Revisjon Øst IKS

FORVALTNINGSREVISJONSRAPPORT

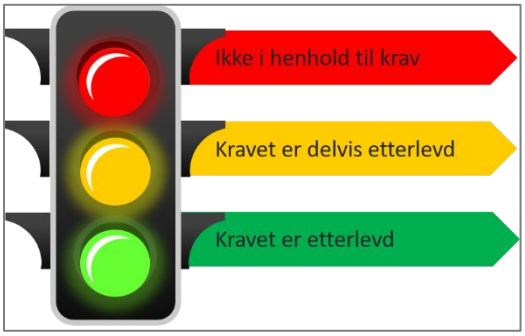
Informasjonssikkerhet

KONGSVINGER KOMMUNE – 2023/2024

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 innledningsvis bygget opp med et kort sammendrag som angir revisors hovedkonklusjon og anbefalinger fra forvaltningsrevisjonen.



I rapporten er det benyttet en «trafikklysmodell» for å illustrere hva revisor anser er i henhold til krav innen området, det som er godkjent med merknad, og det som ikke er i henhold til krav innen området. Hver vurdering er merket med henholdsvis grønt, gult og rødt.

Rapporten er forøvrig utarbeidet med et digitalt tilsnitt og innehar lenker til ulike seksjoner i rapporten. Dette skal gjøre det enklere for leseren å navigere i rapportens innhold.

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

- Sammendrag
- Informasjon om bestillingen (kap. 1)
- Problemstillinger (kap. 2)
- Revisjonskriterier (kap. 2 og vedlegg A)
- Metodebruk (kap. 3 og vedlegg B)
- Presentasjon av data og vurderinger (kap. 4)
- Konklusjon og anbefalinger (kap. 5 og 6)
- Kommunedirektørens uttalelse til rapporten (kap. 7)
- Referanser (kap. 8)

Forvaltningsrevisor Kjetil Kalager har vært utøvende revisor for prosjektet og har ført rapporten i pennen. Jo Erik Skjeggestad har vært oppdragsansvarlig forvaltningsrevisor for prosjektet og har vært tillagt oppgaven med å kvalitetssikre arbeidet.

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 15. januar 2024

Jo Erik Skjeggestad
Oppdragsansvarlig forvaltningsrevisor

Kjetil Kalager
Utøvende forvaltningsrevisor

Innholdsfortegnelse

Forsidebilde: Kongsvinger kommune

Sammendrag

Kontrollutvalget i Kongsvinger kommune fattet i møte den 4. oktober 2022, jf. sak 49/22, vedtak om at det skulle gjennomføres en forvaltningsrevisjon rettet mot informasjonssikkerhet.

Problemstilling og metode

Formålet med forvaltningsrevisjonen har vært å undersøke om Kongsvinger kommune sikrer god informasjonssikkerhet, herunder status knyttet til informasjonssikkerhetsarbeidet. Følgende problemstilling ble satt opp for prosjektet:

- Har Kongsvinger kommune et tilfredsstillende system for å sikre god informasjonssikkerhet?

I undersøkelsen er det gjennomført kvalitative intervjuer med nøkkelpersonell i kommunen, samt dokumentanalyse av styringsdokumenter, rutiner og maler knyttet til informasjonssikkerhet m.v.

Forvaltningsrevisjonens innhentede data er vurdert opp mot utledede revisjonskriterier fra autoritative kilder, så som lovverk, statlige og nasjonale veiledere, samt teori. Kommunedirektøren har mottatt revisjonskriteriene til gjennomsyn og har sagt seg enig i kriteriene.

Konklusjon og anbefalinger

Med bakgrunn i vurderingene som er foretatt i relasjon til problemstillingen, er revisors konklusjon at Kongsvinger kommune har etterlevd de fastsatte revisjonskriteriene på en jevnt over tilfredsstillende måte. Selv om kommunen i hovedsak vurderes å ha et tilfredsstillende system for å sikre god informasjonssikkerhet, herunder en positiv utvikling innen området, foreligger det noen forbedringspunkter som danner grunnlag for revisors anbefalinger. Dette er relatert til forhold som risikoanalyse for internkontroll, risikokartlegging av informasjon i datasystemer, samt utarbeidelse av fullstendig behandlingsprotokoll etter personvernforordningen.

Revisor fremmer følgende anbefalinger:

- Kommunen bør sikre at det utarbeides en samlet risikoanalyse for internkontroll i kommunen.
- Kommunen bør sikre at det gjennomføres en mer detaljert risikokartlegging av informasjonen som befinner seg i datasystemene (kritisk, høy, middels og lav verdi). Der informasjonskartleggingen viser at risikoen er over fastsatt grense for hva som er akseptabelt, bør det utarbeides tydelige tiltaksplaner som viser hvem som er ansvarlig for ulike tiltak.
- Kommunen bør sikre at det utarbeides en fullstendig behandlingsprotokoll etter personvernforordningen.

1 Innledning

1.1 Bakgrunn for prosjektet

I henhold til kommuneloven § 23-2 første ledd bokstav c, skal kontrollutvalget påse at det utføres forvaltningsrevisjon av kommunens virksomhet. Kontrollutvalget i Kongsvinger kommune fattet i møte den 4. oktober 2022, jf. sak 49/22, vedtak om at det, med bakgrunn i utarbeidet prosjektplan, skulle gjennomføres en forvaltningsrevisjon rettet mot informasjonssikkerhet. Temaet er berørt i kontrollutvalgets plan for forvaltningsrevisjon (2021 – 2024).

1.2 Kommunikasjon med revidert enhet

Den 24. april 2023 sendte revisor oppstartsbrev til kommunedirektøren hvor det ble informert om igangsettelsen av inneværende forvaltningsrevisjon. Det ble gjennomført et oppstartsmøte med kommuneadministrasjonen den 31. mai 2023.

Utkastet til forvaltningsrevisjonens revisjonskriterier ble sendt kommunedirektøren til uttalelse den 10. november 2023. Den 4. desember 2023 mottok revisor tilbakemelding på revisjonskriteriene fra kommunen. Det ble opplyst at kommunedirektøren sa seg enig i revisjonskriteriene.

Hovedtyngden av datainnsamlingen har foregått i perioden juni – november 2023.

Forvaltningsrevisjonsrapporten ble sendt kommunedirektøren til uttalelse den 15. desember 2023. Den 12. januar 2024 mottok revisor direktørens uttalelse som er inntatt i rapportens kapittel 7.

2 Formål, problemstilling, revisjonskriterier og avgrensning

2.1 Formål

Formålet med forvaltningsrevisjonen har vært å undersøke om Kongsvinger kommune sikrer god informasjonssikkerhet, herunder status knyttet til informasjonssikkerhetsarbeidet.

2.2 Problemstilling

Følgende problemstilling ble satt opp for forvaltningsrevisjonen:

- Har Kongsvinger kommune et tilfredsstillende system for å sikre god informasjonssikkerhet?

2.3 Revisjonskriterier

Revisjonskriterier skal være utledet fra autoritative eller anerkjente kilder innenfor det reviderte området[1]. 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.

Revisjonskriteriene velges ut med bakgrunn i problemstillingen og danner grunnlaget for hva de innhentede data vurderes opp mot. I og med at revisjonskriteriene er uttrykk for en norm eller et ideal for hvorledes tilstanden bør være på området, er kriteriene også med på å danne utgangspunktet for revisors anbefalinger.

I dette prosjektet benyttes revisjonskriterier fra følgende kilder:

- *Kommuneloven* (2018).
- *Personvernforordningen* (2018).
- *eForvaltningsforskriften* (2004).
- Direktoratet for e-helse (2022): *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.*
- Standard Norge (2017): *Ledelsessystemer for informasjonssikkerhet – ISO/IEC 27001.*
- Kommunal- og moderniseringsdepartementet (2021): *Veileder. Internkontroll i kommunesektoren. Kravene i kommuneloven*.
- KS (2020): *Orden i eget hus. Kommunedirektørens internkontroll.*

[1] NKRF (2020): *RSK 001. Standard for forvaltningsrevisjon.*

- KS (2022b): *Kommunedirektørens verktøykasse for personvern og informasjons-sikkerhet.*
- Digitaliseringsdirektoratet (2020): *Veileder i kompetanse- og kulturutvikling innen digital sikkerhet.*
- Datatilsynet (2018): *Veileder. Informasjonssikkerhet og internkontroll.*
- Direktoratet for forvaltning og IKT (2016): *Internkontroll i praksis – informasjons-sikkerhet. Grunnleggende innføring.*
- Nasjonal sikkerhetsmyndighet (2020): *Grunnprinsipper for IKT-sikkerhet.*
- KS (2022a): *Hovedtariffavtalen (2022– 2024)*. Oslo: Kommuneforlaget.
- COSO (2005): *Helhetlig risikostyring – et integrert rammeverk.*

For nærmere utledelse av revisjonskriterier vises det til vedlegg A.

