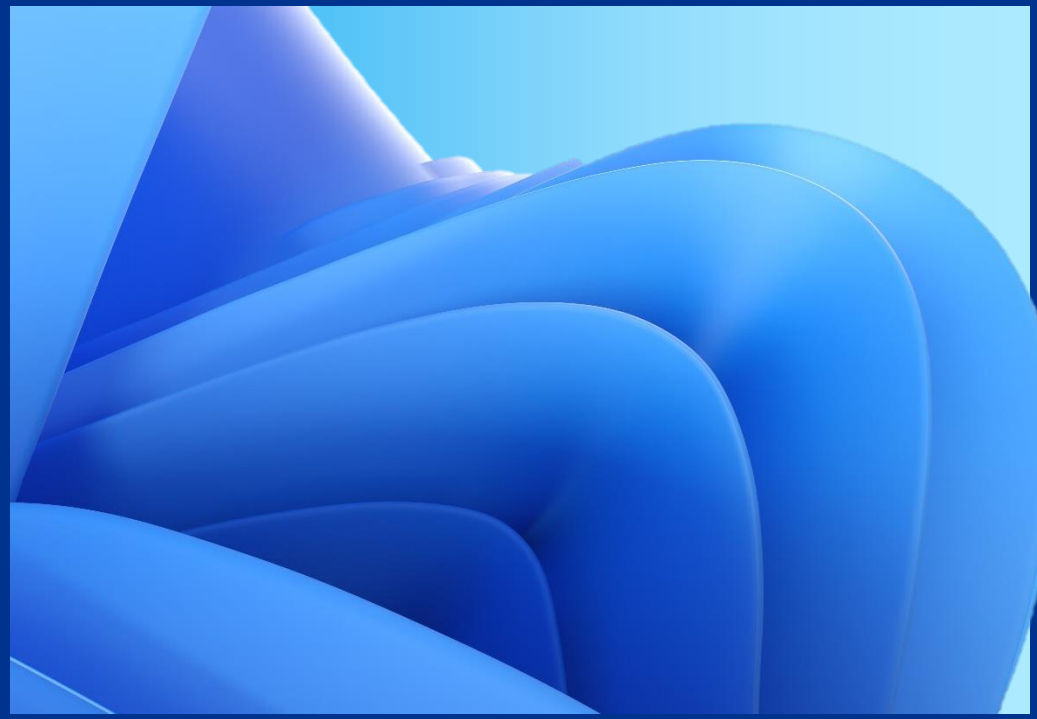
Forvaltningsrevisjon og eierskapskontroll: IKT-sikkerhet og håndtering av GDPR

Oppstartsmøte
Rendalen Kommune

Mai 2026



Innhold

01 Prosjektteam

02 Bakgrunn og formål

03 Tilnærming

04 Fremdriftsplan

Ansvarlig

Oppdragsansvarlig

Thore Kleppen
Partner

Revisjonsteam

Mathias Wasaznik Johannessen
Rolle, prosjektleder

Lisa Malin Pöpplau
Rolle, prosjektmedarbeider

01 Prosjektteam

Om revisjonsteamet

Mathias Johannessen

Senior Manager, Risk & Regulatory

Mathias vil være prosjektleder i internrevisjonen.

Lisa Malin Pöpplau

Associate, Risk & Regulatory

Lisa vil være prosjektressurs i internrevisjonen.

Thore Kleppen

Thore er oppdragsansvarlig partner for revisjon hos Rendalen Kommune.

02 Bakgrunn og formål

Prosjektbeskrivelse (timeomfang og beskrivelse oppdatert etter møtet)

Revisjonsformål og risiko

Formålet med forvaltningsrevisjonen 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.

Rendalen kommune står overfor risiko knyttet til informasjonssikkerhet og personvern, både i samhandlingen med FARTT og i egne ansvarsområder. Tidligere revisjon har avdekket behov for tydeligere roller og ansvar, styrket sikkerhetskultur og økt bevissthet, samt bedre rutiner for håndtering av tilganger ved ansettelse og opphør og for prioritering og innføring av digitale verktøy. Internrevisjonen vil derfor undersøke om ansvarsfordelingen med FARTT fungerer etter hensikten, om det er etablert tilstrekkelig styring av tilganger og digitale verktøy, hvordan forventninger til informasjonssikkerhet kommuniseres i samarbeidet, og i hvilken grad kravene i personvernloven (GDPR) er fulgt opp.

