PM Revisjon Midt-Norge

Informasjonssikkerhet

Levanger kommune

Prosjektplan forvaltningsrevisjon

FR1371

2026

1 FAKTA OM OPPDRAGET

FORMÅL

Formålet med forvaltningsrevisjonen er å belyse i hvilken grad Levanger kommune ivaretar sitt ansvar for styring, kontroll og beredskap innen informasjonssikkerhet, herunder organisering, risikostyring, internkontroll, avvikshåndtering og oppfølging av IKT-oppgavefellesskap. Revisjonen skal videre belyse hvordan kommunen arbeider med digitalisering og effektivisering, og hvordan dette ses i sammenheng med krav og hensyn knyttet til informasjonssikkerhet.

PROBLEMSTILLINGER

1. I hvilken grad ivareta kommunen sitt ansvar for styring, kontroll og beredskap av informasjonssikkerhet?
    - Roller, ansvar og myndighet
    - Risiko og internkontroll
    - Oppfølging av IKT oppgavefellesskap
    - Avvikshåndtering
    - Beredskap ved cyberhendelser
2. Hvordan er kommunens arbeid med digitalisering og effektivisering?

TIDS- OG RESSURSBRUK

Timeforbruk: 300

Rapport til sekretær: 01.11.2026

OPPDRAGSANSVARLIG REVISOR

Cathrine Berg-Mortensen
cathrine.mortensen@revisjonmidtnorge.no

Tlf. 97795080

2 MANDAT

I dette kapittelet redegjøres det for bestillingen.

2.1 Bestilling

Kontrollutvalget i Levanger kommune bestilte den 18.11.2025, sak 60/25 en forvaltningsrevisjon med tema «informasjonssikkerhet». Forvaltningsrevisjonen er bestilt på bakgrunn av revisors risiko- og vesentlighetsvurdering, og ikke som følge av kommunens plan for forvaltningsrevisjon. I vurderingen er informasjonssikkerhet plassert i kategori høy risiko, og begrunnelsen framgår som følger:

I bestillingen viser sekretær for kontrollutvalget til at informasjonssikkerhet i revisors risiko- og vesentlighetsvurdering er plassert i kategori høy risiko. Begrunnelsen som er trukket fram i bestillingen, er blant annet at sannsynligheten for ondsinnede handlinger rettet mot IKT-systemer vurderes som økende, og at kommuner som komplekse og digitalt avhengige organisasjoner er særlig utsatt. Videre pekes det på at de fleste tjenesteområder er avhengige av stabile IKT-løsninger, og at bortfall eller svikt i systemene kan få betydelige konsekvenser for kommunens virksomhet.

Det fremgår videre av bestillingen at økt digitalisering gir mer effektive arbeidsprosesser, samtidig som bevisstheten rundt IKT-sikkerhet kan være varierende i organisasjonen. Brukerhandlinger, som for eksempel åpning av skadelige lenker, kan medføre uautorisert tilgang til kommunens systemer eller data. Det vises også til at informasjonssikkerhet er tett knyttet til etterlevelse av personvernregelverket (GDPR), og at mangler i sikkerheten kan føre til at personopplysninger kommer på avveie.

På denne bakgrunn er informasjonssikkerhet i bestillingen vurdert som et område med både høy sannsynlighet for sikkerhetshendelser og potensielt alvorlige konsekvenser.

2.2 Bakgrunnsinformasjon

Digital sikkerhet og god håndtering av informasjon er en sentral forutsetning for at kommuner kan levere stabile og trygge tjenester. Kommunene forvalter store mengder personopplysninger og er avhengige av digitale løsninger i hele tjenesteporteføljen. Dette understrekes av Personopplysningsloven og EUs personvernforordning (GDPR), som stiller krav til både internkontroll, risikostyring og dokumentasjon av hvordan kommunen beskytter personopplysninger (Personopplysningsloven §§ 1–3; GDPR art. 5, 24, 28 og 32).

Kommunal sektor er vurdert som særlig utsatt for digitale angrep. I Nasjonal sikkerhetsmyndighets (NSM) trusselbilde fremgår det at det er «høy sannsynlighet for at

kommunal og fylkeskommunal sektor blir forsøkt utnyttet digitalt», og at sektoren må forvente både målrettede og opportunistiske angrep (NSM, *Nasjonalt trusselbilde 2025*)[1]. KS peker i sin rapport *Styrking av digital robusthet i kommunal sektor* (2023)[2] på at en betydelig andel kommuner opplever at det er vanskelig å få oversikt over og etterleve regelverk. Digitaliseringsdirektoratets kunnskapsoppsummering *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner* (2020)[3] viser også at mange kommuner har utfordringer knyttet til risikovurderinger, avvikshåndtering og systematisk internkontroll, noe som kan øke sårbarheten ved digitale hendelser.

