gjennomføre sikkerhetsovervåkning og testing av IKT-systemene mer planmessig enn i dag, og at planleggingen baseres på vurdering av risiko.
- Når det gjelder planlegging for håndtering av uønskede hendelser har kommunen egne retningslinjer for utarbeidelse av katastrofeberedskap og en egen prosedyre for planlegging av

utilsiktede avbrudd – IKT som skal sikre at de ulike enheter/virksomheter planlegger for sine egne IKT-systemer. Vi kan imidlertid ikke se at dette følges opp med lokale beredskapsplaner ute i enhetene/virksomhetene. Det er ikke oss bekjent at det øves spesielt på håndtering av uønskede hendelser og krisehåndtering i tilknytning til informasjonssikkerhet. Beredskapen er imidlertid utprøvd i forbindelse med strømbrudd og at nettet har vært nede, og beredskapen rapporteres å ha fungert godt. Det er forventet at kommunene får strengere krav å forholde seg til når det gjelder beredskap og krisehåndtering, og beredskapen på IKT-området må tilpasses disse kravene.

- Vi kan ikke se at det planlegges og gjennomføres sikkerhetsrevisjoner for informasjonssikkerhet i helse- og omsorgssektoren, og at dette dokumenteres slik «Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren» legger opp til.
- Kommunens styringsdokumenter på IKT-området og rutiner legger opp til at avvik skal rapporteres i avviksmodulen i Compilo. I denne avviksmodulen er det også opprettet egen kategori for avvik tilknyttet personvern. Avviksmodulen brukes imidlertid lite. Resultatene fra spørreundersøkelsen viser også at denne måten å melde avvik på ikke er særlig kjent. Vi erkjenner imidlertid at avvik det haster med å få meldt fra om, med fordel kan meldes direkte til nærmeste leder eller IKT-avdelingen slik praksis er i dag. Det er likevel viktig at Compilo benyttes til å registrere avvikene, ettersom dette er en forutsetning for å kunne systematisere avvikene og benytte kunnskapen dette gir i forbedringsarbeidet i kommunen.

Oppfølging av planer, rutiner og sikkerhetstiltak

Kommunen har forbedringspotensial med hensyn til systematisk oppfølging når det gjelder planer, rutiner og sikkerhetstiltak. Slik systematikk er viktig for å sikre at planer, rutiner og sikkerhetstiltak følges opp i kommunens enheter og av den enkelte ansatte. Konklusjonen er basert på at:

- Kommunen har rutiner for å sikre at nytilsatte kjenner til de krav kommunen stiller til sine ansatte når det gjelder informasjonssikkerhet. Planer og reglementer/rutiner oppbevares i kvalitetssystemet Compilo og rutinen er at dokumentene skal vurderes med hensyn til revisjon minst en gang i året. Det varierer imidlertid hvordan rutinen for ajourhold etterleves. Kommunen har heller ingen fast rutine for å bekjentgjøre endringer i planer, rutiner etc. til de som allerede er ansatt i kommunen, eller en plan for oppfriskning av kunnskap om informasjonssikkerhet. Ut fra resultatene fra spørreundersøkelsen til de ansatte, kan det stilles spørsmålstegn ved hvor godt kjent kommunens strategi for informasjonssikkerhet er. En fjerdedel av de ansatte kjenner ikke til at kommunen har regler for informasjonssikkerhet, og vi mener det er en litt for stor andel av de ansatte som ikke etterlever sentrale regler for informasjonssikkerhet, for eksempel når det gjelder det å gå fra en ulåst datamaskin eller undersøke om lenker og vedlegg i e-poster er sikre før de åpnes.
- Vi kan ikke se at kommunen har rapporteringsrutiner som sikrer oppfølging og evaluering av planer, reglementer og rutiner knyttet til informasjonssikkerhet. Det foreligger imidlertid planer om å innføre at kommuneledelsen har en årlig gjennomgang av området. Det er også planlagt årlige egenkontroller ute i enhetene/virksomhetene. I tillegg til egenkontrollgjennomganger ute i enhetene/virksomhetene, vil kvaliteten på kommuneledelsens gjennomgang blant annet være avhengig av at kommunen får på plass gode rutiner og rapportering knyttet til risikovurderinger og registrering av avvik.

- Kommuneledelsen skaffer seg i noen grad oversikt over kompetansebehovet i organisasjonen ved at enhetene/virksomhetene melder inn behov. Noen melder også inn behov for opplæring og oppfriskning på ulike IKT-systemer. Det mottas imidlertid sjelden innspill som gjelder behov for opplæring innen informasjonssikkerhet, og IKT-avdelingen gir derfor de ansatte opplæring/informasjon som i stor grad er basert på tips og råd fra eksterne samarbeidspartnere. Spørreundersøkelsen blant de ansatte viser at det er en ganske stor andel som oppgir å ikke ha fått opplæring i informasjonssikkerhet. Av de som har fått opplæring oppgir imidlertid en stor andel at opplæringen var relatert til deres arbeidsoppgaver og at den viktigste kilden til opplæring/informasjon er arbeidsgiver. Vi mener kommunen vil være tjent med å gjennomføre mer systematiske kartlegginger av opplæringsbehovet der en spør de ansatte direkte hva de har behov for.
- Det finnes ingen overordnede kommunale kompetanseplaner i Våler kommune eller noen egen kompetanseplan knyttet til informasjonssikkerhet. Vi har imidlertid fått opplyst at det skal igangsettes arbeid med en overordnet kompetanseplan. Vi mener at kompetanseplanlegging på IKT-området og for informasjonssikkerhet gjerne kan inkluderes i kommunens øvrige kompetanseplaner. Det er imidlertid viktig at kompetanseplanene samlet fanger opp kompetansebehovet både for nøkkelpersonell innen IKT, ansatte generelt og kommunens ledelse, samt beskriver hvordan ekstern kompetanse skal benyttes. Vi mener også at IKT og informasjonssikkerhet bør inkluderes i kommunens system for forbedringsarbeid.

10 Anbefalinger

Ut fra de vurderinger og konklusjoner som er gjort gir vi kommunen anbefalinger om hvordan informasjonssikkerheten kan bedres. Anbefalingene kan fordeles på de ulike problemstillingene:

Når det gjelder å etablere planer, retningslinjer og rutiner som kan ivareta informasjonssikkerheten anbefaler vi kommunen å:

1. Oppdatere E-strategi for Våler kommune.
2. Vurdere hvordan det generelt kan sikres større fokus på mål og strategi for informasjonssikkerhet i hele kommunens organisasjon. Både gjennom informasjon og opplæring, involvering og rapportering.
    - Få på plass et internkontrollsystem for informasjonssikkerhet som også omfatter:
    - Systematiske risikovurderinger.
    - Oppfølging og kontroll av at målsettinger på området og internkontrolltiltakene etterleves, samt statusrapporteringer i tilknytning til dette.
    - Systematisk forbedringsarbeid.
    - Årlige gjennomganger på området fra ledelsens side, som dokumenteres.
3. Fullføre kartleggingen av risiko i kommunens IKT-systemer og at en i den forbindelse i større grad tydeliggjøre hva som er akseptabel/uakseptabel risiko. Videre at det utarbeides handlingsplaner som beskriver hvordan risikoen skal reduseres til et akseptabelt nivå.