Tilnærming

Forvaltningsrevisjonen avgrenses til kommunens arbeid med informasjonssikkerhet og personvern, inkludert eierskapskontroll av FARTT og en gjennomgang av kommunens AI-bruk.

Forvaltningsrevisjonen vil inkludere dokumentanalyser og intervjuer og sammenholde funnene med relevante krav og god praksis.

Prosjektet vil være forbedringsorientert og resultere i anbefalinger for styrket internkontroll og sikkerhetsstyring

Timer: 300

Gjennomføres: Uke 19-34

Rapportering: Oktober

Evalueringskriterier

Relevante lover og eksterne krav
- Kommuneloven
- Forskrifter

Interne styringsdokumenter og etablerte tiltak

Etterlevelse og praksis
- Relevante standarder og regelverk

Tidligere funn og beste praksis
- Rapport fra 2023 om informasjonssikkerhet i FARTT
- KPMGs rammeverk for AI og bruk av AI
- Beste praksis i sammenliknbare kommuner
- Øvrig veiledningsmateriell fra KS, f.eks. i forbindelse med avtalt eierskapskontroll av FARTT.

Tilleggsproblemstillinger (lysarket ble utarbeidet etter møtet)

KI

Kommunen/Kontrollutvalget av kommunen har bedt om et tillegg til den opprinnelige planen for forvaltningsrevisjonen av deres bruk av KI. Vårt første forslag til hvordan temaet bør behandles, er å ta opp følgende spørsrmål:

- Hva er status på bruk av KI i kommunen (det vil sier: hvordan bruker de KI i nå-situasjonen)
- Hvordan vil de bruke KI? Hva er målbildet for bruk av KI og hva ønsker de å oppnå ved bruk av KI?

For å besvare det innledende spørsmålet skal vi gjennomføre en innledende kartlegging for å få et overblikk over dagens situasjon. Dette kan omfatte:

- Dokumentasjon/informasjon om retningslinjer/rutiner for bruk av KI
- Dokumentasjon/informasjon om hvilke KI-produkter de har implementert og/eller bruker i dag
- Intervjuer med de som har ansvar for den anvendte KI-en, samt et utvalg av brukere i kommunen

Den videre fremgangsmåten for internrevisjonen når det gjelder tilleggstemaet KI vil bli utarbeidet på bakgrunn av svarene på de to første innledende spørsmålene i løpet av prosjektet. Målet med tilleggstemaet er å gi anbefalinger om hensiktsmessig bruk av KI i kommunen, slik at en sikker og effektiv bruk sikres.