Kommunenes økende avhengighet av tredjepartsleverandører for IKT-drift, skyløsninger, fagsystemer og integrasjonstjenester innebærer at styring av databehandlere har blitt et sentralt område innen informasjonssikkerhet. GDPR stiller klare krav til bruk av databehandlere, inkludert skriftlige avtaler, oppfølging, risikovurderinger og dokumentasjon (GDPR art. 28).

IKT-tjenestene i Levanger kommune, leveres gjennom et kommunalt oppgavefellesskap (Digitale Innherred KO). Modellen gir stordriftsfordeler og mulighet for bedre fagkompetanse, men den innebærer også særskilte krav til styring, rolleavklaringer og oppfølging. Kommuneloven § 25-1 krever at kommunen skal ha internkontroll som er tilpasset risiko og vesentlighet, også når tjenester leveres utenfor egen organisasjon.

Slik utviklingen framstår, er informasjonssikkerhet et område med betydelige krav til etterlevelse av lover, forskrifter og interne rutiner. Samtidig har kommunene et ansvar for å sikre robuste tjenester, beskytte personopplysninger og sørge for at digitaliseringen skjer i tråd med rettslige og sikkerhetsmessige krav. Dette gjør temaet særlig relevant for en forvaltningsrevisjon.

2.3 Kommunens organisering

I Levanger kommune er kommunedirektøren øverste administrative leder. Under kommunedirektøren er det fire kommunalsjefer med ansvar for helse og oppvekst, samfunnsutvikling, økonomi, organisasjon og HR.

---

[1] https://nsm.no/getfile.php/1314212-1738741587/NSM/Filer/Dokumenter/Rapporter/Risiko%202025.pdf

[2] https://www.ks.no/contentassets/6394e77225384674b1de93b0203f6825/Digital-robusthet-i-kommunal-sektor-.pdf

[3] https://www.digdir.no/media/1102/download

Levanger kommune har organisert sine IT-tjenester i et kommunalt oppgavefellesskap Digitale Innherred KO. Oppgavefellesskapet omfatter også kommunene Verdal, Steinkjer, Inderøy og Snåsa. Det kommer frem av kommunens delegeringsreglement, at det er kommunedirektøren som har ansvar for å følge opp oppgavefellesskapet[4].

Kommunen opplyser på sine nettsider at den har en ansatt personvernansvarlig, og at personvernombudet spiller en sentral rolle i å sikre etterlevelse av personvernregelverket. Formålet med ordningen er å styrke virksomhetens evne til å behandle personopplysninger på en korrekt måte. Kommunen fremhever at et uavhengig og kompetent personvernombud bidrar til at regelverket følges i praksis, noe som er til fordel både for virksomheten og for de som kommunen behandler opplysninger om (kilde: kommunens egne nettsider om personvernombud).

Videre opplyser kommunen at personvernombudets rolle og oppgaver følger av personvernforordningen (GDPR) artiklene 37, 38 og 39. Ombudet skal gi råd internt og følge med på at virksomheten etterlever regelverket, og fungerer også som kontaktpunkt for personer som kommunen behandler personopplysninger om. Det fremgår også at personvernombudet har taushetsplikt (kilde: kommunens egne nettsider om personvernombud).

[4] Delegeringsreglement | Levanger kommune

3 PROSJEKTDESIGN

Dette kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 Problemstillinger

1. I hvilken grad ivareta kommunen sitt ansvar for styring, kontroll og beredskap av informasjonssikkerhet?
    - Roller, ansvar og myndighet
    - Risiko og internkontroll
    - Oppfølging av IKT oppgavefellesskap
    - Avvikshåndtering
    - Beredskap ved cyberhendelser
2. Hvordan er kommunens arbeid med digitalisering og effektivisering?

Problemstilling 2 er en beskrivende problemstilling og inngår ikke i den kriteriebaserte vurderingen i revisjonen.

3.2 Avgrensing

Revisjonen avgrenses til å undersøke hvordan kommunen ivaretar sitt ansvar for styring og kontroll av informasjonssikkerhet. Undersøkelsen omfatter kommunens egne styrings- og internkontrollaktiviteter, samt hvordan kommunen følger opp det kommunale IKT-oppgavefellesskapet som leverer sentrale IKT-tjenester. Revisjonen vil ikke vurdere kvaliteten i oppgavefellesskapets tekniske løsninger eller gjennomføre tekniske sikkerhetstester.