I tilknytning til oppfølging av anbefalte sikkerhetstiltak anbefaler vi kommunen å:

4. Gjennomføre sikkerhetsgjennomganger, sikkerhetsovervåkning og testing av IKT-systemene mer planmessig, og at planleggingen baseres på vurdering av risiko.

5. Sikre at kommunens interne retningslinjer for beredskap innen informasjonssikkerhet etterleves, og at en vurderer hvordan informasjonssikkerhet kan inkluderes i beredskapsøvelser.
6. Planlegge, gjennomføre, følge opp og dokumentere sikkerhetsrevisjoner for informasjonssikkerhet i helse- og omsorgstjenestene slik det er anbefalt.
7. Sikre opplæring i, og informerer om rutinene knyttet til avviksrapportering.

For å sikre oppfølging av planer, rutiner og sikkerhetstiltak anbefaler vi kommunen å:

8. Innføre faste rutiner for hvordan kommunens ansatte skal informeres om endringer i planer, reglementer og rutiner. Det bør også innføres rutiner for å oppfriske de ansattes kjennskap til disse dokumentene.
9. Innskjerpe etterlevelse av rutinene for oppdatering av planer, reglementer og rutiner i Compilo.
10. Satse mer på opplæring innen informasjonssikkerhet, og å tilpasse opplæringen slik at den er relevant til den enkelte sine arbeidsoppgaver. Det vil i denne forbindelse være hensiktsmessig å gjennomføre mer systematiske kartlegginger av opplæringsbehovet i kommunen.
11. Utarbeide planer for hvordan kommunen skal sikre kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen. Planene kan med fordel knyttes til kommunens øvrige kompetanseplanlegging og system for forbedringsarbeid.

11 Kommunedirektørens uttalelse

Følgende e-post er mottatt fra kommunedirektøren 17.12.2023:

Jeg har gjennomgått rapporten og har ingen kommentarer til funn og konklusjon. På enkelte områder gjennomføres sikkerhetsprosedyrer i praksis, men det er mangler i å beskrive rutinene.
Når det gjelder anbefalinger vil administrasjonen igangsette arbeidet med forbedringer.

Våler kommune avventer samtidig på at Indigo (Hedmark IKT) skal vedta utvidelse med Våler og Åsnes. Når kommunen innlemmes i Indigo vil en del av anbefalingene bli i tråd med retningslinjer gitt av Indigo.

Med hilsen
Anniken Baksjøberget
Kommunedirektør
Tlf. 99254809

VÅLER 1000 ÅR

Våler kommune
- ett gir ekstra

12 Referanser

Datatilsynet (2019). *Virksomhetens plikter innen informasjonssikkerhet og internkontroll: Risikovurdering*

Direktoratet for e-helse (2021). *Normen for informasjonssikkerhet og personvern i helsesektoren*

E-forvaltningsforskriften (2020). *Forskrift om elektronisk kommunikasjon med og i forvaltningen*

Kommuneloven (2018). *Lov om kommuner og fylkeskommuner*

Kommunenes sentralforbund (2020). *«Orden i eget hus: Kommunedirekteørens internkontroll»*

Kommunenes sentralforbund (2022). *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet, Utarbeidet av KPMG for kommunenes sentralforbund.*

Nasjonal sikkerhetsmyndighet (2020). *NSMs grunnprinsipper for IT-sikkerhet*

12.1 Interne dokumenter – Våler kommune

Våler kommune (2016) – Veileder for anskaffelser

E-strategi for Våler kommune 2018-2021

Styringssystem for informasjonssikkerhet og personvern (2023)

Personvernombudet i Våler kommune – årsrapport 2022

HelseCERT – Tilbakeblikk for Våler kommune Hedmark for 2022

Dokumenter hentet fra kvalitetssystemet Compilo mai/juni 2023:

- Sikkerhetsmål og sikkerhetsstrategi for Våler kommune
- Ansattretningslinjer for informasjonssikkerhet og personvern
- Retningslinjer for utarbeidelse av katastrofeberedskap
- Prosedyre for planlegging av utilsiktet avbrudd – IKT
- Prosedyre for avviksbehandling innen informasjonssikkerhet
- Rutine for risikovurderinger knyttet til personopplysninger
- Rutiner for personellopplæring - IKT

12.2 Internettreferanser

Digitaliseringsdirektoratet. *Veileder i kompetanse og kulturutvikling innen digital sikkerhet*

Digitaliseringsdirektoratet. *Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet*

Digitaliseringsdirektoratet. *Styring av informasjonssikkerhet: Gjennomføre en risikovurdering*

Vedlegg A: Utledning av revisjonskriterier

I det følgende utledes kriteriene som er planlagt benyttet i forvaltningsrevisjonsprosjektet. Utledningen er en gjennomgang og drøfting av hva krav og anbefalinger har å si for forventningene til praksis.

Det er i forbindelse med utledningen av revisjonskriteriene tatt hensyn til at det planlegges å gjøre kontroller rettet mot systemer knyttet til kommunens helse- og omsorgstjenester.

Utledning av revisjonskriterier for problemstilling 1

Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte?

Denne problemstillingen søker å besvare om det foreligger og er etablert planer og rutiner som kan ivareta informasjonssikkerheten på en måte som sikrer kommunen ut i fra deres behov.

Generelt om informasjonssikkerhet og presentasjon av nasjonale faglige retningslinjer

Informasjonssikkerhet (også omtalt som digital sikkerhet og datasikkerhet) handler om tilstrekkelig sikring av en virksomhets informasjon og informasjonssystemer. Dette inkluderer digitale tjenester, IKT-systemer og komponenter som inngår i IKT-systemene. Det handler om å tilrettelegge arbeidsoppgaver (prosesser) slik at det er enkelt for mennesker å utføre oppgavene sine med sikkerhet i høysetet, samt å sikre tilstrekkelig kompetanse hos de som utfører oppgaver for virksomheten. I tillegg handler det om å jobbe for en kultur som understøtter arbeidet med informasjonssikkerhet. I følge Digitaliseringsdirektoratet handler informasjonssikkerhet om å sikre *konfidensialitet*, *integritet* og *tilgjengelighet*:

> «Det er vanlig å si at det handler om å sikre at informasjon i alle former:
>
> - ikke blir kjent for uvedkommende (konfidensialitet)
> - ikke blir endret utilsiktet eller av uvedkommende (integritet)
> - er tilgjengelig ved behov (tilgjengelighet)
>
> Brudd på et eller flere av disse punktene er et brudd på informasjonssikkerheten.» [14]

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) stiller krav til at forvaltningsorganer skal ha en internkontroll innenfor informasjonssikkerhet. Internkontrollen skal være basert på anerkjente standarder for styringssystemer for informasjonssikkerhet (§ 15) og være en integrert del av virksomhetens helhetlige styringssystem.