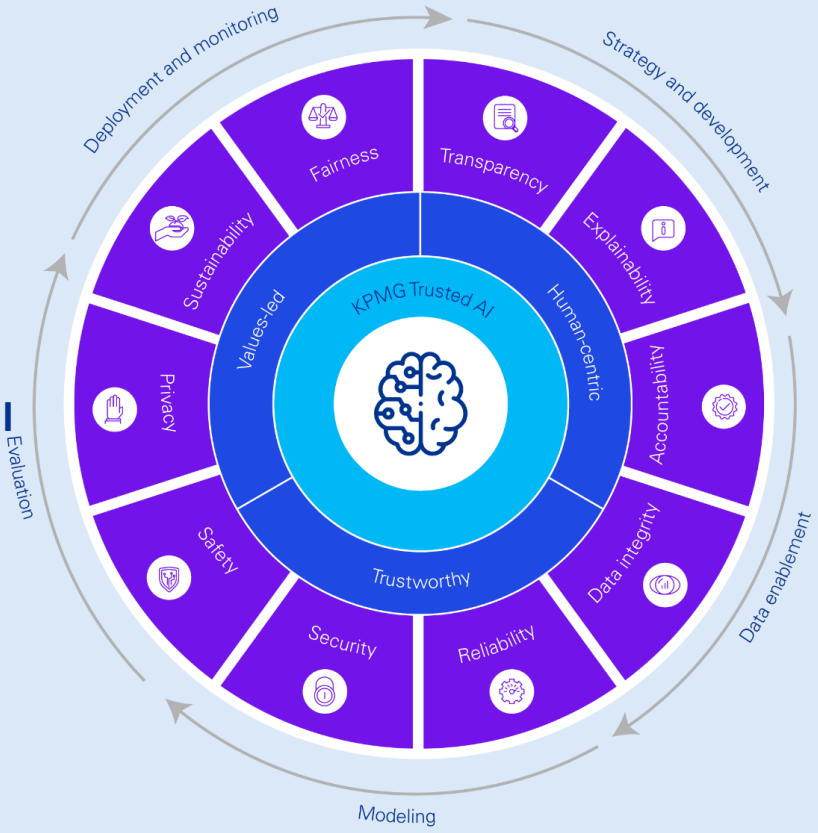
Eierskapskontroll

Et annet tillegg til den opprinnelige planen for forvaltningsrevisjonen som kommunen/kontrollutvalget i dag ba om, er en eierskapskontroll. I denne forbindelse vil vi gjennomføre en eierskapskontroll som del av oppdraget der KS anbefalinger og beste praksis, som sett i andre kommuner, ligger til grunn for gjennomgangen all den tid kommunen for tiden ikke har en godkjent og oppdatert eierskapsmelding.

KPMGs rammeverk for AI

Trusted AI er KPMGs rammeverk for å sikre trygg og etisk forsvarlig bruk av AI. Rammeverket sørger for at Virksomheten kan adressere potensielle problemer ved bruk av AI på en strukturert og helhetlig måte.

Vi vil i vår gjennomgang legge dette rammeverket til grunn og gjennomføre vurderinger av AI-bruk i henhold til punktene 1-10. Dette er et eksempel og vi vil i varierende grad gå inn på innholdselementene



1. **Rettferdighet**
   Sikre at skjevheter i datasett blir redusert til virksomhetens akseptable nivå for rettferdig behandling, slik at diskriminering og urettferdighet forhindres.
2. **Åpenhet**
   Sikre ansvarlig rapportering for å gi en klar forståelse av hvordan AI-løsningen fungerer gjennom hele livssyklusen.
3. **Forklarbarhet**
   Sikre at resultatene som AI produserer kan forklares, slik at brukerne kan opprettholde tillit, aktørene kan holdes ansvarlige, og løsningen forbedres.
4. **Ansvarlighet**
   Sikre at mekanismer som fremmer ansvar er på plass, slik at negative konsekvenser med AI kan forutses, og rettslige hensyn ivaretas.
5. **Integritet**
   Sikre kvalitet i datahåndtering og berikelse gjennom hele livssyklusen, slik at AI produserer riktig beslutningsgrunnlag og overholder reguleringer.
6. **Pålitelighet**
   Sikre at innhold og prediksjoner fra AI er i tråd med tiltenkt formål og ytelse, slik at økonomisk- og sikkerhetsrisiko holdes innenfor terskelverdiene.
7. **Sikkerhet**
   Beskytt mot uautorisert tilgang, lekkasjer og manipulasjon, slik at gjeldende prinsipper og regulatoriske krav til informasjonssikkerhet overholdes for AI.
8. **Trygghet**
   Fastsett risikotoleranse og reguler tillatte bruksområder, slik at AI ikke får negativ innvirkning på mennesker, gjenstander og miljøet.
9. **Personvern**
   Benytt prinsippene for innebygget personvern, vurder konsekvenser og andre krav til personvern slik at personvernforordningen etterleves for AI.
10. **Bærekraft**
    Optimalisere for å begrense negative miljøpåvirkninger der det er mulig.

