

Plan for forvaltningsrevisjon og eierskapskontroll: IKT-sikkerhet i kommunen

Rendalen kommune – Forslag til innretning på
forvaltningsrevisjon

5. september 2025 KPMG

Innhold

1	Innledning	3
1.1	Bakgrunn	3
1.2	Beskrivelse fra plan for forvaltningsrevisjon	3
1.3	Bakgrunn	3
1.4	Møte med kommunedirektør	4
2	Formål, problemstillinger og revisjonskriterier	5
2.1	Formål	5
2.2	Problemstillinger	5
2.3	Revisjonskriterier	5
3	Tilnærming	7
3.1	Metode	7
3.2	Aktivitets- og framdriftsplan	8
4	Prosjektteam og honorar	9
4.1	Prosjektteam	9
4.2	Honorar	9

1 Innledning

1.1 Bakgrunn

Kontrollutvalget i Rendalen bestilte i sak 21/25 02.06.2025 forvaltningsrevisjon for prosjekt nummer 1 og 2 i plan for forvaltningsrevisjon og eierskapskontroll for 2024 – 2028. Kontrollutvalget gjorde følgende vedtak:

1. *Kontrollutvalget viser til plan for forvaltningsrevisjon 2024 - 2028 og bestiller forvaltningsrevisjoner av "IKT-sikkerhet i kommunen og håndtering av GDPR" og "Skolens læringsmiljø og tilpasset undervisning" for gjennomføring i 2025 og 2026.*
2. *Prosjektplan med ressursramme og tidspunkt for ferdig rapport oversendes kontrollutvalgets sekretariat innen 1. september 2025 og legges fram i kontrollutvalgets møte 15. september 2025*

Denne prosjektplanen svarer ut bestillingen for prosjektet «IKT-sikkerhet i kommunen og håndtering av GDPR». Prosjektet er avgrenset til IKT-sikkerhet og håndtering av GDPR i kommunen.

1.2 Beskrivelse fra plan for forvaltningsrevisjon

I forvaltningsrevisjonen fra 2023 om IKT-sikkerhet i IKT Fjellregionen IKS, fremkommer det at det ligger et større potensiale i å utvikle sikkerhetsarbeidet i kommunene, bygge bedre sikkerhetskultur og øke bevisstheten blant ansatte. Det kan være risiko knyttet til kommunens samhandling med FARTT i det interkommunale samarbeidet, og innen det som er kommunens ansvarsområder. Det gjelder særlig innen sikkerhet og personvern, og er spesielt knyttet til tilgang og avgang av personell. Det er også et spørsmål om ansvarsområdene mot FARTT er godt nok avklart. Et eksempel er de mange programmene som skolen bruker, hva som skal prioriteres og hvordan dette skal innføres. Dette har også sammenheng med ulike interesser i det interkommunale samarbeidet, og det kreves at kommunen har gode rutiner for sine side krav til prioriteringer. En forvaltningsrevisjon av informasjonssikkerhet i FARTT ble gjennomført i 2023, og kan ligge til grunn for arbeidet.

Mulige innfallsvinkler:

- Er det en tydelig rolle- og ansvarsfordeling mellom FARTT og kommunen, og blir dette fulgt?
- Følger kommunen opp sine ansvarsområder i samarbeidet med FARTT på en slik måte at sikkerhet og personvern ivaretas?
- Har kommunene etablert tiltak for å ivareta kravene i personopplysningsloven?

1.3 Bakgrunn

I forvaltningsrevisjonen fra 2023 om IKT-sikkerhet i IKT Fjellregionen IKS ble det avdekket et betydelig potensial for forbedring i kommunenes sikkerhetsarbeid. Det ble særlig pekt på behovet for bedre sikkerhetskultur og økt bevissthet blant ansatte. Rendalen kommune har selv uttrykt bekymring knyttet til:

- Uklar rolle- og ansvarsfordeling mellom kommunen og FARTT.
- Risiko ved tilgang og avgang av personell.
- Manglende rutiner for prioritering og innføring av digitale verktøy, spesielt i skolesektoren.
- Ulike interesser i det interkommunale samarbeidet som kan påvirke sikkerhetsarbeidet.