Revisjonen vil videre avgrenses mot en vurdering av kommunens arbeid med digitalisering og effektivisering. Problemstillingen om digitalisering inngår som en beskrivende del av rapporten og skal gi et bakteppe for å forstå kommunens digitale organisering og eventuelle bruk av digitale verktøy og KI-løsninger. Denne delen vil ikke vurderes opp mot revisjonskriterier, og den inngår ikke i selve vurderingen av kommunens arbeid med informasjonssikkerhet.

Revisjonen omfatter ikke en vurdering av måloppnåelse, gevinstrealisering eller effekter av digitaliseringsarbeidet. Undersøkelsen vil heller ikke inkludere en helhetlig modenhetsvurdering innen digitalisering eller informasjonssikkerhet, eller gå inn i enkeltsaker som gjelder avvik, sikkerhetshendelser eller personvernbrudd utover det som er nødvendig for å belyse praksis.

Revisjonen vil ikke omfatte tjenester som ligger utenfor kommunens ansvar etter kommuneloven og personvernregelverket, eller områder der ansvar og beslutningsmyndighet ligger hos andre virksomheter enn kommunen selv. Undersøkelsen vil heller ikke vurdere

kommunens arbeid med arkitektur, systemutvikling eller digital infrastruktur utover det som er relevant for styring og kontroll av informasjonssikkerhet.

3.3 Aktuelle kilder til kriterier kan være

- Lov om behandlingsmåter i forvaltningssaker (forvaltningsloven)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Lov om kommuner og fylkeskommuner (kommuneloven)
- Lov om Arkiv (arkivlova)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Lov om digital sikkerhet (digitalsikkerhetsloven)
- KS: veiledere om digitalisering, internkontroll og informasjonssikkerhet
- Datatilsynet, veileder om internkontroll og informasjonssikkerhet
- Nasjonal sikkerhetsmyndighet (NSM), Grunnprinsipper for IKT-sikkerhet
- Digitaliseringsdirektoratet, veileder om informasjonsstyring i offentlig sektor
- Eventuelle interne styringsdokumenter i Levanger kommune

3.4 Metoder for innsamling av data

For å besvare problemstillingene, vil revisjonen benytte flere datainnsamlingsmetoder. Metodene er valgt for å gi et bilde av hvordan kommunen ivaretar sitt ansvar for styring, kontroll og beredskap av informasjonssikkerhet.

System- og dokumentgjennomgang

Dokumentanalyse inngår som en sentral metode for å få et overordnet bilde av kommunens arbeid med informasjonssikkerhet. Analysen omfatter gjennomgang av styringsdokumenter, planer, rutiner og tilgjengelig rapportering som beskriver organisering, rolle- og ansvarsfordeling, risikovurderinger, internkontroll og håndtering av avvik og hendelser. I denne delen inngår også dokumenter som viser hvordan kommunen følger opp databehandlere og leverandører, herunder det kommunale IKT-oppgavefellesskapet.

Dokumentene og systemene kan gi grunnlag for å forstå hvilke rammer som ligger til grunn for beredskap og kontinuitet ved digitale hendelser, samt hvilke føringer som finnes for bruk av digitale verktøy og eventuelle KI-løsninger. Opplysninger fra dokumenter kan bidra til å identifisere forhold som kan utforskes nærmere gjennom intervju eller stikkprøver. Dokumentanalysen utgjør dermed en del av helheten i datainnsamlingen knyttet til revisjonens problemstillinger.

Intervju

Intervju benyttes som metode for å innhente utfyllende informasjon om hvordan arbeidet med informasjonssikkerhet er organisert og praktisert i kommunen. Intervjuene gjennomføres som digitale samtaler via Microsoft Teams med relevante personer i administrasjonen som har ansvar eller oppgaver knyttet til temaet.

Intervju kan gi mulighet til å få fram beskrivelser av praksis, rolleforståelse og eventuelle forhold som ikke kommer frem av skriftlig dokumentasjon. Informasjonen kan bidra til å supplere dokumentanalysen og gi grunnlag for eventuelle stikkprøver. Intervjuene inngår dermed som en del av den samlede metoden for å innhente informasjon knyttet til revisjonens problemstillinger.

Vurdering av metode

Valgte metoder innebærer enkelte begrensninger det er relevant å være oppmerksom på. System- og dokumentanalyse gir et innblikk i formelle rammer, beskrivelser og prosedyrer, men gir i mindre grad informasjon om hvordan disse fungerer i praksis. Det kan også forekomme variasjoner i hvordan dokumenter er utformet, oppdatert eller anvendt i organisasjonen, noe som kan påvirke hvilke forhold som framkommer.

Intervju gir mulighet for utdypende beskrivelser, men bygger på informantenes egne fremstillinger og erfaringer. Informasjon som kommer frem i intervju kan være påvirket av individuelle perspektiver, og det kan forekomme forskjeller i hvordan ulike aktører oppfatter roller, ansvar og praksis. Intervju fanger dermed ikke nødvendigvis opp alle sider ved organisasjonens arbeid.

Siden revisjonen ikke omfatter tekniske tester eller vurderinger av enkelthendelser, gir datainnsamlingen et overordnet bilde av hvordan arbeidet med informasjonssikkerhet er organisert og forstått, men ikke et detaljert innblikk i den faktiske gjennomføringen av alle prosesser. Metodevalgene innebærer derfor at funnene vil bygge på tilgjengelig dokumentasjon og de beskrivelsene som kommer frem i intervju.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig revisor	Cathrine Berg-Mortensen
Prosjektmedarbeider	Hanne Marit Ulseth Bjerkan
Kvalitetssikrer	Anna Ølnes
Kvalitetssikrer	Anne Grete Wold

4.2 Milepælsplan

Bestillingsdato	18.11.2025
Prosjektplan til sekretær	06.01.2026
Oppstartsmøte	Medio mars 2026
Datainnsamling ferdig	Medio september 2026
Rapport til uttalelse	Medio oktober 2026
Rapport til sekretær	01.11.2026

Mo i Rana/06.01.2026

Cathrine Berg-Mortensen

Oppdragsansvarlig revisor

VEDLEGG 1: UAVHENGIGHETSERKLÆRING

Vurdering av uavhengighet.
Revisors egenvurdering i forbindelse med forvaltningsrevisjonsprosjekt:

Prosjektnr: FR 1371	**Kommune: Levanger**

Hovedreferanse: Kommuneloven § 24-4 Forskrift om kontrollutvalg og revisjon kapittel 3 ISA 200 - Formål og generelle prinsipper for revisjon av regnskaper pkt. 4 ISA 220 - Vilkår for revisjonsoppdrag pkt. 4, 12-13 ISA 300 - Planlegging av revisjon av regnskaper pkt. 6 Standard for forvaltningsrevisjon RSK 001 pkt. 8 Standard for eierskapskontroll RSK 002 pkt. 3

Ansettelsesforhold:	Undertegnede har ikke ansettelsesforhold i andre stillinger enn Revisjon Midt-Norge SA
Medlem i styrende organer	Undertegnede er ikke medlem av styrende organ i noen virksomhet som ovenfor nevnte kommune deltar i.
Delta eller inneha funksjoner i annen virksomhet, som kan føre til interessekonflikt eller svekket tillit	Undertegnede deltar ikke i eller innehar funksjoner i annen virksomhet som kan føre til interessekonflikt eller svekket tillit til rollen som revisor.
Nærstående	Undertegnede har ikke nærstående som har tilknytning til ovenfor nevnte kommune som har betydning for uavhengighet og objektivitet.
Rådgivnings- eller andre tjenester som er egnet til å påvirke revisors habilitet	Før slike tjenester utføres foretas en vurdering av rådgivningens eller tjenestens art i forhold til revisors uavhengighet og objektivitet. Dersom vurderingen konkluderer med at utøvelse av slik tjeneste kommer i konflikt med bestemmelsen i forskriften § 18, skal revisor ikke utføre tjenesten. Hvert enkelt tilfelle må vurderes særskilt. Revisor besvarer løpende spørsmål/henvendelser som er å betrakte som veiledning og bistand og ikke revisjon. Paragrafen sier at også slike veiledninger må skje med varsomhet og på en måte som ikke binder opp revisors senere revisjons- og kontrollvurderinger. Undertegnede har ikke ytet rådgivnings- eller andre tjenester overfor ovenfor nevnte kommune som kommer i konflikt med denne bestemmelsen.
Tjenesten under kommunens egne ledelses- og kontrolloppgaver	Undertegnede har ikke ytet tjenester overfor ovenfor nevnte kommune som hører inn under kommunens egne ledelses- og kontrolloppgaver.
Opptre som fullmektig for den revisjonspliktige	Undertegnede opptrer ikke som fullmektig for ovenfor nevnte kommune.
Andre særegne forhold	Undertegnede kjenner ikke til andre særegne forhold som er egnet til å svekke tilliten til uavhengighet og objektivitet.

Sted: Mo i Rana Dato: 06.01.26
Rolle: Oppdragsansvarlig revisor
Navn: Cathrine Berg Mortensen

Revisjon Midt-Norge SA
Brugata 2
7716 Steinkjer
post@revisjonmidtnorge.no
907 30 300
www.revisjonmidtnorge.no
Kontonummer: 4270.18.38658
Org.nr: 919 90 2310 MVA

Dokumentet er signert digitalt av:
- CATHRINE BERG-MORTENSEN, 06.01.2026

Forseglet av
Posten Norge

Revisjon Midt-Norge

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no