Når det gjelder kommunens helhetlige styringssystem stiller kommuneloven spesifikke krav til internkontroll i koml. § 25-1. KS sin verktøykasse for personvern og informasjonssikkerhet er videre sentral med hensyn til den delen av internkontroll og styring som gjelder informasjonssikkerhet i kommunen. Det er forutsatt at kommunen selv skal tilpasse internkontroll og styringssystemet til egen organisasjon. Andre sentrale anbefalinger som kommunen vil måtte forholde seg til er Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren (heretter kalt Normen) og Nasjonal Sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet. Gjennomgående for de anbefalingene som er gitt på området er at styringssystemet og internkontroll for informasjonssikkerhet er en integrert del

[14] www.digdir.no

av kommuneledelsens helhetlige styrings- og internkontrollsystem. Dette jfr. eForvaltningsforskriften § 15.

Det er Direktoratet for e-helse som sammen med helse- og omsorgssektoren har utarbeidet Normen for ivaretakelse av informasjonshåndtering, informasjonssikkerhet og personvern. Det heter i denne at:

> «Opplysningene må behandles slik at helse- og omsorgstjenester kan tilbys på en forsvarlig måte og samtidig ivaretar innbyggernes tillit til sektoren. God informasjonssikkerhet og godt personvern er en forutsetning for digitalisering. Sektoren må bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur.» [15]

Normen legges til grunn som et av flere relevante regelverk som gjelder for fastsatte sikkerhetsmål og sikkerhetsstrategi i Våler kommune. Selv om den er rettet mot helse- og omsorgssektoren er prinsippene i Normen også relevante for andre sektorer i kommunal virksomhet. Normen stiller følgende krav for å sikre *konfidensialitet* i virksomheten:

- ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger,
- hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten,
- avgrense tilgang for autorisert personell iht. tjenstlige behov, og
- ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten.

Normen stiller følgende krav for å sikre *integritet* i virksomheten:

- at virksomheten sikrer at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er sikret mot utilsiktet eller uautorisert endring eller sletting,
- integritet er en forutsetning for god og forsvarlig hjelp, og det skal logges hvem som har rettet, registrert, endret og slettet informasjon,
- sikre at helse- og personopplysninger blir registrert på rett person og at disse føres i henhold til relevant kodeverk/terminologi, og
- sikre at opplysninger er korrekte og nødvendig relaterte og forhindre at kopier blir en kilde til utdatert informasjon.

Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er *tilgjengelig*:

- rett informasjon er tilgjengelig til rett tid og ut i fra tjenstlige behov,
- sikre forsvarlig og stabil drift i alle informasjonssystemer,
- sikre at det foretas egnede tiltak for å sikre forebygging, oppdagelse, håndtering og gjenoppretting av informasjon.

Brudd på alle disse kravene må etter Normen behandles som avvik. [16]

Informasjonssikkerhet krever i så måte at en kommune forvalter sine oppgaver i en digital hverdag på forsvarlig vis, og at de ansatte som forvalter dette også er i stand til å kunne utføre oppgavene sine på en sikker måte. Forsvarligheten sikres konkret gjennom blant annet:

- et etablert tilgangsstyringssystem,

[15] Norm for informasjonssikkerhet og personvern

[16] Norm for E-helse, opprinnelig kalt Norm for informasjonssikkerhet og personvern, side 16

- programvare som loggfører aktivitet og endring av informasjon,
- gjennom klare risiko- og vesentlighetsanalyser for bruk av de ulike programmer.

Kommunens internkontroll

Med ny kommunelov av 2019 ble internkontrollansvaret i kommunesektoren tydeliggjort. Dette fordi begrepet ble fjernet fra øvrige lovverk og forskrifter, og at internkontrollansvaret ble «samlet på et sted». Kommunens internkontroll skal tilpasses kommunens behov og risikoforhold. [17]

KS har utarbeidet en veileder for kommunedirektørens internkontroll til støtte for hvordan kommunene kan identifisere risiko og utarbeide en risikobasert internkontroll tilpasset kommunens behov. Det fremgår i veilederen at hensikten med internkontrollen i kommunen er å sikre at lover og forskrifter følges.

Kommuneloven angir minstekrav til internkontrollen, og er beskrevet i koml. §25-1:

> «Ved internkontroll etter denne paragrafen skal kommunedirektøren
>
> a. utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
>
> b. ha nødvendige rutiner og prosedyrer
>
> c. avdekke og følge opp avvik og risiko for avvik
>
> d. dokumentere internkontrollen i den formen og det omfanget som er nødvendig
>
> e. evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.» [18]

Kommunen kan velge å etablere en internkontroll som går lenger enn disse minstekravene. I KS sin veileder «Orden i eget hus – Kommunedirektørens internkontroll», står følgende:

> «God internkontroll handler i stor grad om systematisk arbeid, god organisering og dokumentasjon, arbeidsmetoder og samhandling som kan forebygge lovbrudd og uønskede hendelser». [19]

KS skriver videre at selv om internkontroll og virksomhetsstyring kan overlappe, er internkontrollen mer risikobasert enn mål- og resultatstyrt, slik virksomhetsstyring ofte er.

Kontrollbegrepet kan deles i to perspektiver:

- Et strategisk perspektiv hvor man ønsker å etablere et felles styringssystem og verktøy for å nå en virksomhets mål.
- Et operasjonelt perspektiv hvor man omtaler de løpende prosessene og de praktiske aktivitetene i tjenesteproduksjonen og i støtteprosesser.

Risikobasert utarbeidelse av dokumentasjon for internkontroll, som tilpasses underveis, er derfor et sentralt element ved hvordan internkontrollen bør formes.

eForvaltningsforskriften § 15 viser til følgende:

> *«Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på*

[17] KS: Kommunedirektørens internkontroll, side 9
[18] Kommuneloven: Lov om kommuner og fylkeskommuner
[19] KS: Kommunedirektørens internkontroll, side 24

> *informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.»* [20]

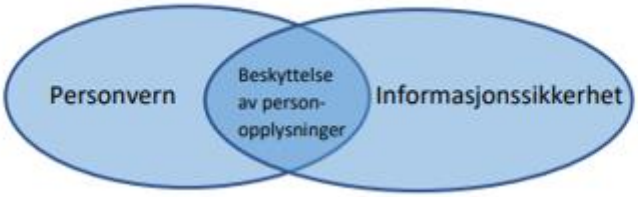
Sikkerhetsstrategi og mål er også beskrevet i Normen: «Alle offentlige virksomheter skal beskrive mål og etablere strategi for informasjonssikkerhet. Dette skal danne grunnlaget for styringssystemet.» [21]