2.4 Avgrensning

Informasjonssikkerhet kan omfatte både digital, papirbasert og muntlig behandling av informasjon. Denne forvaltningsrevisjonen er primært avgrenset til digital behandling av informasjon, nærmere bestemt digital sikkerhet. Personvern inngår som en del av informasjonssikkerheten.

Ansvaret for tekniske IKT-løsninger, så som sikkerhetskopiering og brannmur, tilligger primært Indigo IKT IKS og er ikke direkte omfattet av forvaltningsrevisjonen. Det settes imidlertid fokus på hvordan Kongsvinger kommune håndterer informasjonssikkerheten innenfor løsningene, eksempelvis i form av rutiner og opplæring.

I samsvar med problemstillingen er forvaltningsrevisjonen avgrenset til systemnivå, det vil si at kommunens operative praksis i mindre grad er omfattet av revisjonen.

3 Metode for revisjonen

3.1 Om metodevalget

Det er hva problemstillingen ønsker å undersøke som bør avgjøre metodevalget (Holme og Solvang: 1996). I undersøkelsen har det blitt gjennomført kvalitative intervjuer og dokumentanalyse.

Metodevalget begrunnes ut ifra problemstillingens sammensatte karakter, herunder ønsket om å fremskaffe varierte data. Det er således tale om en kombinasjon av ulike metoder, det vil si metodetriangulering.

3.2 Intervjuer

I undersøkelsen er det gjennomført kvalitative intervjuer med åtte nøkkelinformanter. Dette er gjort i form av seks enkeltvise intervjuer og ett gruppeintervju. Alle intervjuene har blitt avholdt på Teams høsten 2023.

De kvalitative intervjuene har blitt gjennomført som semistrukturerte intervjuer basert på en intervjuguide. I forkant av intervjuene har intervjuobjektene mottatt informasjon om prosjektets problemstilling og fokusområder. Følgende representanter er intervjuet:

Enhet for økonomi og regionale tjenester (stabsenhet)

- Informasjonssikkerhetsansvarlig i Kongsvinger kommune
- Rådgiver med sentralt ansvar for kvalitetsarbeid/internkontroll i Kongsvinger kommune

Enhet for HR og organisasjon (stabsenhet)

- Rådgiver (HR) og spesialkonsulent (lønn) (gruppeintervju)

Kommunalområdet for miljø og samfunnsutvikling

- Kommunalsjef

Kommunalområdet for helse og mestring

- Rådgiver (fagkoordinator) i enhet for tilrettelagte tjenester

Kommunalområdet for oppvekst og læring

- Rådgiver i stab for oppvekst og læring

Personvernombud

- Regionalt personvernombud for kommunene i Kongsvingerregionen (Kongsvinger kommune er vertskommune for samarbeidet)

* * *

Intervjuobjektene er valgt ut i dialog med kommunen og arbeider enten direkte med informasjonssikkerhet eller har kjennskap til området i arbeidet. Ved siden av personvernombudet er det valgt ut representanter fra kommunens tre kommunalområder og to sentrale stabsenheter.

Det er et bevisst valg å intervjue representanter fra ulike ansvarsområder. Utgangspunktet er at disse personene innehar ulike posisjoner og roller. Informasjonen som det enkelte intervjuobjekt gir vil svært ofte være påvirket av posisjonen og dermed også rollen som det enkelte intervjuobjekt innehar (Andersen, J. A.: 1995).

Referatene fra intervjuene har i etterkant blitt verifisert av de aktuelle informantene.

3.3 Dokumentanalyse

Det har i undersøkelsen blitt gjennomført dokumentanalyse av styringsdokumenter, rutiner og maler knyttet til informasjonssikkerhet. Hensikten har vært å vurdere dokumentenes innhold opp mot krav og føringer som blant annet fremkommer av lovverk og veiledere innen området. På denne måten undersøkes Kongsvinger kommunes dokumenterte system innen informasjonssikkerhet.

Dokumentanalysen søker å supplere intervjudataene ved å blant annet undersøke dokumenter som er felles for hele kommuneorganisasjonen.

For nærmere angivelse av undersøkelsens reliabilitet og validitet vises det til vedlegg B.

4 Data og vurderinger

- Har Kongsvinger kommune et tilfredsstillende system for å sikre god informasjonssikkerhet?

4.1 Revisjonskriterier for problemstillingen

I det følgende fremkommer det revisjonskriterier revisor har benyttet for å besvare problemstillingen og revisors vurderinger av dette. Kriteriene er gjengitt i kortform. For en full utledelse av kriteriene, se vedlegg A. Leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriterium. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt nedenfor. Leseren gjøres derfor oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

Kriterium 1	Kommunen må ha utarbeidet en samlet risikoanalyse for internkontroll. Analysen bør omfatte informasjonssikkerhetsområdet.
Kriterium 2	Kommunen må ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).
Kriterium 3	Kommunen må ha gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi.
Kriterium 4	Der informasjonskartleggingen viser at 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 5	Kommunen må føre en behandlingsprotokoll over behandlingsaktivitetene som utføres under kommunens ansvar.
Kriterium 6	Kommunen må ha et system for å sikre at personvernkonsekvenser (DPIA) vurderes der det er nødvendig.
Kriterium 7	Kommunen må ha utarbeidet nødvendige rutiner for håndtering av personopplysninger.

	Kriterium 8	Kommunen må ha utarbeidet rutiner for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet.
	Kriterium 9	Kommunen må ha utarbeidet nødrutiner som skal sikre kommunens tjenestetilbud ved utfall av elektroniske datasystemer.
	Kriterium 10	Kommunen må ha et system som sørger for at rutinene gjøres kjent blant de ansatte.
	Kriterium 11	Kommunen må ha et system som sørger for at rutinene evalueres og ajourføres.
	Kriterium 12	Kommunen må ha etablert et system for å rapportere og følge opp avvik, herunder eventuelle avvik knyttet til informasjonssikkerhet.
	Kriterium 13	Kommunen må ha en planmessig ordning for å sikre kompetanse innen informasjonssikkerhetsområdet.
	Kriterium 14	Kommunens ledelse bør minst en gang i året, foreta en dokumentert gjennomgang av kommunens aktiviteter innen informasjons-sikkerhetsområdet.

4.2 Innhentede data

I intervjuundersøkelsen fremkommer det at Kongsvinger kommune ikke har utarbeidet en samlet risikoanalyse for internkontroll i kommunen. Det er imidlertid utarbeidet bestemmelser for internkontroll, som ble godkjent av kommunedirektøren i august 2023 (Kongsvinger kommune: 2023b). Av revisors dokumentanalyse går det frem at bestemmelsene blant annet vil danne basis for årlige overordnede risikovurderinger i kommunen. I intervjuundersøkelsen blir det opplyst at den første overordnede risikovurderingen vil bli gjennomført i 2024 og gis virkning i handlingsplanarbeidet for 2025. Det blir samtidig opplyst at det legges til grunn at informasjonssikkerhetsområdet vil inngå i de

overordnede risikovurderingene. Dette da emnet er gjennomgripende og omfatter sentrale risikoforhold i hele kommuneorganisasjonen.

I Kongsvinger kommune er det utarbeidet en skriftlig fremstilling benevnt «overordnet styringsdokument for informasjonssikkerhet og personvern», som sist ble godkjent administrativt i mai 2023 (Kongsvinger kommune: 2023h). Av revisors dokumentanalyse går det frem at styringsdokumentet blant annet inneholder kommunens mål og strategi for informasjonssikkerhet. I styringsdokumentet er det fastsatt følgende sikkerhetsmål:

- Kongsvinger kommunes behandling av informasjon skal være i samsvar med regulatoriske, interne og avtalerettslige krav til informasjonssikkerhet og personopplysningssikkerhet.
- Personopplysninger og annen beskyttelsesverdig informasjon sikres på en betryggende måte gjennom fysiske, tekniske og organisatoriske krav.
- Personopplysninger skal behandles i samsvar med personvernprinsippene, særlig prinsippet om formålsbegrensning og lovens grunnkrav om lovlighet.

For å oppnå sikkerhetsmålene vil kommunen i henhold til det nevnte styringsdokumentet, blant annet legge til grunn følgende strategi:

- Prioritere arbeidet med å oppdatere oversikt over all behandling (protokoll).
- Prioritere helhetlig og systematisk styring, internkontroll og avvikshåndtering, god sikkerhetskultur, samt kontinuerlig forbedring.
- Sikre tilstrekkelig kompetanse i kommuneorganisasjonen knyttet til informasjonssikkerhet og personvern.
- Gi kommunedirektøren en sentral pådriverrolle i informasjonssikkerhetsarbeidet, herunder sette emnet jevnlig på agendaen i direktørens ledermøter.