03 Tilnærming

Metodikk og kilder

01 Dokumentasjon
Gjennomgå sentral dokumentasjon

Liste opp typer dokumentasjon vi ønsker å gjennomgå her:

- Styringsdokumenter og retningslinjer
- Saksdokumenter og vedtak
- Korrespondanse og kommunikasjonsdokumenter
- Systemoversikter og programbruk
- Tidligere revisjons- og tilsynsrapporter
- Opplærings- og kompetansedokumentasjon

02 Intervjuer

Fokus på intervjuobjekter innenfor følgende områder:

- Relevante informanter
- IT-leder
- HR-leder
- Representanter fra FARTT
- Andre avhengig av funn i dokumentasjonen og den endelige avgrensningen

03 Analyse
Vurdere data i sammenheng

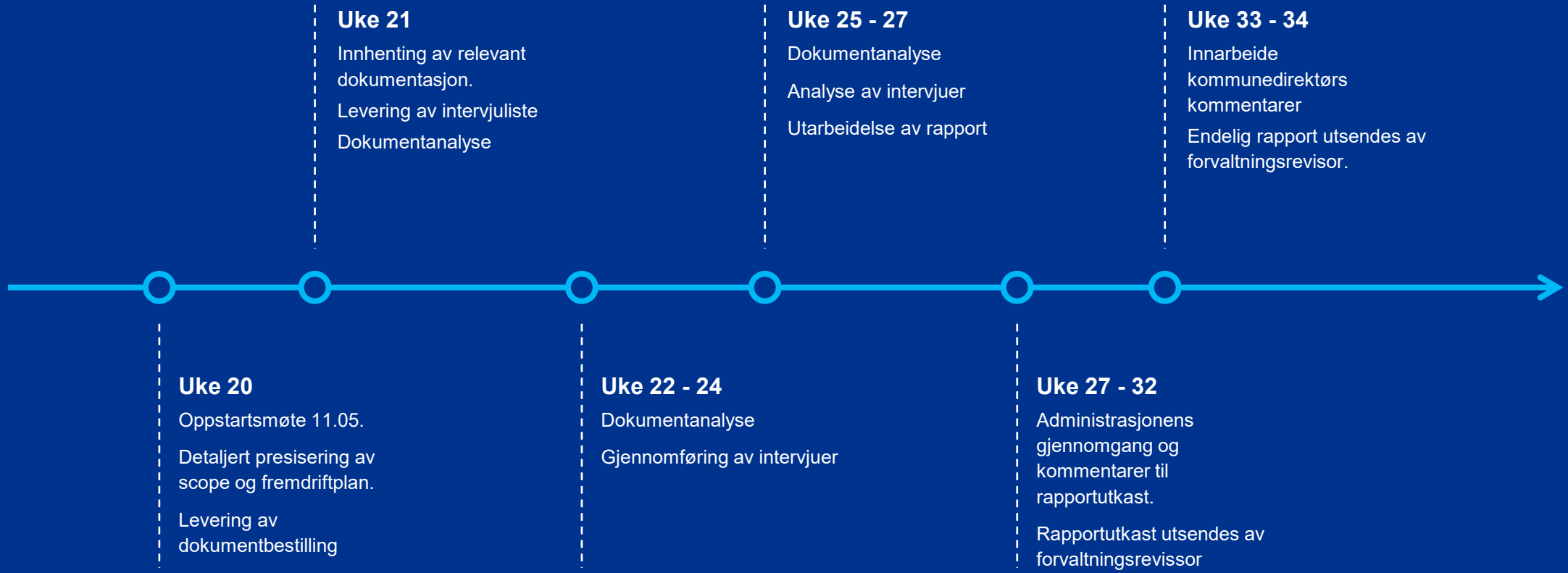
- Dokumentanalyse
- Analyse av intervjudata
- Vurdere styrker og forbedringsområder

04 Rapport
Endelig leveranse til Kontrollutvalget

- Redegjørelse for kriterier, observasjoner og funn
- Kategorisering av funn
- Anbefalinger
- Endelig rapport legges frem for kontrollutvalget etter at den har vært på høring hos kommuneadministrasjonens ledelrgruppe.

04 Fremdriftsplan

Fremdriftsplan



Thore Kleppen
Oppdragsansvarlig

T: +47 406 395 15

E: thore.kleppen@kpmg.no

Mathias W. Johannessen
Prosjektleder

T: +47 91 84 74 43

E: mathias.johannessen
@kpmg.no

kpmg.no/sosialemedier

kpmg.no