Anbefalinger for informasjonssikkerhet og personvern

KS ga i januar 2022 ut et tillegg til kommunedirektørens internkontroll. [22] Dokumentet er utarbeidet av KPMG og skal fungere som en verktøykasse for kommunedirektører for temaene informasjonssikkerhet og personvern. [23] Her står det følgende:

> «Internkontrollen skal bidra til at kommunen ivaretar beskyttelsesbehovet til informasjon og personopplysninger og er kommunaldirektørens viktigste verktøy for å styre risiko på personvern- og informasjonssikkerhetsområdet». [24]

KS sin verktøykasse viser i dokumentet til at GDPR og ny personvernlovgivning visker ut noen av forskjellene mellom informasjonssikkerhet og personvern. Samtidig viser de også til at informasjonssikkerhet og personvern er to forskjellige fagområder med overlappende temaer. Selv om denne forvaltningsrevisjonen omhandler informasjonssikkerhet vil den også i noen grad omhandle forhold knyttet til personvern, ettersom IKT-systemene skal innrettes slik at personopplysninger er beskyttet. Følgende modell benyttes for å skissere at personvern og informasjonssikkerhet overlapper der hvor det omhandler beskyttelse av personopplysninger:



Figur 1 - hentet fra kommunedirektørens verktøykasse for informasjonssikkerhet og personvern, side 6.

KS sin verktøykasse inneholder en rekke anbefalinger for hvordan kommunedirektøren best kan ha kontroll med kravene til informasjonssikkerhet og personvern.

Det anbefales i første omgang å tilegne seg en oversikt over hva man har av informasjon og opplysninger, og kategorisere disse etter hva slags verdi de har. Inndelingen som anbefalingen viser til er ikke en mal, men et eksempel på hvordan dette kan gjøres. KS deler først inn informasjonen i ulike verdinivåer med hensyn til hvor viktig informasjonen er for tjenesteytelsen i kommunen:

- Kritisk verdi
  - Informasjon som er kritisk i en krisesituasjon (for eksempel samfunnskritiske funksjoner, beredskapsplaner, helseopplysninger).
- Høy verdi

[20] Eforvaltningsforskriften: Forskrift om elektronisk kommunikasjon med og i forvaltningen
[21] Norm for e-helse, side 13
[22] KS: Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet.
[23] Vi vil i det følgende omtale dette dokumentet som «KS sin verktøykasse for informasjonssikkerhet og personvern», eller bare KS sin verktøykasse».
[24] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern, side 26

    - Informasjon som vil være ødeleggende for funksjoner og tjenester som er kritisk for daglig drift (for eksempel strategidokumenter, eksamener/tentamener, informasjonssystem for lønnsutbetaling).
- Middels verdi
    - Informasjon som kan skade kommunens tjenester og funksjoner i daglig drift (for eksempel informasjon unntatt offentlighet, læringsplattform for kommunikasjon mellom elever og skole).
- Lav verdi
    - Åpen informasjon uten særskilte sikkerhetsbehov (for eksempel informasjon fra hjemmesiden til virksomheten).

KS sin verktøykasse for informasjonssikkerhet og personvern viser til at det etter en slik gjennomgang vil være naturlig å starte med den informasjonen det er knyttet størst negativ risiko til. Disse vurderingene skal ende opp i en tiltaksplan. Tiltaksplanen må inneholde hvem som er ansvarlige for det enkelte tiltak og hvilke risikovurderinger som er gjort. Risikovurderingene bør i tillegg kobles opp til den sektorovergripende internkontrollen. I denne internkontrollen bør kommunen vurdere hvor ofte man bør kontrollere tiltakene i forbindelse med evaluering av om iverksatte tiltak fungerer etter hensikten.

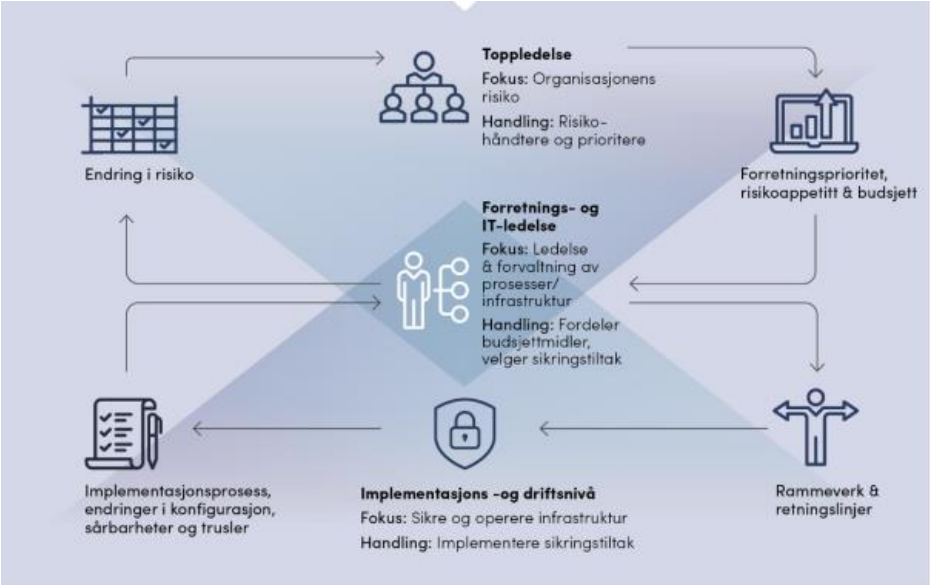
I anbefalinger beskrives også ulike sikkerhetstiltak knyttet til om risikoen er relatert til informasjonssikkerhet eller personvern. Informasjonssikkerhetstiltak kan knyttes både til gode arbeidsrutiner og sikkerhetsbevissthet hos de ansatte i kommunen, og til teknisk drift. Gode arbeidsrutiner og sikkerhetsbevissthet hos de ansatte kan for eksempel dreie seg om tilgangsstyring, internkontroll, opplæringstiltak og adgangskontroll til fysiske bygg og gjenstander. Andre momenter som kan være viktige er retningslinjer for bruk av sosiale medier, bruk av samme passord over flere plattformer, eller bruk av samme passord både privat og på jobb m.m. Vi mener at det er naturlig å forvente at kommunen kan dokumentere at det er foretatt vurderinger av hvilke typer informasjon kommunen bør prioritere å sikre, og at det er iverksatt tiltak basert på disse prioriteringene.

Særlig ledelsesansvar

Normen beskriver at det ligger et særlig ledelsesansvar i informasjonssikkerhet. Dette innebærer at ledelsen i organisasjonen både har vurdert og bestemt riktig nivå for akseptabel risiko, og at det gjennomføres en systematisk og bevisst oppfølging for å sikre organisasjonens informasjonssikkerhet. Dette bør gjenspeiles i virksomhetens aktiviteter, planverk, retningslinjer og kvalitetssystem.