I kommunens overordnede styringsdokument for informasjonssikkerhet og personvern, er det gitt en beskrivelse relatert til kommunens modenhetsnivå innen området. Modenhetsnivået angis etter følgende skala: «Tilfeldig», «fragmentert», «formalisert», «systematisert» og «optimalisert». Av styringsdokumentet går det frem kommunens modenhetsnivå ble vurdert som «fragmentert» pr. januar 2021.

I intervjuundersøkelsen betrakter informasjonssikkerhetsansvarlig kommunens nåværende modenhetsnivå, det vil si ved utgangen av 2023, som et sted mellom nivå «formalisert» og «systematisert». Målsettingen er å nå nivå «optimalisert» innen 2025.

Siden 2018 har det forelagt et lovkrav om at kommunen skal ha en behandlingsprotokoll over behandlingsaktivitetene etter personvernforordningen. I intervjuundersøkelsen blir det opplyst at Kongsvinger kommune har hatt en systembasert oversikt knyttet til IKT-systemer og applikasjoner (systemer), men at dette ikke regnes som en fullstendig behandlingsprotokoll etter personvernforordningen. Det blir samtidig tilkjennegitt at en rekke av kommunens enheter allerede har levert inn forslag til delprotokoller for sine områder, og at en fullstendig behandlingsprotokoll antas å foreligge i løpet av 2024.

I intervjuundersøkelsen opplyser informasjonssikkerhetsansvarlig at kommunene i Indigo-samarbeidet har som mål å få på plass et felles styringssystem for GDPR (personvernforordningen). Styringssystemet vil i stor grad være relatert til behandlingsprotokoll og antas å være på plass innen sommeren 2024. Med styringssystemet vil man blant annet kunne benytte analyser på tvers av kommuner. Dette opplyses å være rasjonelt og tidsbesparende når behandlingsprotokollen skal utformes eller oppdateres i den enkelte kommune.

Revisors dokumentanalyse viser at Kongsvinger kommune har foretatt en overordnet kritikalitetsvurdering av kommunens datasystemer (Kongsvinger kommune: 2023d, Kongsvinger kommune: 2023j). Dette er blant annet relatert til der stans i systemer kan medføre alvorlige konsekvenser for liv, helse, effektivitet og tillit til kommunen. Alle systemene er rangert på en skala fra 1 til 5, der verdien 1 representerer høyest kritikalitet.

Informasjonssikkerhetsansvarlig forteller overfor revisor i intervju, at det neste trinnet etter kritikalitetsvurderingen, vil være å gå ned i datasystemene og foreta en mer detaljert risikokartlegging av informasjonen som befinner seg i systemene (kritisk, høy, middels og lav verdi etc.). Det blir opplyst at dette arbeidet antas å bli ferdigstilt i løpet av 2024, og at det vil bli utarbeidet tiltaksplaner i de tilfeller hvor risikoen viser seg å være over fastsatt grense.

I intervjuundersøkelsen blir det fra flere respondenter, opplyst at det i Kongsvinger kommune gjennomfører en del vurderinger av personvernkonsekvenser etter personvernforordningen (DPIA). Det blir blant annet tilkjennegitt at kommunen gjennomfører DPIA i forkant av at det tas i bruk nye datasystemer som behandler personopplysninger. Personvernombudet tilkjennegir i intervju overfor revisor, at hun generelt opplever at Kongsvinger kommune er gode til å gjennomføre DPIA.

I revisors dokumentanalyse går det eksempelvis frem at det er gjennomført DPIA for datasystemene «Visma Enterprise Plus» (HR og økonomi), «Spekter» (skole) og «Komp» (helse og mestring) (Kongsvinger kommune: 2023c). I relasjon til vurderingene er det blant annet foretatt analyser av nødvendighet, proporsjonalitet og risiko med tilhørende tiltak.

I intervjuundersøkelsen blir det i alminnelighet tilkjennegitt at Kongsvinger kommune vurderes å ha nødvendige og tilfredsstillende rutiner for å ivareta personvern og sikre informasjonens konfidensialitet, integritet og tilgjengelighet. Det blir samtidig gitt uttrykk for at det alltids vil være mulig å videreutvikle rutinene.

Av revisors dokumentanalyse går det frem at kommunens nevnte styringsdokument for informasjonssikkerhet og personvern, inneholder en rekke rutinebeskrivelser knyttet til håndtering av personopplysninger, herunder innen Datatilsynets anbefalte områder:

- Iverksettelse og opphør av behandling.
- Informasjon (rettferdig og gjennomsiktig behandling, personvernforordningens artikkel 12, 13 og 14).
- Innhenting og kontroll av samtykke (personvernforordningens artikkel 7 og 8).
- Den registrertes rett til innsyn (personvernforordningens artikkel 15).
- Dataportabilitet (personvernforordningens artikkel 20).
- Den registrertes rett til å få korrigert og slettet personopplysninger (personvernforordningens artikkel 16, 17 og 19).
- Begrensning av behandling (personvernforordningens artikkel 18 og 19).
- Den registrertes rett til å protestere (personvernforordningens artikkel 21).
- Særskilte regler for automatiserte avgjørelser (personvernforordningens artikkel 22).
- Utlevering av personopplysninger til andre.
- Overføring til tredjestater (personvernforordningens artikkel 44-49).

Ved siden av rutinebeskrivelsene som inngår i det overordnede styringsdokumentet, er det også utarbeidet flere enkeltstående rutinebeskrivelser knyttet til håndtering av personopplysninger (Kongsvinger kommune: 2023i). Revisors dokumentanalyse viser at dette blant annet relaterer seg til følgende områder:

- Informasjonsplikt ved behandling av personopplysninger.
- Begjæring om innsyn i personopplysninger fra en registrert.
- Retting av helse- og personopplysninger.

Det er utarbeidet en nasjonal norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (normen). Informasjonssikkerhetsansvarlig forteller i intervju overfor revisor, at normen ligger som et bakteppe og brukes ikke bare i kommunens helse- og omsorgssektor, men også i resten av kommunen. I denne forbindelse blir det tilkjennegitt at normen har medvirket generelt i utformingen av Kongsvinger kommunes rutiner innen informasjonssikkerhet og personvern.

Ansvaret for tekniske IKT-løsninger tilligger primært Indigo IKT, men baserer seg samtidig på et samarbeid med eierkommunene. I intervjuundersøkelsen trekker mange respondenter frem at det er etablert forsvarlige løsninger for å ivareta informasjonens konfidensialitet, integritet og tilgjengelighet. Dette gjøres blant annet i form av tilgangsstyring, logging av aktiviteter samt backupløsninger:

- Tilgangsstyringen til Kongsvinger kommunes datasystemer beskrives som god. I kommunen tildeles tilganger av Indigo IKT eller av systemansvarlige i kommunen. Det blir tilkjennegitt at det er et stort fokus på å sikre at ansatte ikke har tilgang til flere funksjoner eller mer informasjon enn hva tjenstlig behov tilsier. Samtidig blir det opplyst at det vektlegges å avslutte tilganger når ansatte slutter eller går over i ny stilling.
- I Kongsvinger kommune loggføres alle aktiviteter i datasystemene og er sporbare på den enkelte bruker. Det blir det tilkjennegitt at mange av systemene krever tofaktorautentisering ved innlogging.
- Indigo IKT tar daglig, ukentlig og månedlig backup av alle systemer og filer på egne servere, foruten at det tas det backup av databaser hver time. Det blir samtidig gitt uttrykk for at kommunen i praksis har noe mindre kontroll over backupløsningene til eksterne skyleverandører, selv om løsningen er regulert i avtaler og vurderes som tilfredsstillende.

Av revisors dokumentanalyse går det frem at Kongsvinger kommune har utarbeidet en rekke rutinebeskrivelser for å ivareta informasjonssikkerhet, herunder informasjonens konfidensialitet, integritet og tilgjengelighet (ibid.). Dette omfatter blant annet rutinebeskrivelser knyttet til:

- IKT-sikkerhet for ansatte i kommunen
- Håndtering av dokumenter med personsensitivt innhold
- Håndtering av passord
- Bruk av e-post og kalender
- Innsyn i e-post
- Bruk av internett og sosiale medier

- Bruk av kommunens bærbare IKT-utstyr
- Behandling av avvik innen informasjonssikkerhet
- Rollebeskrivelser for systemansvarlig og systemeier
- Logging av kommunens datasystemer
- Sikkerhetsrevisjon
- Databehandleravtaler

I intervjuundersøkelsen og av dokumentanalysen går det frem at Kongsvinger kommune har utarbeidet flere nødrutiner (manuelle rutiner) for å sikre kommunens oppgavehåndtering og tjenestetilbud ved utfall av elektroniske datasystemer (Kongsvinger kommune: 2022, Kongsvinger kommune: 2023g). Det er i denne forbindelse blant annet utarbeidet rutinebeskrivelser innen følgende områder:

- Skole og barnehage
- Legevakt
- Hjemmebaserte tjenester
- Institusjonstjenester
- Tilrettelagte tjenester
- Helsestasjon og skolehelsetjeneste
- Økonomisk sosialhjelp
- Drift av kommunale bygg
- Kommunal lønnsutbetaling

I intervjuundersøkelsen beskrives de kommunale nødrutinene som jevnt over tilfredsstillende og dekkende for kommunens kritiske tjenestetilbud m.v.

