RM Revisjon Midt-Norge

Forvaltningsrevisjon

IT-sikkerhet

Rennebu kommune

2022

FR2112

1 PROSJEKTFAKTA

Problemstilling	1. Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket? 2. Har kommunen tilfredsstillende tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet?
Kilder til kriterier	• eForvaltningsforskriften • Sikkerhetsloven • Personopplysningsloven • Nasjonal sikkerhetsmyndighet • Faglitteratur
Metode	Dokumentstudier, intervjuer
Tidsplan	• 250 timer • Levering til sekretær 01.05.2023
Oppdragsansvarlig revisor	Forvaltningsrevisor Margrete Haugum, mha@revisjonmidtnorge.no
Kontaktperson Rennebu kommune	Kommunedirektør eller den som kommunedirektør utpeker

2 MANDAT

I dette kapittelet presenteres bestillingen og bakgrunnsinformasjon for prosjektet.

2.1 Bestilling

Kontrollutvalget i Rennebu kommune bestilte en forvaltningsrevisjon med tema IT-sikkerhet i kontrollutvalgsmøtet 21.09.2022, sak 34/22. Kontrollutvalget gjorde følgende vedtak:

1. Kontrollutvalget bestiller en forvaltningsrevisjon for IKT-sikkerhet. Timerammen på forvaltningsrevisjonen kan være på inntil 250 timer.
2. Revisor bes om å utarbeide prosjektplan til neste møte, og det bes om at prosjektplanen er sekretariatet i hende innen den 01.11.2022.

Kontrollutvalget har bestilt forvaltningsrevisjon på IT-sikkerhet utenom plan for forvaltningsrevisjonen.

Bakgrunnen for bestillingen er et vedtak i kontrollutvalget 16.03.2022, sak 19/22 hvor kontrollutvalget ber om en orientering om IKT-sikkerheten i kommunen, og hvilke risiko og sårbarhetsvurderinger som er knyttet til vurderingen. I kontrollutvalgsmøtet 03.05.2022, sak 24/22 orienterte IKT-rådgiver og personal- og stabssjef om hvordan den digitale sikkerheten ivaretas i Rennebu kommune. I denne saken gjør kontrollutvalget følgende vedtak:

> *Kontrollutvalget tar informasjonen om kommunens digitale sikkerhet til orientering.*
>
> *Ut fra en generell risiko- og vesentlighetsvurdering mener kontrollutvalget at det bør gjennomføres en forvaltningsrevisjon innenfor IT-sikkerhet. Også Nasjonal Sikkerhetsmyndighet har kommet med klare råd til virksomheter om å forebygge og avverge cyberangrep. Forvaltningsrevisjon innen IT-sikkerhet står ikke i plan for forvaltningsrevisjon. På den bakgrunn ber kontrollutvalget om at en forvaltningsrevisjon på dette området blir prioritert og gjennomføres utenom planen.*
>
> *Kontrollutvalget oversender saken til kommunestyret med følgende forslag til vedtak: Kommunestyret ber kontrollutvalget om å gjennomføre en forvaltningsrevisjon innenfor IT-sikkerhet utenom gjeldende plan for forvaltningsrevisjon.*

Kommunestyret behandler saken 16.06.2022, sak 22/2022 og ba om at det det gjennomføres en forvaltningsrevisjon innenfor IT-sikkerhet.

Dette vedtaket er bakgrunn for kontrollutvalgets bestilling 21.09.2022.

Kontrollutvalgets bestilling er begrunnet i blant annet Nasjonal Sikkerhetsmyndighet sine klare råd til virksomheter om å forebygge og avverge cyberangrep og dataangrepet som rammet Østre Toten.

I saksframlegget til kontrollutvalgets sak 34/22 nevnes følgende forhold

> • *I hvilken grad fungerer fastlagte rutiner og systemer for IKT-sikkerhet i praksis? Som bl.a opplæring, bevisstgjøring og tydeliggjøring for ansatte av hva som er potensielle farer og hva som er den enkeltes ansvar.*
>
> • *Har kommunen tilfredsstillende systemer og rutiner for å avdekke, redusere og forhindre mulige IKT-risikoer i forhold til tilgjengelige ressurser? Det gjelder:*
>
> *o Rutiner for sikkerhet, drift og vedlikehold av IKT-systemer?*
>
> *o Rutiner for å gjenoppta normal drift etter en driftsstans?*
>
> • *Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket? Det gjelder bl.a personvern, kriseløsninger, sikkerhetskopiering av data (backup) mv.*

2.2 IT-sikkerhet

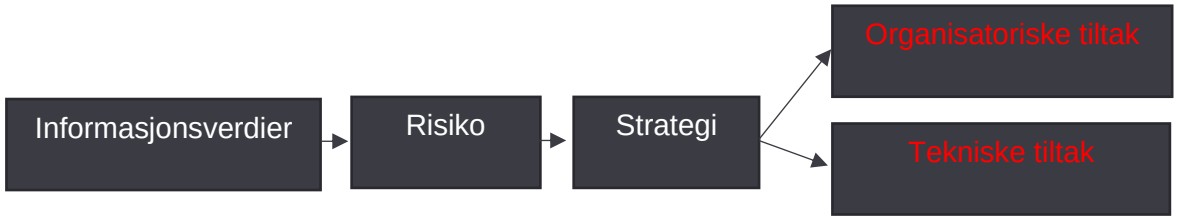
Kontrollutvalgets bestilling tar utgangspunkt i IKT-sikkerhet. Ofte og i dagligtale brukes begrepene IKT-sikkerhet og IT-sikkerhet om hverandre. I forvaltningsrevisjonen vil begge begrepene bli brukt uten at det gjøres noe prinsipielt skille mellom dem.

Det er minst tre juridiske tilnærminger til sikkerhetsarbeid. Det er:

1. eForvaltningsforskriften, § 15 om internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan
2. Sikkerhetsloven, kapittel 4 om krav til forebyggende sikkerhetsarbeid
3. Personopplysningsloven, hvor EUs personvernforordning er inntatt i loven og bestemmelsene omtales som artikler.

Sikkerhetsloven stiller krav om at sikkerhetsstyringen skal gjennomføres planlagt og systematisk i et sikkerhetsstyringssystem som samordnes med virksomhetens styringssystem.

Nasjonal sikkerhetsmyndighet har utarbeidet en veileder i sikkerhetsstyring[1] basert på kravene i sikkerhetsloven. Ifølge veilederen i sikkerhetsstyring handler sikkerhetsstyring om systematiske aktiviteter som er nødvendig for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Utgangspunktet for sikkerhetsstyringen er risikovurderinger som omfatter informasjon om verdier, identifisering av trusler og avdekking av sårbarheter. Risikovurderingen danner grunnlag for risikohåndteringen som handler om hvilke sikkerhetstiltak som skal iverksettes. Disse sammenhengene er illustrert i figur 1.



Figur 1. En visualisering av sammenhenger

Nasjonal sikkerhetsmyndighet har også utarbeidet grunnprinsipper for IKT-sikkerhet (NSM 2020). Grunnprinsippene for IKT-sikkerhet fokuserer på teknologiske og organisatoriske tiltak. Grunnprinsippene er delt i fire kategorier og er gjengitt i tabellen under.

Tabell 1. Grunnprinsipper for IKT-sikkerhet

1. Identifisere og kartlegge	**2. Beskytte og opprettholde**
Kartlegge styringsstrukturer, leveranser og understøttende system Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i utviklings- og anskaffelsesprosesser Etablere en sikker IKT-arkitektur Ivareta en sikker konfigurasjon Beskytte virksomhetens nettverk Kontroller dataflyt Ha kontroll på identiteter og tilganger Beskytt data i ro og i transitt Beskytt e-post og nettleser Etablere evne til gjenoppretting av data Integrere sikkerhet i prosess for endringshåndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trussel Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomføre inntrengningstester	Forbered virksomheten på håndtering av hendelser Vurder og klassifiser hendelser Kontroller og håndter hendelser

Kilde: NSM 2020

[1] veileder-i-sikkerhetsstyring.pdf (nsm.no)

2.3 Kommunens organisering

Rennebu kommune har en IKT-avdeling med to ansatte. En IKT-rådgiver og en IKT-konsulent. IKT-avdelingen går ikke fram av kommunens organisasjonskart som finnes på kommunens hjemmeside. Revisor antar at IKT-avdelingen er en del av stab organisert under personal- og stabssjef.

3 PROSJEKTDESIGN

3.1 Avgrensing

IT-sikkerhet henger tett sammen med bestemmelser i personopplysningsloven. Personopplysningsloven stiller nærmere krav til behandlingen av personopplysninger enn andre informasjonsverdier. Denne forvaltningsrevisjonen avgrenses bort fra å se på de spesifikke kravene som omhandler behandling av personopplysninger, men har en mer overordnet tilnærming til informasjonsverdier, hvor personopplysninger er en bestemt type informasjonsverdi.

3.2 Problemstillinger

Med utgangspunkt i kontrollutvalgets bestilling har revisor utarbeidet følgende problemstillinger for forvaltningsrevisjonen.

1. *Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?*
2. *Har kommunen tilfredsstillende tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet?*

Den første problemstilling har utgangspunkt hva som kreves av et styringssystem for informasjonssikkerhet. Her er risikovurderinger og risikohåndtering sentralt. Det handler blant annet om kommunen har vurdert hvilke informasjonsverdier som kommunen har, hvilke trusler som finnes og hvor sårbar kommunen er hvis denne informasjonen ikke blir tilgjengelig eller kommer på avveie. Et konkret eksempel koblet til personvern, er om kommunen har den lovpålagte oversikten over hvilke personopplysninger som håndteres hvor i kommune-organisasjonen. Et annet eksempel er om kommunen har internkontroll på området.

Aktuelle revisjonskriterier knyttet til styringssystem for informasjonssikkerhet er:

- Kommunen skal regelmessig gjennomføre og dokumentere overordnede risiko-vurderinger som grunnlag for informasjonssikkerhetstiltak
- Det skal gjennomføres og dokumenteres risikovurderinger innenfor informasjons-sikkerhet
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem
- Kommunen må ha rutiner med tilhørende praksis for tildeling og fjerning av tilganger og jevnlig kontrollere identiteter og tilganger
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet
- Kommunen bør vurdere og dokumentere IKT-risiko ved anskaffelser av datasystemer

Den andre problemstillingen handler om konkrete organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten. Rammene for denne problemstillingen er Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet og inndelingen i:

- Identifisere og kartlegge
- Beskytte og opprettholde
- Oppdage
- Håndtere og gjenopprette

CISA (2015) har en annen tilnærming som er delvis overlappende og snakker om forebyggende, oppdagende og korrigerende tiltak.

Aktuelle revisjonskriterier relatert til organisatoriske og tekniske tiltak er:

- Kommunen må ha en oversikt over enheter i IT-systemet
- Kommunen bør etablere en sikker IT-arkitektur
- Kommunen må ha en oversikt over programvare som er i bruk, som tilfredsstiller kravene til en behandlingsoversikt
- Kommunen skal beskytte virksomhetens data
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer
- Kommunen må sikkerhetskopier
- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen
- Kommunen bør ha et system for å oppdage og fjerne kjente sårbarheter (automatisert og sentralisert verktøy eks antivirus, loggføring og sikkerhetsovervåkning)
- Kommunen bør gjennomføre sikkerhetstester
- Kommunen bør ha en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon, gjenopprettingsplan og loggføring)
- Kommunen må ha en plan for gjenoppretting
- Kommunen må ha en beredskapsplan som omfatter IKT-hendelser

3.3 Kilder til kriterier

Aktuelle kilder til revisjonskriterier er:

- eForvaltningsforskriften (FOR2004-06-25-088), § 15 om internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan.

- Lov om nasjonal sikkerhet (Sikkerhetsloven) LOV-2018-06-01-24, kapittel 4 om krav til forebyggende sikkerhetsarbeid
- Lov om behandling av personopplysninger (Personopplysningsloven) LOV-2018-06-15-38
- Nasjonal sikkerhetsmyndighet, udatert, Veileder i sikkerhetsstyring. Versjon 1. Nasjonal sikkerhetsmyndighet
- Nasjonal sikkerhetsmyndighet (2020) NSMs grunnprinsipper for IKT-sikkerhet, versjon 2.0. 15.04.2020
- CISA (2015) CISA Review Manual 26th Edition. CISA

3.4 Metoder for innsamling av data

I denne forvaltningsrevisjonen vil kommunale dokumenter være en viktig datakilde for å undersøke hvilke systemer kommunen har innenfor det reviderte området. Dette kan være politiske dokumenter som gir føringer, risikovurderinger, dokumentasjon av behandling av personopplysninger, rutinebeskrivelser for ulike tiltak, planer for gjenopprettelse med mer.

Intervju med kommunens ledelse og ansatte innenfor IT er viktig for å forstå sammenhengene og få dybdekunnskap om hvordan arbeidet i kommunen foregår. Det kan også være aktuelt å intervjue andre ansatte i kommunen.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Forvaltningsrevisor Margrete Haugum er oppdragsansvarlig og har med seg prosjektmedarbeider Merete Lykken. I tillegg er Merete Montero og Arve Gausen oppnevnt som kvalitetssikrere for prosjektet.

Ingen av de involverte revisorer vil få habilitetsproblemer ved gjennomføringen av prosjektet. Oppdragsansvarlig forvaltningsrevisors uavhengighetserklæring er vedlagt prosjektplanen.

4.2 Tidsplan

Eierskapskontrollen er planlagt med et omfang på 250 timer. Levering til sekretær er foreslått til 01.05.2023. Før den tid får kommunedirektøren et utkast til rapport på høring.

Steinkjer 28.10.2022

Margrete Haugum

Oppdragsansvarlig revisor

VEDLEGG 1: UAVHENGIGHETSERKLÆRING

Prosjekt nr FR1221	**Kommune:** Rennebu kommune
Vurdering av uavhengighet - revisors egenvurdering i forbindelse med forvaltningsrevisjonsprosjekt: IKT-sikkerhet	

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

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.*

Steinkjer 26.10.2022

Margrete Haugum

Margrete Haugum
Oppdragsansvarlig forvaltningsrevisor

Revisjon

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no