Digitaliseringsdirektoratet beskriver forankring i ledelse som et viktig punkt i sin veileder for informasjonssikkerhet. KS skriver i sin veileder for kommunedirektørens verktøykasse at: «I en stadig mer digitalisert verden, er det viktig at toppledere har kunnskap om digital risiko, muligheter for å redusere risiko og hvilke regelverk som må etterleves». [25] Nasjonal sikkerhetsmyndighet viser også til at ledelse og ledelsesforankring skal sikre redusert risiko og kontinuerlig oppfølging av informasjonssikkerhet i en virksomhet, som vist i denne figuren: [26]

[25] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern, side 4
[26] Nasjonal sikkerhetsmyndighet, «grunnprinsipper for IKT-sikkerhet», side 4



Figur 2 hentet fra Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet, side 4.

Nasjonal sikkerhetsmyndighet mener at: «Det er avgjørende at toppledelsen tar eierskap og involverer seg i sikkerhetsarbeidet i egen virksomhet.». [27]

Ledelsens gjennomgang av informasjonssikkerhetsområdet

I KS sin verktøykasse legges det til grunn at ledelsen som minimum en gang per år bør holde en gjennomgang av personvern og informasjonssikkerhet. Formålet med møtet bør være å gå gjennom status for arbeidet med personvern og informasjonssikkerhet i kommunen. På den måten vil ledelsen få tilstrekkelig informasjon om status og risikoer knyttet til området. Det gjør det enklere å ta avgjørelser om nødvendige tiltak og forbedringer i internkontrollen, type aktiviteter i internkontrollen eller organiseringen av arbeidet med personvern og informasjonssikkerhet.

Til dette arbeidet bør personer som jobber med fagområdene i kommunen inviteres, dvs. sikkerhetsansvarlig, ansvarlig for personvern i kommunen, personvernombudet etc. Det heter videre at det bør settes opp noen enkle rutiner for hvordan dette møtet skal gjennomføres og hvilke forberedelser og oppfølgingsaktiviteter som forventes etter at møtet er gjennomført.

Det kan forvente at ledelsens gjennomgang omfatter:

- Orientering om relevante endringer på rettsområdet.
- Orientering om risiko- og trusselbildet for personvern og informasjonssikkerhet.
- Gjennomgang av vesentlige og/eller alvorlige avviksaker i kommunen siden forrige ledelsens gjennomgang, herunder hvordan disse er håndtert og fulgt opp.
- Gjennomgang av behandlingsaktivitetene (behandlingsprotokoller).
- Overordnet gjennomgang av endringer i risikovurderinger og tiltak som er innført.
- Gjennomgang av oppfølgingen av leverandører.

Normen for E-helse legger til grunn en tilsvarende gjennomgang spesielt for helse- og omsorgs-tjenestene. Her stilles det også krav om at dersom gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt, skal det vedtas tiltaksplaner for å rette opp dette, med tidsfrister og plassering av ansvar. Ledelsens gjennomgang skal også dokumenteres.

[27] Nasjonal sikkerhetsmyndighet: NSMs grunnprinsipper for IT-sikkerhet, side 4

Punktvis oppsummering av revisjonskriterier for problemstilling 1

1. Kommunen må ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).
2. Kommunen og kommunens øverste ledelse må ha en tilpasset og risikobasert internkontroll for informasjonssikkerhet. Internkontrollen inneholder både et strategisk og langsiktig perspektiv, og et operasjonelt perspektiv som omhandler daglig virksomhetsstyring.
3. Kommunen må ha fastsatt hva som kan aksepteres av risiko og gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi. Der risikoen er over fastsatt grense for hva som er akseptabelt bør det utarbeides tydelige tiltaksplaner som viser hvem som er ansvarlig for ulike tiltak.
4. Kommunen må ha rutiner og prosedyrer som sørger for at informasjon ikke blir kjent for uvedkommende.
5. Kommunen må ha rutiner og prosedyrer som sørger for at informasjon ikke blir endret utilsiktet, eller av uvedkommende.
6. Kommunen må ha rutiner og prosedyrer som sørger for at informasjon er tilgjengelig ut ifra tjenstlige behov.
7. Kommunens ledelse må ha rutiner for å gjennomgå kommunens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året.
8. Ledelsen årlige gjennomgang innen informasjonssikkerhet og personvern i helse- og omsorgstjenestene må dokumenteres, og dersom gjennomgangen har avdekket at virksomhetens risikonivå ikke er i henhold til akseptabelt risikonivå må det være vedtatt tiltaksplaner for å rette opp avviket.

Utledning av revisjonskriterier for problemstilling 2

Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?

Denne problemstillingen tar sikte på å belyse om kommunen har satt i gang og implementert de konkrete sikkerhetstiltakene som trengs for å sikre seg mot uautorisert tilgang på informasjon.

Risikoforståelse

Digitaliseringsdirektoratet skriver på sine informasjonssider at innen informasjonssikkerhet er det svært viktig å etablere og forvalte varige tiltak som reduserer risiko, slik at virksomheten kan utføre sine oppgaver og levere tjenester på en god måte. Slike varige tiltak reduserer risiko ved å redusere konsekvenser av uønskede hendelser eller sannsynligheten for at de inntreffer. Det er disse varige tiltakene vi som regel omtaler som sikkerhetstiltak.

Datatilsynet skriver at vurderinger av risiko er en viktig del av det kontinuerlige arbeidet innenfor informasjonssikkerhet:

> «*Risiko* betegner forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse. Risikovurderingen må ses i sammenheng med etablerte akseptkriterier for risiko, og den behandlingsansvarlige skal iverksette nødvendige tiltak for å oppnå tilfredsstillende *informasjonssikkerhet*». [28]

KS viser til at det å ha en rettmessig forståelse av risiko innebærer en forståelse av hvilken risiko virksomheten kan være utsatt for:

> «Kommunen bør ha oppdatert innsikt i overordnede trender og utviklingen i kommunens risikobilde. Fagpersoner på informasjonssikkerhets- og personvernområdet bør ha i oppgave å ivareta denne type risikovurderinger». [29]

Risikobildet er i stadig endring og krever at det følges med i utviklingen. Sikkerhetstiltak må tilpasses ut fra:

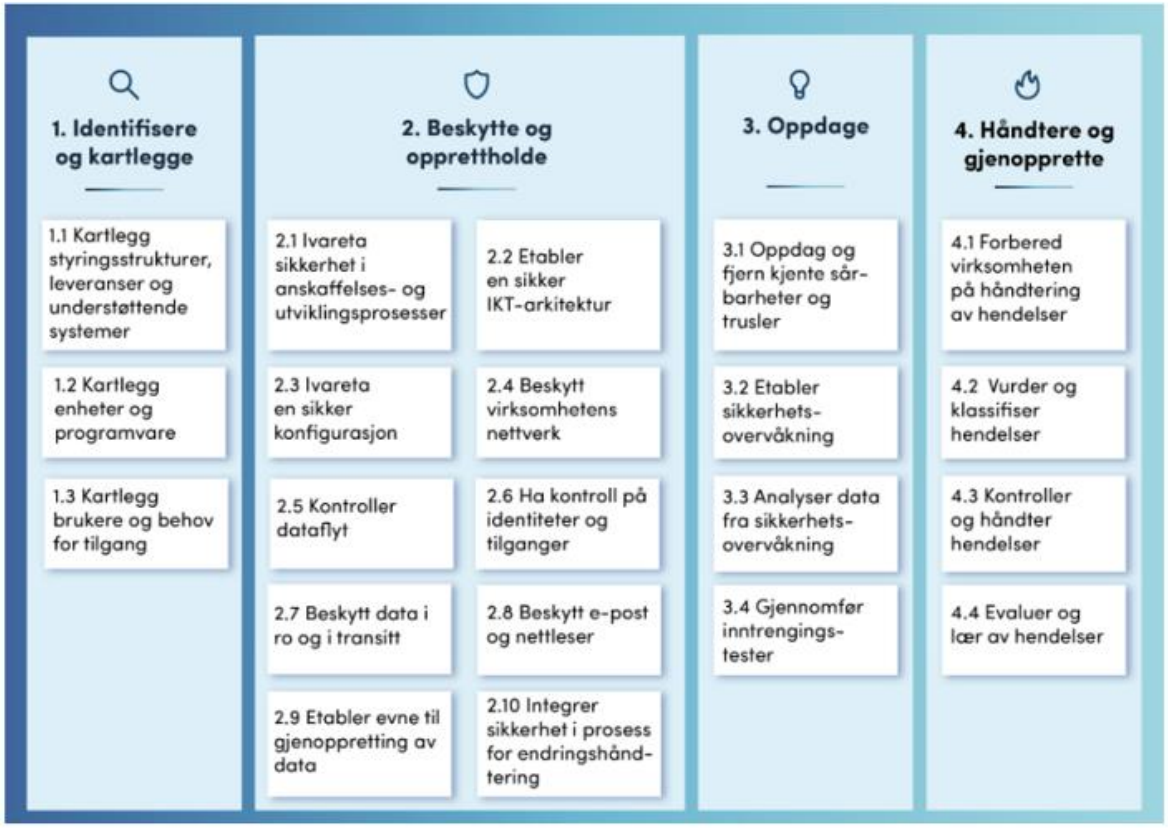
- Sikkerhetshendelser og hackerangrep som oppstår
- Læring av egne feil eller når ting gjøres riktig
- Anvendelse av ny teknologi eller programvare
- Utvikling av ulike arbeidsmetoder
- Sektorovergripende internkontrollaktiviteter
- Hvordan iverksetting av ulike sikkerhetstiltak samvirker med tekniske, organisatoriske og menneskelige faktorer

Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern anbefaler derfor:

> «…å bygge et rammeverk som stiller krav til sikkerhetstiltak, som bidrar til at kommunen forholdsvis enkelt kan få en god informasjonssikkerhet og godt personvern som bidrar til å håndtere mange risikoer». [30]

[28] Datatilsynet: Virksomhetens plikter innen informasjonssikkerhet og internkontroll: Risikovurdering
[29] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet, side 16
[30] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet, side 20

Det bør etableres rutiner og roller i organisasjonen som sikrer at alle systemer er risikovurdert ved oppstart, og at de jevnlig risikovurderes i tilknytning til større endringer i systemet eller når det skjer endring i risikoforholdene ellers. Et eksempel på rammeverk som KS anbefaler er NSMs grunnprinsipper for IKT-sikkerhet:



Figur 3 Oversikt over NSMs grunnprinsipper for IKT-sikkerhet, kilde: www.nsm.no

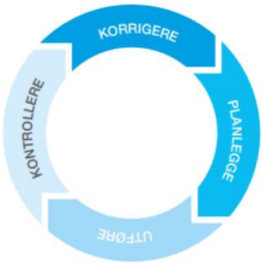
Det legges til grunn at de ulike komponentene i oversikten er til stede, at risiko er vurdert og at det er iverksatt kompenserende tiltak. Det er ellers flere av komponentene som fordrer jevnlig oppfølging gjennom kommunens internkontrollsystem og risikovurderinger. NSMs grunnprinsipper legger til grunn at det gjennomføres risikovurderinger i forhold til IKT-arkitektur, konfigurasjon av maskin- og programvare, nettverk, e-post, nettlesere og data. Risikovurderinger knyttet til data vil i denne forbindelse omfatte kontroll på boksene i figur 3 som hender om dataflyt, brukertilganger og behov for kryptering. På grunn av at sikkerhetsrisikoen stadig endrer seg vil det være behov for jevnlige gjennomganger. Dette må gjøres planmessig og det må være avklart hvem som skal gjøre dette. Det er ellers viktig at sikkerhetsarbeidet er forankret i kommuneledelsen og at det ses i sammenheng med kommunens strategi og målsettinger for informasjonssikkehetsarbeidet.

Oversikten viser også hvordan vurderinger med hensyn til informasjonssikkerhet er en viktig del av endringsprosesser, anskaffelses- og utviklingsprosesser og beredskapen i kommunen. Det anbefales at hensynet til informasjonssikkerhet er integrert i anskaffelses- og endringsprosessene og at kommunene er bevisste på hvilke krav som stilles til tjeneste- og utstyrsleverandørene. Å ta hensyn til sikkerhetskravene er også i høyeste grad relevant dersom kommunen utvikler sine egne informasjonssystemer.

Risiko- og vesentlighetsvurderinger, sikkerhetsrevisjoner

Digitaliseringsdirektoratet (Digdir) viser til at risikovurderinger er et viktig verktøy som må være en del av virksomhetens sikkerhetstiltak: «Vurdering av risiko er «hjertet» i internkontrollen. Risiko som angår informasjonssikkerhet må identifiseres, analyseres og evalueres». [31]

Datatilsynet, Digdir, Normen og KS (Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern) presenterer modeller for internkontroll og risikovurderinger som er relativt like i sine prinsipper, der kontinuerlig forbedring sikres gjennom at de er sirkulære i sine aktiviteter. KS sin modell har fire aktiviteter, eller faser; planlegge, utføre, kontrollere, korrigere. Felles for alle disse modellene er at de sikrer kontinuitet, og at det jevnlig gjennomføres revisjoner etter at en risikovurdering er gjennomført. KS og Normen bruker «Demings sirkel» som modell for å beskrive dette:



Figur 8: Demings sirkel: Plan, Do, Check, Act

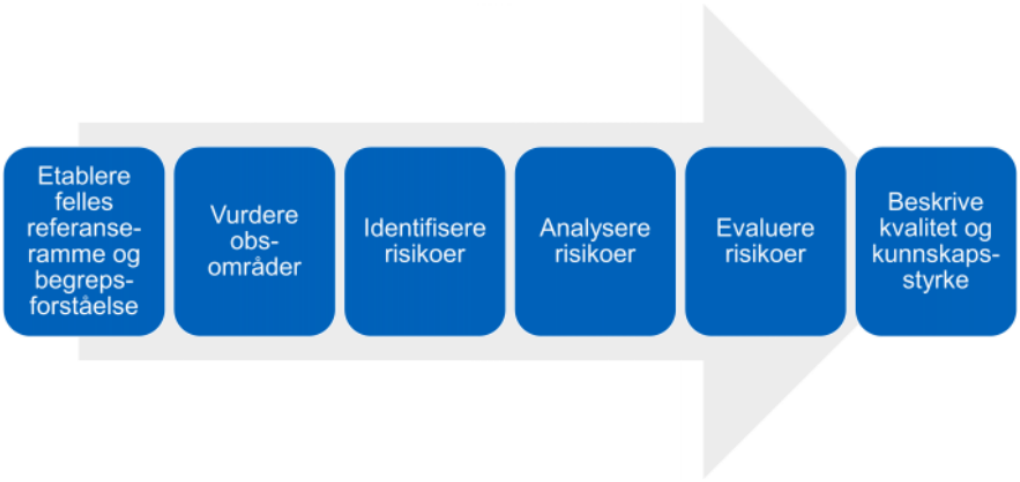
Figur 4 Demings sirkel, kilde: www.ks.no

Når det gjelder uønskede hendelser er det i hovedsak to komponenter som spiller inn og som kan føre til at ting går galt. Det ene er sårbarhetene som kommunen selv har, og det andre er de truslene som kommunen står overfor. Eksempler på uønskede hendelser kan være feilkoding av saker som fører til at personlig informasjon havner på postlister, en brann kan oppstå som fører til at en server blir ødelagt, en skole kan bli hacket og informasjon kan lekkes, en ansatt kan bli utsatt for phishing og gi uønskede tilgang til informasjon, eller at det kan innføres skyggesystemer av enheter som ikke er sikret gjennom de faste prosedyrer som virksomheten har for informasjonssikkerhet og anskaffelser. Slike hendelser har ofte omdømmemessige og økonomiske konsekvenser for virksomhetene.

NSMs grunnprinsipper for IKT-sikkerhet vektlegger sikkerhetsovervåkning og testing av informasjonssystemene, for eksempel i form av inntrengningstester. Det anbefales å utarbeide planer for dette og at det samles inn sikkerhetsdata og trusselinformasjon for analyse og vurdering av risiko i egen organisasjon.

Vurdering av risiko er viktig i arbeidet med informasjonssikkerhet. Dette må organiseres på en god måte, for å gi et godt grunnlag for håndtering av risiko. Digitaliseringsdirektoratet har beskrevet følgende modell for risikovurdering i forbindelse med informasjonssikkerhet:

[31] Digitaliseringsdirektorate*t: Gjennomføre en risikovurdering*



Figur 5 - Kilde: Digitaliseringsdirektoratet, Gjennomføre en risikovurdering

I Normen står det at virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner. Formålet med en sikkerhetsrevisjon er å gjennomføre kontrollaktiviteter og kvalitetssikring av etablerte tiltak og fastsatte rutiner. Det skal foreligge en godkjent plan for sikkerhetsrevisjoner. Det viktigste med å ha en kontinuitet i revisjonene er å sikre kontinuerlig forbedring, slik at virksomheten sikrer at de er oppdaterte og videreutvikler sine systemer i takt med trusselbildet. [32]

Avvikshåndtering og gjenopprettelse av IT-drift

Hvis det oppstår hendelser som fører til at IKT-tjenestene er nede og at informasjon som er nødvendig å gjennomføre ikke er tilgjengelig, er det viktig å ha beredskapsplaner og jevnlige øvelser som sikrer at man kan gjenopprette normal drift ved en digital sikkerhetshendelse. Her er det viktig at disse planene er utformet slik at de ivaretar kravene til personvern og informasjonssikkerhet. [33] NSMs grunnprinsipper for IKT sikkerhet legger vekt på at det er klartgjort hvordan uønskede hendelser skal håndteres, hvordan systemer og nettverk skal gjenopprettes og hvem som har hvilke roller og ansvar. Det legges videre vekt på gode rutiner for sikkerhetskopiering og at det øves på håndtering av uønskede hendelser og krisesituasjoner. Det er også viktig å ha rutiner for å registrere, håndtere, evaluere og følge opp avvik i drift.

KS sin verktøykasse legger til grunn at håndtering av avvik knyttet til personvern og informasjonssikkerhet gjøres som en integrert del av kommunens avvikssystem. For avvik i tilknytning til helse- og omsorgstjenesten er Normen mer spesifikk med hensyn til håndtering av avvik:

> «*For å sikre at regelverket følges skal det etableres avviksrutiner slik at avvik oppdages og at årsak til avviket, korrigerende tiltak, læring og rapportering blir dokumentert. Avvikshåndtering kan også iverksettes ved tilfeller av manglende eller uhensiktsmessige rutiner. Virksomheten skal samle inn fakta om hendelsesforløpet for etablering av korrigerende tiltak og effekten av korrigerende tiltak skal vurderes og eventuelle andre tiltak skal settes i verk ved behov».*

Det er den enkelte ansatte som er ansvarlig for å rapportere avvikshendelser.

[32] Normen: Veileder om internkontroll for sikkerhet og personvern
[33] Kommunedirektørens verktøykasse for informasjonssikkerhet, side 20

Punktvis oppsummering av revisjonskriterier for problemstilling 2

9. Kommunen må gjennomføre systematiske risikovurderinger på informasjonssikkerhets-området.
10. Kommuneledelsen må ha oversikt over og et bevisst forhold til:
    a. Styringsstrukturer, leveranser og understøttende systemer
    b. Enheter og programvare
    c. Brukere og behov for tilganger
11. Det må sikres jevnlig gjennomgang og vurdering av risiko når det gjelder:
    a. IKT-arkitektur
    b. Konfigurasjon av maskin- og programvare
    c. Nettverk
    d. Dataflyt, brukertilganger og behov for kryptering
    e. E-post og nettlesere
12. Kommunen må ta hensyn til informasjonssikkerheten i forbindelse med anskaffelser og utviklingsprosesser.
13. Kommunen må gjennomføre planmessig sikkerhetsovervåkning og testing på området.
14. Det må planlegges hvordan uønskede hendelser skal behandles, hvordan systemer og nettverk kan gjenopprettes og det gjennomføres øvelser på området.
15. For helse- og omsorgstjenestene må det planlegges og gjennomføres sikkerhetsrevisjoner. Resultatene fra sikkerhetsrevisjonene må følges opp og dokumenteres.
16. Kommunen må ha klare rutiner for avviksrapportering og -håndtering.