Disse forholdene tilsier behov for en systematisk gjennomgang av kommunens praksis og rutiner.

1.4 Møte med kommunedirektør

Forvaltningsrevisor gjennomførte 18.08.2025 et møte med kommunedirektøren i Rendalen kommune. Kommunedirektøren viste i møtet til at IKT-sikkerhet er et viktig område å undersøke, men at området ellers er mindre pressende enn psykososialt skolemiljø per tid. Det er avtalt med kommunedirektør å følge opp en eventuell bestilling med administrasjonen for å sikre at den skal være så relevant som mulig inn i kommunens utviklings- og forbedringsarbeid

2 Formål, problemstillinger og revisjonskriterier

2.1 Formål

Formålet med revisjonen er å undersøke hvordan Rendalen kommune ivaretar kravene til informasjonssikkerhet og personvern, herunder etterlevelse av personopplysningsloven (GDPR), i sin samhandling med FARTT og i egne ansvarsområder. Revisjonen skal bidra til å identifisere forbedringsområder og gi anbefalinger for styrket sikkerhetskultur og rutiner.

2.2 Problemstillinger

På bakgrunn av formålet blir følgende problemstillinger foreslått:

- Hvordan praktiseres ansvarsdelingen mellom FARTT og Rendalen kommune i det daglige arbeidet med informasjonssikkerhet og personvern?**
 - Utforsker om det finnes klare retningslinjer og om disse følges i praksis.
- I hvilken grad har kommunen etablert rutiner som sikrer kontroll ved tilgang og avslutning av arbeidsforhold, med tanke på informasjonssikkerhet?**
 - Ser på hvordan kommunen håndterer risiko knyttet til personellendringer.
- Hvordan sikrer kommunen at digitale verktøy og systemer som benyttes er vurdert og innført i tråd med personvernlovgivningen?**
 - Undersøker om det finnes prioriteringskriterier og rutiner for innfasing av programmer.
- Er kommunens krav og forventninger til informasjonssikkerhet tydelig kommunisert og ivaretatt i det interkommunale samarbeidet med FARTT?**
 - Vurderer om kommunen har tilstrekkelig styring og kontroll over egne interesser i samarbeidet.
- I hvilken grad har kommunen implementert tiltak som oppfyller kravene i personopplysningsloven, og hvordan følges disse opp?**
 - Ser på både formelle tiltak og faktisk etterlevelse.

Ved gjennomføring av prosjektet som kombinert eierskapskontroll og forvaltningsrevisjon vil det legges vesentlig mer vekt på problemstilling 1 og 4, herunder dokumentinnhenting og intervjuer med sentrale personer i FARTT.

2.3 Revisjonskriterier

Til problemstillingene stiller vi opp revisjonskriterier. Revisjonskriterier er krav og normer som tilstand og/eller praksis i kommunen måles mot. Revisjonskriterier må være aktuelle, relevante og gyldige for kommunen. Sentrale kilder for revisjonskriterier vil være:

- Personopplysningsloven og GDPR.
- Kommuneloven og relevante forskrifter.

- Anbefalinger fra tidligere revisjoner, inkludert rapporten fra 2023 om informasjonssikkerhet i FARTT.
- Beste praksis for tilgangsstyring, sikkerhetskultur og digital samhandling i offentlig sektor.

3 Tilnærming

3.1 Metode

For å svare på problemstillingene vil vi samle inn data ved bruk av følgende teknikker:

- Dokumentanalyse
- Intervju

Dokumentanalyse er en strukturert og systematisk gjennomgang av relevante dokumenter knyttet til IKT-sikkert. Relevant dokumentasjon er eksempelvis:

1. Styringsdokumenter og retningslinjer
 - Overordnede strategier og planer for informasjonssikkerhet og personvern.
 - Rutiner for tilgangsstyring, avgang av personell og bruk av digitale verktøy.
 - Samarbeidsavtaler og ansvarsfordeling mellom kommunen og FARTT.
2. Saksdokumenter og vedtak
 - Kommunestyrets bestilling og vedtak knyttet til IKT-sikkerhet og GDPR.
 - Referater fra relevante møter, inkludert interkommunale samarbeidsfora.
3. Korrespondanse og kommunikasjon
 - E-poster og notater som belyser hvordan kommunen har fulgt opp sine ansvarsområder.
 - Kommunikasjon med FARTT om roller, ansvar og prioriteringer.
4. Systemoversikter og programbruk
 - Oversikt over digitale verktøy og programmer brukt i skolen og andre sektorer.
 - Dokumentasjon på vurderinger av personvern og sikkerhet ved innføring av nye systemer.
5. Tidligere revisjonsrapporter
 - Forvaltningsrevisjonen fra 2023 om informasjonssikkerhet i FARTT.
 - Eventuelle interne evalueringer eller tilsynsrapporter.
6. Opplærings- og kompetansedokumentasjon
 - Kursmateriell og opplæringsplaner for ansatte om GDPR og sikkerhetskultur.
 - Dokumentasjon på gjennomførte tiltak for bevisstgjøring og kompetanseheving.

Det vil bli gjennomført intervjuer med relevante informanter, inkludert IT-leder, HR-leder, representanter fra FARTT osv. Hensikten med intervjuene er å få utfyllende informasjon og forklaringer til oversendt dokumentasjon. Ved gjennomføring av intervjuene vil det bli utarbeidet intervjuguider, og referat fra hvert intervju

Vi ser at kunstig intelligens (KI) forventes tatt i bruk, også i kommuner. Noen er i gang, mens andre er i planleggingsfasen. Forståelse for lovkrav på området – og konsekvenser for IKT er sentralt.

Dette har betydelig effekt for IKT-området, på områder som:

- Organisering, definering av roller og ansvar – internt og med eksterne, inkl avtaleverk
- KI og konsekvenser for risikovurderinger
- KI og konsekvenser for internkontrollen i drifts- og rapporteringsprosesser
- KI og konsekvenser for generelle IT-kontroller
- KI - konsekvenser for informasjon, kommunikasjon og bla effekter for opplæring

Det er derfor sentralt at dette blir innarbeidet i virksomhetsstyringen og forvaltningen.

Hvis dere er i gang med dette, så vil dette også innarbeides i prosjektet, og det er integrert i vår tilnærming.

vil bli sendt til den enkelte informant for verifisering. Svarene vil deretter bli analysert og sammenstilt med annen dokumentasjon.

Prosjektet vil avsluttes med en skriftlig sluttrapport som gir klarhet om undersøkelsen, funnene og anbefalingene. Utkast til rapport vil bli sendt på høring til relevante aktører før det utarbeides en endelig sluttrapport. Rapporten vil være kvalitetssikret med en rød tråd gjennom hele dokumentet.

3.2 Aktivitets- og framdriftsplan

Prosjektet vil verte fordelt på hovedaktivitetane planlegging, gjennomføring og rapportering. Punktene under viser forslag til aktivitets- og framdriftsplan:

1. Planlegging
 - ✓ Utarbeide prosjektplan
2. Gjennomføring
 - ✓ Bestilling og gjennomgang av dokumentasjon
 - ✓ Utarbeide intervjumal
 - ✓ Gjennomføring av intervju
3. Rapport
 - ✓ Analyse og rapportutkast
 - ✓ Høring av rapport
 - ✓ Oversendelse av endelig rapport til kontrollutvalget

Tidsplan for gjennomføring av forvaltningsrevisjonen vil avhenge av kontrollutvalgets prioritering av prosjekt for henholdsvis høst 2025 og vår 2026.

4 Prosjektteam og honorar

4.1 Prosjektteam

KPMG sitt team i forvaltningsrevisjonen består av følgende:

- Oppdragsansvarlig revisor: Thore Kleppen
- Prosjektleder: Mathias W Johannessen
- Prosjektmedarbeider: Brage Midbrød
- Prosjektmedarbeider Kaiwan Salim

4.2 Honorar

220-300 timer i tråd med avtale og avhengig av om det velges å gjennomføre prosjekt som forvaltningsrevisjon eller kombinert forvaltningsrevisjon og eierskapskontroll.



Kontakt oss



Thore Kleppen

Partner

Tlf: +47 406 39 515

Thore.kleppen@kpmg.no