***

I Kongsvinger kommune er ledelsen ansvarlig for å løpende informere medarbeiderne om nye rutiner eller endringer i rutiner. Alle rutinene er lagret i kommunens kvalitetssystem som de ansatte er gitt tilgang til. En ny funksjon i kvalitetssystemet fra januar 2024, er at dokumenter, herunder rutiner, kan sendes ut til ansatte for lesebekreftelse. I intervjuundersøkelsen beskrives dette som en viktig fremtidig funksjon for å sikre at sentrale dokumenter blir gjort kjent i organisasjonen.

I Kongsvinger kommune får alle nyansatte i henhold til fastsatt prosedyre, utdelt et introduksjonsskjema som blant annet innebære en gjennomgang av arbeidsreglement, etiske retningslinjer, oppgaver og aktuelle rutiner. Etter gjennomgang skal skjemaet signeres av den nyansatte og dennes nærmeste overordnede. Revisors dokumentanalyse viser at introduksjonsskjemaet blant annet inneholder punkter om bruk av IKT og tilgang til datasystemer (Kongsvinger kommune: 2020).

I Kongsvinger kommunes kvalitetssystem er det lagt inn en revisjonsfrist for hver rutine, som gjerne er på 12 måneder. Den revisjonsansvarlige mottar et elektronisk varsel når revisjonsfristen nærmer seg, eventuelt gjentatte varsler dersom fristen ikke overholdes. Når den revisjonsansvarlige foretar justeringer eller endringer i et dokument, skal dette som hovedregel godkjennes av en overordnet (godkjenningsansvarlig). I intervjuundersøkelsen tilkjennegir personvernombudet at hun opplever at kommunen har blitt bedre til å ajourføre rutinene i kvalitetssystemet.

I Kongsvinger kommunens kvalitetssystem er de ansatte gitt mulighet til å melde avvik. Det er i utgangspunktet nærmeste leder som mottar og behandler avvik i kvalitetssystemet, men innmeldte avvik kan eventuelt sendes videre til et høyere ledernivå ved behov. I kvalitetssystemet er det en egen kategori for avvik knyttet til informasjonssikkerhet og personvern. Informasjonssikkerhetsansvarlig tilkjennegir overfor revisor i intervju, at han mottar kopi av avvikene som meldes innen dette området.

Revisors dokumentanalyse viser at kommunen har utarbeidet en egen rutinebeskrivelse for behandling av avvik innen informasjonssikkerhet og personvern (Kongsvinger kommune: 2023a). Rutine-beskrivelsen skal blant annet sikre at alvorlige avvik blir meldt til Datatilsynet.

I intervjuundersøkelsen blir det opplyst at Kongsvinger har etablert en planmessig ordning for å sikre kompetanse innen informasjonssikkerhet og personvern. Fra høsten 2022 har kommunen benyttet nanolæring. Nanolæringen sendes ut på e-post til alle kommunens ansatte hver andre uke og inneholder små fagbolker knyttet til informasjonssikkerhet og personvern. Flere av de som er intervjuet gir uttrykk for at dette er et godt og viktig tiltak for å spre kunnskap i kommuneorganisasjonen.

Kommunedirektørens lederteam[2] fastsatte høsten 2022 at alle kommunens ansatte skulle gjennomføre et modulbasert e-læringskurs fra KINS[3] knyttet til grunnleggende informasjonssikkerhet. Det ble bestemt at ledere skulle gjennomføre alle kursets åtte moduler[4], mens de øvrige ansatte skulle gjennomføre kursets fem første moduler. I intervjuundersøkelsen blir det tilkjennegitt at kurset er faglig

[2] Ved siden av kommunedirektøren består lederteamet av kommunalsjefene, økonomisjefen, samt HR- og organisasjonssjefen.

[3] Foreningen for kommunal informasjonssikkerhet.

[4] Kurset består av følgende moduler i løpende rekkefølge: Grunnleggende informasjonssikkerhet, sikkerhet på mobile enheter, trusler fra IT-kriminelle, fysisk sikkerhet, grunnleggende personvern, utvidet personvern, informasjonssikkerhet for ledere, samt håndtering av sikkerhetshendelser.

godt, men at det har vært vanskelig å få ansatte til å prioritere kurset i en travel hverdag, særlig dersom man arbeider deltid.

Utover ovennevnte forekommer det at kommuneansatte gjennomfører enkeltkurs relatert til informasjonssikkerhet og personvern. Personvernombudet forteller for eksempel overfor revisor, at hun har avholdt noen overordnede kursforedrag for ledere i Kongsvinger kommune. Selv om kommunen i første omgang har valgt å prioritere grunnleggende informasjonssikkerhetskompetanse til alle ansatte, foreligger det også planer om å gjennomføre mer sektorspesifikk opplæring.

I intervjuundersøkelsen blir det tilkjennegitt at kommunedirektørens lederteam, i samarbeid med informasjonssikkerhetsansvarlig og personvernombudet, gjennomfører to årlige dokumenterte gjennomganger av kommunens aktiviteter innen informasjonssikkerhet og personvern. Det blir opplyst at det avholdes et møte i januar/februar og et oppfølgingsmøte på høsten. Kommunalsjef for miljø og samfunnsutvikling tilkjennegir overfor revisor, at han opplever gjennomgangene som nyttige og viktige, noe blant annet dagangrepet i Østre Toten kommune illustrerer.

Revisors dokumentanalyse viser at kommunen har utbeidet rutinebeskrivelser knyttet til hvilke punkter som skal vurderes i lederteamets gjennomgang (Kongsvinger kommune: 2023e, Kongsvinger kommune: 2023h). Dette relaterer seg blant annet til KS sine anbefalte punkter innen området:

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

Av dokumentanalysen går det frem at det er ført skriftlige referater fra møtene der lederteamet har gjennomgått informasjonssikkerhet og personvern (Kongsvinger kommune: 2023f). I referatene er det inntatt status knyttet til de aktuelle punktene, samt eventuelt tilhørende tiltak og frister.

I mange intervjuer blir det gitt uttrykk for at Kongsvinger kommune vurderes å ha et godt fokus på informasjonssikkerhet og personvern. Særlig i løpet av de siste årene oppleves det å ha forekommet bedre rutiner og opplæring, samt en økt bevisstgjøring og forankring i kommuneorganisasjonen,

herunder i toppledelsen. I denne forbindelse pekes det blant annet positivt på arbeidet til personvernombudet og informasjonssikkerhetsansvarlig.

4.3 Revisors vurdering

4.3.1 Samlet risikoanalyse for internkontroll

Revisor anser kriterium nummer 1 som delvis etterlevd. I undersøkelsen går det frem at Kongsvinger kommune har utarbeidet bestemmelser for internkontroll, men ikke en samlet risikoanalyse. Etter hva revisor forstår vil bestemmelsene, fra og med handlingsplanprosessen for 2025, danne basis for årlige overordnede risikovurderinger, herunder innen informasjonssikkerhetsområdet.

Kommunen må ha utarbeidet en samlet risikoanalyse for internkontroll. Analysen bør omfatte informasjonssikkerhetsområdet.

4.3.2 Mål og strategi for informasjonssikkerhet

Etter revisors vurdering er kriterium nummer 2 etterlevd. I Kongsvinger kommunes overordnede styringsdokument for informasjonssikkerhet og personvern, er det gitt en beskrivelse av kommunens mål og strategi for informasjonssikkerhet (sikkerhetsmål og sikkerhetsstrategi).

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

4.3.3 Inndeling av informasjon etter verdinivå

Revisor anser kriterium nummer 3 som delvis etterlevd. I undersøkelsen går det frem at Kongsvinger kommune har gjennomført en overordnet kritikalitetsvurdering av kommunens datasystemer. Kommunen har imidlertid ikke gjennomført en samlet og mer detaljert risikokartlegging av informasjonen som befinner seg i systemene (kritisk, høy, middels og lav verdi etc.). Etter hva revisor forstår planlegges dette arbeidet å bli ferdigstilt i løpet av 2024.

Kommunen må ha gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi.

4.3.4 Informasjonskartlegging – tiltaksplaner

Etter revisors vurdering er kriterium nummer 4 ikke etterlevd på det nåværende tidspunkt. I intervjuundersøkelsen blir det tilkjennegitt at det vil bli utarbeidet tiltaksplaner etter at informasjonskartleggingen i datasystemene er ferdig, det vil si i tilfeller hvor risikoen viser seg å være over fastsatt grense. Revisor legger til grunn at dette vil være en forutsetning for at

informasjonskartleggingen skal ha en sentral nytteverdi. Samtidig er det viktig at kommuneorganisasjonen ansvarliggjøres i form av tydelige tiltaksplaner.

Der informasjonskartleggingen viser at risikoen er over fastsatt grense for hva som er akseptabelt, bør det utarbeides tydelige tiltaksplaner som viser hvem som er ansvarlig for ulike tiltak.

4.3.5 Behandlingsprotokoll

Revisor anser kriterium nummer 5 som delvis etterlevd. Det fremkommer at Kongsvinger kommune har hatt en systembasert oversikt knyttet til IKT-systemer og applikasjoner (systemer), men uten at dette regnes som en fullstendig behandlingsprotokoll etter personvernforordningen. Revisor registrere at en fullstendig behandlingsprotokoll antas å foreligge i løpet av 2024.

Kommunen må føre en behandlingsprotokoll over behandlingsaktivitetene som utføres under kommunens ansvar.

4.3.6 Vurdering av personvernkonsekvenser (DPIA)

Etter revisors vurdering er kriterium nummer 6 etterlevd. Både dokumentanalysen og informasjon fra intervjuer understøtter at Kongsvinger kommune har etablert et tilfredsstillende system for å gjennomføre DPIA. Det fremkommer blant annet at det iverksettes DPIA i forkant av at det tas i bruk nye datasystemer som behandler personopplysninger.

Kommunen må ha et system for å sikre at personvernkonsekvenser (DPIA) vurderes der det er nødvendig.

4.3.7 Rutiner for håndtering av personopplysninger

Revisor anser kriterium nummer 7 som etterlevd, da både dokumentanalysen og informasjon fra intervjuer understøtter at Kongsvinger kommune har utarbeidet nødvendige rutiner innen området. Kommunens overordnede styringsdokument for informasjonssikkerhet og personvern, inneholder blant annet en rekke rutinebeskrivelser knyttet til håndtering av personopplysninger, herunder innen Datatilsynets anbefalte områder.

Kommunen må ha utarbeidet nødvendige rutiner for håndtering av personopplysninger.

4.3.8 Rutiner – konfidensialitet, integritet og tilgjengelighet

Etter revisors vurdering er kriterium nummer 8 etterlevd. Både dokumentanalysen og informasjon fra intervjuer understøtter at Kongsvinger kommune har utarbeidet tilfredsstillende rutiner for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet. Det er blant annet utarbeidet en rekke rutinebeskrivelser samt etablert ordninger for tilgangsstyring, logging av aktiviteter samt backupløsninger.

Kommunen må ha utarbeidet rutiner for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet.

4.3.9 Nødrutiner ved utfall av elektroniske datasystemer

Revisor anser kriterium nummer 9 som etterlevd, da både dokumentanalysen og informasjon fra intervjuer understøtter at Kongsvinger kommune har utarbeidet dekkende nødrutiner for å sikre kommunens kritiske tjenestetilbud ved utfall av elektroniske datasystemer. I denne forbindelse er det utformet en rekke rutinebeskrivelser for ulike tjenesteområder.

Kommunen må ha utarbeidet nødrutiner som skal sikre kommunens tjenestetilbud ved utfall av elektroniske datasystemer.

4.3.10 Bekjentgjørelse av rutiner

Etter revisors vurdering er kriterium nummer 10 etterlevd. Det er etablert et system for å gjøre rutiner kjent, da alle rutiner er lagret i kommunens kvalitetssystem som de ansatte er gitt tilgang til. Samtidig er ledelsen ansvarlig for å løpende informere medarbeiderne om rutiner eller endringer i rutiner. Et introduksjonsskjema for nyansatte skal videre sikre at blant annet sentrale rutiner gjennomgås ved arbeidsoppstart.

En ny funksjon i kvalitetssystemet fra januar 2024, er at dokumenter, herunder rutiner, kan sendes ut til ansatte for lesebekreftelse. Revisor anser dette som en viktig funksjon for å sikre en systematisk tilnærming innen området.

Kommunen må ha et system som sørger for at rutinene gjøres kjent blant de ansatte.

4.3.11 Evaluering og ajourføring av rutiner

Revisor anser kriterium nummer 11 som etterlevd. I Kongsvinger kommunes kvalitetssystem er det lagt inn en revisjonsfrist for hver rutine, som skal sørge for at rutinen blir evaluert og ajourført. Den revisjonsansvarlige mottar et elektronisk varsel når revisjonsfristen nærmer seg, eventuelt gjentatte varsler dersom fristen ikke overholdes. Når den revisjonsansvarlige foretar justeringer eller endringer i et dokument, skal dette som hovedregel godkjennes av en overordnet (godkjenningsansvarlig).

Kommunen må ha et system som sørger for at rutinene evalueres og ajourføres.

4.3.12 System for avvikshåndtering

Etter revisors vurdering er kriterium nummer 12 etterlevd. I Kongsvinger kommunes kvalitetssystem er de ansatte gitt mulighet til å melde avvik. Det er i utgangspunktet nærmeste leder som mottar og behandler avvik i kvalitetssystemet, men innmeldte avvik kan eventuelt sendes videre til et høyere ledernivå ved behov. I kvalitetssystemet er det en egen kategori for avvik knyttet til informasjonssikkerhet og personvern.

Kommunen må ha etablert et system for å rapportere og følge opp avvik, herunder eventuelle avvik knyttet til informasjonssikkerhet.

4.3.13 System for kompetanse innen informasjonssikkerhet

Revisor anser kriterium nummer 13 som etterlevd, da Kongsvinger kommune har etablert en planmessig ordning for å sikre kompetanse innen informasjonssikkerhet og personvern. I første omgang har kommunen valgt å prioritere grunnleggende informasjonssikkerhetskompetanse til alle ansatte, det vil si i form av nanolæring på e-post og et modulbasert e-læringskurs, men det foreligger også planer om å gjennomføre mer sektorspesifikk opplæring.

Kommunen må ha en planmessig ordning for å sikre kompetanse innen informasjons-sikkerhetsområdet.

4.3.14 Gjennomgang av informasjonssikkerhet i kommuneledelsen

Etter revisors vurdering er kriterium nummer 14 etterlevd. I undersøkelsen går det frem at kommunedirektørens lederteam, i samarbeid med informasjonssikkerhetsansvarlig og personvern-ombudet, gjennomfører to årlige dokumenterte gjennomganger av kommunens aktiviteter innen informasjonssikkerhet og personvern.

Informasjon fra intervjuer indikerer at det i løpet av de siste årene har forekommet en positiv utvikling i kommunens informasjonssikkerhetsarbeid, herunder økt bevisstgjøring og forankring i kommune-organisasjonen med toppledelse.

Kommunens ledelse bør minst en gang i året, foreta en dokumentert gjennomgang av kommunens aktiviteter innen informasjonssikkerhetsområdet.

5 Konklusjon

Med bakgrunn i vurderingene som er foretatt i relasjon til problemstillingen, er revisors konklusjon at Kongsvinger kommune har etterlevd de fastsatte revisjonskriteriene på en jevnt over tilfredsstillende måte. Selv om kommunen i hovedsak vurderes å ha et tilfredsstillende system for å sikre god informasjonssikkerhet, herunder en positiv utvikling innen området, foreligger det noen forbedringspunkter som danner grunnlag for revisors anbefalinger. Dette er relatert til forhold som risikoanalyse for internkontroll, risikokartlegging av informasjon i datasystemer, samt utarbeidelse av fullstendig behandlingsprotokoll etter personvernforordningen.

6 Anbefalinger

Med bakgrunn i den gjennomførte forvaltningsrevisjonen fremmer revisor følgende anbefalinger:

- Kommunen bør sikre at det utarbeides en samlet risikoanalyse for internkontroll i kommunen.
- Kommunen bør sikre at det gjennomføres en mer detaljert risikokartlegging av informasjonen som befinner seg i datasystemene (kritisk, høy, middels og lav verdi). Der informasjons-kartleggingen viser at risikoen er over fastsatt grense for hva som er akseptabelt, bør det utarbeides tydelige tiltaksplaner som viser hvem som er ansvarlig for ulike tiltak.
- Kommunen bør sikre at det utarbeides en fullstendig behandlingsprotokoll etter personvernforordningen.

7 Kommunedirektørens uttalelse til rapporten

Den 12. januar 2024 mottok revisor kommunedirektørens uttalelse til forvaltningsrevisjonsrapporten.

Uttalelsen gjengis i det følgende.

***

Kommunedirektørens syn på foreløpig forvaltningsrevisjonsrapport:

Rapporten fremgår som tydelig og grundig, der de identifiserte funnene er klare og forståelige.

Det er ingen grunn til å betvile funnene, og vi er enige om at status i kommunen er som identifisert.

Denne rapporten peker på viktige områder som kommunen til dels var klar over og der en del tiltak allerede er / delvis er iverksatt (samt er under arbeide.)
Vi anser rapporten som en god pekepinn på retningen vi må jobbe mot.

Det vil ila året 2024 være hovedfokus på å fullføre disse tiltakene:

1. Gjennomføre en samlet risikoanalyse for internkontroll i kommunen.

    - Kommunenes arbeid med internkontroll er regulert i kommunelovens §25, punkt c, og presiserer at kommunedirektøren har ansvar for å «avdekke og følge opp avvik og risiko for avvik» i organisasjonen.
      Kongsvinger kommune har på bakgrunn av dette i løpet av 2023 utarbeidet egne bestemmelser for internkontroll som vil være førende for hele organisasjonen. I bestemmelsenes kap. 1.7.2 er det redegjort for krav til risikovurderinger, og her er det fastsatt at det årlig i forbindelse med planprosessen skal gjennomføres overordnede risikovurderinger knyttet til virksomhetens overordnede mål.
      Ikt og sikkerhet er et område som er områdeovergripende hvor kommunen må ha overordnede mål, og det er derfor naturlig at dette området vil være en del av en slik overordnet risikoanalyse. Bestemmelsene trådte i kraft med virkning fra 29.08.23, og en overordnet risikoanalyse vil derfor første gang bli utarbeidet som en del av handlingsplanarbeidet for 2025.

2. Kartlegge og identifisere bruk av personopplysninger i kommunens datasystem, samt kategorisere verdien på disse (kritisk, høy, middels og lav verdi.)

    - Dette arbeidet er noe avhengig av pkt 3, behandlingsprotokoll.

3. Få på plass fullstendig behandlingsprotokoll (så godt som mulig, da dette er et levende dokument, og vil være objekt for stadig endringer.) Men dette arbeidet ble påbegynt i 2023, med mål om å være ferdig ila 2024. Så her er vi i god gang.

Utover punktene ovenfor vil det selvsagt jobbes kontinuerlig med å forbedre og sikre kommunens informasjonssikkerhet og personvern for de registrerte (og kommunen.)

I 2024 vil det anskaffes ett nytt felles system for GDPR, som vil forenkle samt gi en bedre oversikt over tilstanden i kommunens arbeide med informasjonssikkerhet og personvern.

Det vil være fortsatt fokus på at alle ansatte skal gjennomføre sikkerhetskurs, delta i kampanjer og annen opplæring.

Også arbeidet med internkontroll er satt høyt på dagsorden, og vil gis en ekstra høy prioritet inneværende år. Og som del av dette tas det i bruk ett nytt Kvalitetssystem, nå i januar 2024.

Mvh

Kommunedirektør i Kongsvinger kommune

Lars A. Uglem

8 Referanser

Andersen, Jon Aarum (1995): *Ledelse og ledelsesteorier. Om hvilke svar ledelsesforskningen kan gi*. Oslo: Bedriftsøkonomens forlag.

Bryman, Alan (2004): *Social research methods*. 2. utgave. Oxford: Oxford University Press.

COSO (2005): *Helhetlig risikostyring – et integrert rammeverk.* Oslo: Norges Interne Revisorers Forening.

Dahler-Larsen, Peter (2002): *At fremstille kvalitative data*. Odense: Odense universitetsforlag.

Datatilsynet (2018): *Veileder. Informasjonssikkerhet og internkontroll.*

Digitaliseringsdirektoratet (2020): *Veileder i kompetanse- og kulturutvikling innen digital sikkerhet.*

Direktoratet for e-helse (2022): *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.*

Direktoratet for forvaltning og IKT (2016): *Internkontroll i praksis – informasjonssikkerhet. Grunnleggende innføring.*

eForvaltningsforskriften (2004).

Eriksen, Frits A., Ole Kr. Rogndokken og Stein Ove Songstad (2000): *Veileder forvaltningsrevisjon*. Oslo: NKRF.

Holme, Idar Magne og Bernt Krohn Solvang (1996): *Metodevalg og metodebruk*. 3. utgave. Oslo: Tano.

Jacobsen, Dag Ingvar (2005): *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. 2. utgave. Kristiansand: Høyskoleforlaget.

Kommunal- og moderniseringsdepartementet (2021): *Veileder. Internkontroll i kommunesektoren. Kravene i kommuneloven.*

Kommuneloven (2018).

Kongsvinger kommune (2020): *Introduksjon for nye medarbeidere.*

Kongsvinger kommune (2022): *Nødrutiner ved bortfall av IKT-systemer.*

Kongsvinger kommune (2023a): *Behandling av avvik innen området informasjonssikkerhet.*

Kongsvinger kommune (2023b): *Bestemmelser for internkontroll i Kongsvinger kommune.*

Kongsvinger kommune (2023c): *DPIA.*

Kongsvinger kommune (2023d): *Kartlegge og klassifisere systemer.*

Kongsvinger kommune (2023e): *Ledelsens gjennomgang av informasjonssikkerheten.*

Kongsvinger kommune (2023f): *Ledelsens gjennomgang – referat og tiltaksliste.*

Kongsvinger kommune (2023g): *Manuelle rutiner (frafall IKT).*

Kongsvinger kommune (2023h): *Overordnet styringsdokument for informasjonssikkerhet og personvern.*

Kongsvinger kommune (2023i): *Styringssystem – styrende dokumenter, gjennomførende dokumenter, kontrollerende dokumenter.*

Kongsvinger kommune (2023j): *Systemoversikt – Kongsvinger kommune.*

KS (2020): *Orden i eget hus. Kommunedirektørens internkontroll.*

KS (2022a): *Hovedtariffavtalen (2022 – 2024)*. Oslo: Kommuneforlaget.

KS (2022b): *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet.*

Larsen, Ann Kristin (2007): *En enklere metode. Veiledning i samfunnsvitenskapelig forskningsmetode*. Bergen: Fagbokforlaget.

Nasjonal sikkerhetsmyndighet (2020): *Grunnprinsipper for IKT-sikkerhet.*

NKRF (2020): *RSK 001. Standard for forvaltningsrevisjon*. Oslo: NKRF.

Personvernforordningen (2018).

Ryen, Anne (2002): *Det kvalitative intervjuet. Fra vitenskapsteori til feltarbeid*. Bergen: Fagbokforlaget.

Standard Norge (2017): *Ledelsessystemer for informasjonssikkerhet – ISO/IEC 27001.*

Thagaard, Tove (1998): *Systematikk og innlevelse*. Bergen: Fagbokforlaget

Vedlegg A: Revisjonskriterier

I det følgende utledes det revisjonskriterier for problemstillingen, som igjen oppsummeres i kortpunkter. Disse kortpunktene er videre inntatt i selve rapporten, og revisors vurderinger og konklusjoner bygges rundt disse punktene.

Innledende om kommunens internkontroll – samlet risikoanalyse

Av § 25-1 første ledd i kommuneloven (2018) går det frem at kommunen skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Dette forutsetter at det er etablert en tilstrekkelig internkontroll i hele kommunens organisasjon, herunder i forbindelse med informasjonssikkerhetsområdet[5]. Internkontrollen kan også kan omfatte andre mål enn direkte oppfølging av lovpålagte krav, så som læring i organisasjoner og en effektiv og målrettet forvaltning og tjenesteproduksjon/-kvalitet (Kommunal- og moderniseringsdepartementet: 2021). Den nevnte bestemmelsen fastsetter at det er kommunedirektøren som er ansvarlig for internkontrollen i kommunen.

Etter kommuneloven § 25-1 annet ledd skal internkontrollen være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risiko, noe som også understøttes av anerkjente prinsipper for internkontroll (COSO: 2005). Følgelig er det sentralt at innretning og omfang på internkontrollen er egnet til å sikre etterlevelse av lover og forskrifter, samt innfrielse av kommunale mål.

Risikovurderinger er sentralt etter kommuneloven § 25-1 annet ledd og kommunen må foreta en konkret analyse og vurdering av sannsynligheten for at lover og forskrifter ikke følges, og hvilke konsekvenser dette i så fall kan få (Kommunal- og moderniseringsdepartementet: 2021). Det tilsvarende vil gjelde for øvrige kommunale mål.

En samlet risikoanalyse vil til dels bero på mer generelle vurderinger, som at noen tjenester, saksfelt eller sektorer generelt har en større risiko, og til dels vil dette være mer konkrete vurderinger av forholdene i den enkelte kommunen. Vurderingene må gjøres både samlet for kommunen som helhet og innenfor de enkelte delene av kommunens virksomhet (ibid.).

[5] Informasjonssikkerhet kan omfatte både digital, papirbasert og muntlig behandling av informasjon. Denne forvaltningsrevisjonen er primært avgrenset til digital behandling av informasjon, nærmere bestemt digital sikkerhet. Personvern inngår som en del av informasjonssikkerheten.

Ansvaret for tekniske IKT-løsninger, så som sikkerhetskopiering og brannmur, tilligger primært Indigo IKT IKS og er ikke direkte omfattet av forvaltningsrevisjonen. Det settes imidlertid fokus på hvordan Kongsvinger kommune håndterer informasjonssikkerheten innenfor løsningene, eksempelvis i form av rutiner og opplæring.

Revisor legger til grunn at kommunens risikoanalyse for internkontroll bør omfatte informasjonssikkerhetsområdet, da kommunen er avhengig av IKT-tjenester for å fungere i det daglige, foruten at området også er forbundet med betydelige personvernhensyn. Innretningen på kommunens internkontrolltiltak må igjen bygge på den samlede risikoanalysen for internkontroll.

Rutiner, kompetanse og system for avvikshåndtering

Det er i tråd med allment aksepterte ledelsesprinsipper at en leder for en virksomhet etablerer rutiner og systemer som blant annet skal bidra til å sikre at organisasjonen når de mål som er satt. I følge anerkjente normer for internkontroll, slik som COSO-rammeverket (2005), medvirker rutiner og systemer til gjennomføring av virksomhetens mål. Dette ved at aktiviteter og oppgaver blir systematisert og formalisert.

Av kommuneloven § 25-1 tredje ledd bokstav b, går det frem at kommunen skal etablere nødvendige rutiner i arbeidet. Som en del av internkontrollen må virksomheten sørge for at rutinene gjøres kjent blant de ansatte (Kommunal- og moderniseringsdepartementet: 2021). I denne forbindelse bør de ansatte eksempelvis gis innsikt i sikkerhetsprosedyrer og riktig bruk av datasystemer (Datatilsynet: 2018, Digitaliseringsdirektoratet: 2020). For å sikre at rutinene fungerer etter hensikten, må rutinene evalueres og ajourføres, jf. kommuneloven § 25-1 tredje ledd bokstav e.

En side ved internkontrollen vil være å sikre at kommunen besitter nødvendig kompetanse i arbeidet, herunder i forbindelse med informasjonssikkerhet (KS: 2020). At organisasjonen og de ansatte innehar tilstrekkelig kompetanse, samt at det tilbys mulighet for oppdatering, vil normalt ha betydning for kvaliteten på arbeidsoppgavene som utføres. Med dette som bakgrunn vil det være et strategisk ledelsesansvar å veie kommunens kompetansebehov opp mot kostnad (COSO: 2005).

Hovedtariffavtalen for KS-området inneholder i punkt 3.3, flere bestemmelser om kompetanse og kompetanseutvikling (KS: 2022a). I avtalen heter det at kompetanseområdet har stor betydning for den enkelte ansatte, kommunen og samfunnet som helhet. Hovedtariffavtalen understreker viktigheten av at kommunen arbeider målrettet og planmessig med opplæring og utvikling av arbeidstakerne gjennom interne og/eller eksterne tiltak.

Internkontrollen skal videre avdekke og følge opp konkrete avvik, jf. kommuneloven § 25-1 tredje ledd bokstav c. I følge COSO (2005) vil et siktemål med internkontroll være å fokusere på om aktiviteter leveres i tråd med fastsatte mål og intensjoner. Det bør derfor være etablert kanaler som sikrer at nødvendig informasjon blir mottatt og fulgt opp. Dette inkluderer iverksettelse av eventuell avvikshåndtering.

Sikkerhetsmål og sikkerhetsstrategi

I § 15 første ledd i eForvaltningsforskriften (2004) stilles det krav om at offentlige forvaltningsorgan, herunder kommuner, skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten. Dette benevnes som sikkerhetsmål og sikkerhetsstrategi og skal danne grunnlaget for forvaltningsorganets internkontroll, eksempelvis rutiner, innen informasjonssikkerhetsområdet.

En side ved internkontrollen er også å besitte nødrutiner som skal sikre kommunens tjenestetilbud ved utfall av elektroniske datasystemer.

Konfidensialitet, integritet og tilgjengelighet

Behandling av informasjon er både en kjerneaktivitet og en viktig støtteaktivitet i norske kommuner (Direktoratet for forvaltning og IKT: 2016). Effektiv og pålitelig informasjonsbehandling er avgjørende for at virksomheten skal nå sine mål. Informasjonssikkerhet knytter seg til å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte (Datatilsynet: 2018). Dette omfatter å sikre:

- Konfidensialitet – at informasjonen ikke blir kjent for uvedkommende.
- Integritet – at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
- Tilgjengelighet – at informasjonen er tilgjengelig for autoriserte ved behov.

Brudd på konfidensialitet, integritet eller tilgjengelighet kan få konsekvenser for både virksomheten selv, innbyggerne og andre offentlige og private virksomheter (Direktoratet for forvaltning og IKT: 2016). Det kan for eksempel medføre:

- Feil beslutninger.
- Brudd på rettigheter og rettssikkerhet.
- Omdømmetap og økonomiske tap for innbyggere, næringsliv og virksomheten selv.
- Ødeleggende livssituasjon.
- Effektivitetstap for virksomheten selv og andre.
- Tap av liv og helse.

De ovennevnte prinsippene om konfidensialitet, integritet og tilgjengelighet understøttes også av norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Direktoratet for e-helse: 2022). Selv om normen 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 forøvrig 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. tjenstlig behov.
- 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.
- Sikre at opplysninger er korrekte og nødvendig relaterte og forhindre at kopier blir en kilde til utdatert informasjon.

Virksomheten skal etter normen 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 tjenstlig behov.
- Sikre forsvarlig og stabil drift i alle datasystemer.
- Sikre at det foretas egnede tiltak for å sikre forebygging, oppdagelse, håndtering og gjenoppretting av informasjon.

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 blant annet gjennom:

- Et etablert tilgangsstyringssystem.
- Programvare som loggfører aktivitet og endring av informasjon.
- Klare risiko- og vesentlighetsanalyser for bruk av alle programmer.

Personvernforordningen m.v.

Artikkel 24 i personvernforordningen (2018) stiller krav til internkontroll i form av egnede tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen. Dette innebærer en forholdsmessighet hvor en ser på behandlingens art, omfang, formål og sammenheng, samt risikoene for fysiske personers rettigheter og friheter, og ut fra det gjennomfører egnede tiltak. Ved innføring av internkontroll bør virksomheten først identifisere hvilke personopplysninger som behandles, og deretter gjennomføre en risikovurdering for å avklare føringer for internkontrollen (Datatilsynet: 2018). Dette som en del av internkontrollens styrende elementer, hvilket igjen vil gi grunnlag for å utarbeide de rutinene det er behov for.

Internkontrollens gjennomførende elementer inneholder rutinene som skal brukes av de ansatte i deres arbeidssituasjon. Virksomheten må utarbeide de nødvendige rutinene for at behandlingen skal gjennomføres i forsvarlige former. Datatilsynet (2018) anfører at det kan være hensiktsmessig å utarbeide rutiner innen følgende områder for håndtering av personopplysninger:

- Iverksettelse og opphør av behandling.
- Informasjon (rettferdig og gjennomsiktig behandling, personvernforordningens artikkel 12, 13 og 14).
- Innhenting og kontroll av samtykke (personvernforordningens artikkel 7 og 8).
- Den registrertes rett til innsyn (personvernforordningens artikkel 15).
- Dataportabilitet (personvernforordningens artikkel 20).
- Den registrertes rett til å få korrigert og slettet personopplysninger (personvernforordningens artikkel 16, 17 og 19).
- Begrensning av behandling (personvernforordningens artikkel 18 og 19).
- Den registrertes rett til å protestere (personvernforordningens artikkel 21).
- Særskilte regler for automatiserte avgjørelser (personvernforordningens artikkel 22).
- Utlevering av personopplysninger til andre.
- Overføring til tredjestater (personvernforordningens artikkel 44-49).

***

Alle virksomheter som behandler personopplysninger, skal føre en behandlingsprotokoll over behandlingsaktivitetene[6] de har ansvaret for, jf. personvernforordningens artikkel 30. En applikasjons- og IKT-systemoversikt er blant annet nødvendig for å kunne utarbeide en fullstendig behandlingsprotokoll.

Der det er nødvendig, skal kommunen vurdere personvernkonsekvensene (DPIA[7]) ved behandlingen og eventuelt kontakte Datatilsynet for forhåndsdrøftelse ved høy risiko for de registrertes rettigheter og friheter, jf. personvernforordningens artikkel 35 og 36. I en slik vurdering skal det blant annet vurderes om den beskrevne behandlingen av personopplysninger er nødvendig og proporsjonal. Videre skal vurderingen bidra til å håndtere risikoen som behandlingen medfører.

Inndeling av informasjon etter verdinivå

Kommunesektorens organisasjon (KS) gav i januar 2022 ut en veileder knyttet til informasjonssikkerhet, herunder personvern (KS: 2022b). Dokumentet er utarbeidet av KPMG og skal fungere som en verktøykasse for kommunene innen tematikken. Her står det blant annet følgende:

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

Dokumentet inneholder en rekke anbefalinger til hvordan kommunedirektøren best kan ha kontroll med kravene til informasjonssikkerhet, herunder 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 KPMG viser til er ikke en mal, men et eksempel på hvordan dette kan gjøres. KPMG 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
  - Informasjon som vil være ødeleggende for funksjoner og tjenester som er kritisk for daglig drift (for eksempel strategidokumenter, eksamener/tentamener, informasjons-system for lønnsutbetaling).

[6] Behandlingsaktiviteter utgjør enhver operasjon eller rekke av operasjoner/prosesser som gjøres med personopplysninger, herunder innsamling, registrering, sammenstilling, vurdering, strukturering, lagring, endring, bruk, utlevering og sletting.

[7] Data Protection Impact Assessment.

- 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).

KPMG tilkjennegir 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.

Kommuneledelsens rolle – informasjonssikkerhet

Av ovennevnte går det frem at det er kommunedirektøren som er ansvarlig for internkontrollen i kommunen. Nasjonal sikkerhetsmyndighet (2020) tilkjennegir samtidig at det er avgjørende at toppledelsen tar eierskap og involverer seg i virksomhetens sikkerhetsarbeid.

Ledelsesansvaret og forankringen knyttet til informasjonssikkerhet, herunder personvern, er tydelig i ISO/IEC-standard 27001 (Standard Norge: 2017). Dette understøttes også av veiledere fra Digitaliseringsdirektoratet (2020) og KS (2022b). I KS sin veileder fremkommer blant annet følgende:

> «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».

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

Det kan ut ifra KS sin veileder, forventes at ledelsens gjennomgang omfatter:

- Orientering om relevante endringer innen rettsområdet.
- Orientering om risiko- og trusselbildet for informasjonssikkerhet og personvern.
- Gjennomgang av vesentlige og/eller alvorlige avviksaker i kommunen siden forrige gjennomgang, herunder hvordan disse er håndtert og fulgt opp.
- Gjennomgang av behandlingsaktivitetene.

- Overordnet gjennomgang av endringer i risikovurderinger og tiltak som er innført.
- Gjennomgang av oppfølgingen av leverandører.

***

Oppsummerte revisjonskriterier for problemstillingen

1. Kommunen må ha utarbeidet en samlet risikoanalyse for internkontroll. Analysen bør omfatte informasjonssikkerhetsområdet.
2. Kommunen må ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).
3. Kommunen må ha gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi.
4. Der informasjonskartleggingen viser at risikoen er over fastsatt grense for hva som er akseptabelt, bør det utarbeides tydelige tiltaksplaner som viser hvem som er ansvarlig for ulike tiltak.
5. Kommunen må føre en behandlingsprotokoll over behandlingsaktivitetene som utføres under kommunens ansvar.
6. Kommunen må ha et system for å sikre at personvernkonsekvenser (DPIA) vurderes der det er nødvendig.
7. Kommunen må ha utarbeidet nødvendige rutiner for håndtering av personopplysninger.
8. Kommunen må ha utarbeidet rutiner for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet.
9. Kommunen må ha utarbeidet nødrutiner som skal sikre kommunens tjenestetilbud ved utfall av elektroniske datasystemer.
10. Kommunen må ha et system som sørger for at rutinene gjøres kjent blant de ansatte.
11. Kommunen må ha et system som sørger for at rutinene evalueres og ajourføres.
12. Kommunen må ha etablert et system for å rapportere og følge opp avvik, herunder eventuelle avvik knyttet til informasjonssikkerhet.
13. Kommunen må ha en planmessig ordning for å sikre kompetanse innen informasjons-sikkerhetsområdet.
14. Kommunens ledelse bør minst en gang i året, foreta en dokumentert gjennomgang av kommunens aktiviteter innen informasjonssikkerhetsområdet.

Vedlegg B: Relabilitet og validitet

Reliabilitet og validitet er sentrale begreper i kvalitetssikringen av undersøkelser. I det følgende angis sider ved undersøkelsens reliabilitet og validitet.

Reliabilitet

En undersøkelses reliabilitet bestemmes av hvordan målingene er gjort og hvor nøyaktig en er i den videre behandlingen av dataene (Holme og Solvang: 1996). For å sikre at respondentene «kjenner seg igjen» i de nedtegnede intervjudataene forelegges de sine respektive intervjureferater til verifisering.

Jacobsen (2005) fremhever at respondentene kan bli utsatt for en undersøkelseseffekt. Det er ikke uvanlig at en undersøkelsessituasjon kan oppfattes som kunstig og unaturlig. Dette kan få intervjuobjektene til å opptre noe annerledes enn de ellers ville ha gjort. Enkelte kan for eksempel bli reserverte med å svare på kritiske spørsmål. Som et ledd i å forhindre noe av dette, forsøkes det i størst mulig grad å behandle respondentene anonymt.

For at intervjusituasjonen skal oppleves så naturlig som mulig vektlegges det at intervjuene skal foregå i rolige omgivelser og at respondentene skal få snakke relativt fritt. En fordel med de kvalitative intervjuene er nettopp muligheten til å snakke relativt fritt. Imidlertid er det nødvendig med en viss struktur på intervjuene. Derfor utvikles det en intervjuguide med de sentrale temaene og spørsmålene for undersøkelsen. På denne måten unngås det i større grad at sentrale spørsmål kan utebli, foruten at det også forenkler analysearbeidet. Når det stilles spørsmål om bestemte temaer, blir det enklere å kategorisere og tolke dataene ut ifra dette. Hvilke spørsmål som stilles til hver enkelt respondent vil imidlertid variere noe. Dette kommer av deres ulike posisjoner og roller (jf. punkt 3.2). Fleksibilitet er som Thagaard (1998) fremhever, viktig for å knytte spørsmålene til den enkelte respondents forutsetninger.

Videre har det vært fokus på å sikre at rapportens innhold stemmer overens med mottatte opplysninger og innhentede dokumenter. Derfor har forvaltningsrevisjonsrapporten blitt underlagt intern kvalitetssikring i henhold til Revisjon Øst IKS sine rutiner for intern kvalitetskontroll av forvaltningsrevisjonsprosjekter. Rapportens grunnlag har i denne forbindelse blitt kontrollert flere ganger.

Validitet

Validiteten sier noe om hvor gyldige eller relevante dataene er for det en søker å undersøke (Eriksen m.fl.: 2000).

En fordel med den kvalitative intervjuundersøkelsen er at den sikrer høy begrepsvaliditet, hvilket omhandler at en faktisk måler det en søker å måle. Det er nemlig intervjuobjektene som i stor grad definerer hva som er den «riktige» forståelsen av fenomenet (Jacobsen: 2005). Ved å stille utdypende spørsmål kan man således styrke muligheten for å avklare eventuelle misforståelser (Larsen: 2007). For å forenkle analyse- og kategoriseringsarbeidet har det imidlertid blitt valgt å strukturere intervjuene noe (jf. ovennevnte punkt om reliabilitet). Intervjuene «flyter således ikke helt fritt».

Selv om det kvalitative intervjuet er egnet til å sikre høy begrepsvaliditet er det ikke like egnet til generalisering. Den kvalitative metoden vektlegger detaljer, nyanserikdom og det unike ved hver enkelt respondent (Jacobsen: 2005). En styrke ved metoden er at den er egnet til å oppnå nærhet og dybde på et avgrenset område (Ryen: 2002). Metoden kan være egnet til å undersøke komplekse problemer (Dahler-Larsen: 2002). En svakhet med metoden er imidlertid at den kan være lite egnet til generalisering. Ofte deltar det kun et fåtall personer i kvalitative intervjuundersøkelser. Gjennomføring av intervjuer er nemlig en omfattende og tidkrevende prosess. En konsekvens er at det kan bli problemer med representativiteten og dermed også muligheten til å generalisere (Bryman: 2004). Den angitte dokumentanalysen (jf. punkt 3.2) søker å supplere intervjudataene ved å fremskaffe et mer skriftlig underlag for deler av undersøkelsen, herunder undersøke dokumenter som er felles for hele kommuneorganisasjonen.

For å styrke undersøkelsens validitet har det videre blitt trukket inn sentral litteratur og regelverk som berører forvaltningsrevisjonens problemområde, noe som vil bidra til at det gis større visshet om at undersøkelsen og funnene er relevante.