Utledning av revisjonskriterier for problemstilling 3

I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

Denne problemstillingen søker å besvare om de ansatte følger opp sin rolle i tilknytning til informasjonssikkerhet og om de har den kompetansen som behøves for å kunne gjøre dette.

Forankring av rutiner

I KS sin veileder for internkontroll blir det omtalt ulike områder som vil avkreve sektorovergripende regler. Her blir blant annet datasikkerhet og håndtering av personopplysninger nevnt. KS skriver at det vanligvis ikke er mangel på rutiner som er utfordringen ved internkontrollen, men at rutinene ikke følges. For å sikre at rutinene følges, må disse gjøres kjent for de ansatte og kommunen bør ha egne rutiner som sikrer dette. I enkelte tilfeller vil det også være behov for opplæring i rutinene. Det kan også være aktuelt å sikre at de ansatte har forstått og forpliktet seg til å følge de rutiner som er fastsatt. En annen årsak til at rutiner ikke følges, kan være at rutinene fremstår som rigide eller tungvinne sett opp mot andre krav i arbeidshverdagen i den enkelte tjeneste. Dette er spesielt kjent innenfor IKT-sikkerhet hvor man lett kan sikre systemer ved å lukke de fullstendig fra tilgang på internett eller fastsette krav til komplekse passord og flertrinnsverifisering ved enhver pålogging, noe som vil være lite hensiktsmessig dersom brukerne av systemene skal være i stand til å gjennomføre arbeidsoppgavene sine på en effektiv måte. Det er derfor viktig at regler og rutiner er utarbeidet og

tilpasset den faktiske situasjonen for kommunen og kommunens tjenester og at ledelsen får tilbakemelding på hvordan de fungerer i praksis.

Kommunen bør ha rutiner for oppbevaring, evaluering og ajourhold av planer, reglementer, rutiner etc. Etter koml. § 25-1 pkt. e) er kommunene pålagt å ha et internkontrollsystem der en evaluerer, og ved behov forbedrer skriftlige prosedyrer og andre tiltak for internkontroll.

Når det gjelder oppfølging av planer, reglementer og rutiner, så legger KS sin veileder om kommunedirektørens internkontroll vekt på rapportering fra virksomhetene. Det heter at en gjennom oppfølging og styringssløyfer skal sikre nødvendige tilbakemeldinger og justeringer i internkontrolltiltakene slik at kommunedirektøren har betryggende kontroll selv om denne ikke har innsikt i alle detaljer. Ut fra dette legger vi til grunn at kommunens enheter rapporterer på sitt arbeid med internkontroll, og at en samlet vurdering/oppsummering av dette gjøres i forbindelse med ledelsens årlige gjennomgang av kommunens aktiviteter innen informasjonssikkerhet og personvern.

Den menneskelige faktoren, en viktig del av god informasjonssikkerhet

Mange tenker at fysiske og tekniske sikkerhetstiltak, eksempelvis kryptering, tilgangsstyring, passordstyrke eller utvikling av sikre IKT-systemer, er det som skal til for å ivareta krav til informasjonssikkerhet og personvern. Den menneskelige faktoren er likeså viktig, og god informasjonssikkerhet og godt personvern er også avhengig av ansatte med gode arbeidsrutiner og en klar bevissthet rundt sikkerhet i bruk av digitale hjelpemidler. [34] Etterlevelse, riktig teknologi, god virksomhetsstyring, risikovurderinger og en kontinuitet er alt sammen avhengig av menneskers ferdigheter og kunnskap. I en virksomhet favner informasjonssikkerhet alle og krever at alle bidrar og har riktig kunnskap i forhold til hvordan de hjelper til med å sikre informasjonssikkerheten. [35]

Digitaliseringsdirektoratet har utarbeidet en egen veileder som omhandler kompetanse og kulturutvikling innen digital sikkerhet. [36] Deriblant er det også utarbeidet egne kompetansebeskrivelser som angir krav til både nøkkelpersoner innen IT, ansatte generelt og ledelsen i virksomheten. Det legges generelt vekt på en kontinuitet i forståelsen av hvilke handlinger som kompromitterer informasjonssikkerheten og at man generelt må ta ansvar for å skape både et planverk og kontinuerlige aktiviteter i virksomheten som sikrer tilstrekkelig kompetanse innen informasjonssikkerhet og som skaper en kultur som ivaretar informasjonssikkerheten. Det forutsettes at kommunen har oversikt, og kartlegger behovet for kompetansetiltak. De ansatte trenger kunnskap om hvilken betydning informasjonssikkerhet har i de arbeidsoppgavene de utfører, og hvordan de kan gjennomføre arbeidet sitt på en måte som ivaretar behovet for informasjonssikkerhet. Her handler det blant annet om å inneha en tilfredsstillende forståelse av trusler og risiko, slik at de utfører arbeidsoppgavene på en sikker måte. De må også forstå hvordan uønskede hendelser kan hindre dem i å få gjort jobben sin slik de skal, eller hvordan dette kan få konsekvenser for andre parter. Det er viktig at ansatte kjenner til kommunens interne rutiner for varsling av informasjonssikkerhetshendelser. [37]

Opplærings- og utviklingsaktiviteten må være forankret i ledelsen og det må planlegges hvordan kommunen skal sikres tilstrekkelig kompetanse på kort og lang sikt, basert på risiko og hva kommunen kan akseptere av risiko. Planleggingen kan for eksempel omfatte kompetansebehov i ledelsen, blant

[34] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

[35] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

[36] Veileder i kompetanse og kulturutvikling innen digital sikkerhet

[37] Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet

nøkkelpersonell og blant vanlig ansatte. Den kan gå på hva som kommunen må ha av kompetanse selv, og hva som kan kjøpes av andre, samarbeid etc. KS sin veileder for personvern og informasjonssikkerhet anbefaler blant annet at kommunen har en egen rådgiver eller sikkerhetsansvarlig på området. Alle kommuner plikter også å ha et personvernombud. Det er i tillegg viktig at kommunen organiserer oppgaver og kompetanse slik at informasjonssikkerheten blir ivaretatt. En viktig del av dette er tydelig delegering av oppgaver og ansvar med hensyn til informasjonssikkerhet.

Punktvis oppsummering av revisjonskriterier for problemstilling 3

17. Kommunen må ha rutiner for bekjentgjøring, oppbevaring og ajourhold som sikrer at gjeldende planer, reglementer og rutiner knyttet til informasjonssikkerhet er kjent og tilgjengelig.
18. Kommunen må ha rapporteringsrutiner som sikrer oppfølging og evaluering av planer, reglementer og rutiner knyttet til informasjonssikkerhet.
19. Kommunen må sikre oversikt over kompetansebehovet og sørge for at den enkelte ansatte både får generell og tilpasset opplæring i hvordan informasjonssikkerheten kan ivaretas.
20. Det bør planlegges hvordan kommunen skal sikre kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen.