PM Revisjon Midt-Norge

Beredskap og informasjonssikkerhet

Vefsn kommune

Prosjektplan forvaltningsrevisjon

FR1301

2024

1 FAKTA OM OPPDRAGET

FORMÅL

Søke å få svar på om Vefsn kommune har betryggende informasjonssikkerhet og beredskap for å ivareta nødvendig drift ved eventuelle hendelser rundt informasjonssikkerhet.

PROBLEMSTILLINGER

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

Problemstillingene, særlig nummer to, vil se nærmere på sikkerheten rundt saks- og arkivsystem og helsejournaler.

Problemstillingene er utdypet i kapittel 3.1.

TIDS- OG RESSURSBRUK

Timeforbruk: 350

Rapport til sekretær: februar/mars 2025

OPPDRAGSANSVARLIG REVISOR

Anna Ølnes

aol@rmnsa.no

2 MANDAT

I dette kapittelet redegjøres det for bestillingen.

2.1 Bestilling

Kontrollutvalget i Vefsn kommune bestilte den 25.04.2024, sak 14/24 en forvaltningsrevisjon om beredskap og IT-sikkerhet. Vedtaket i kontrollutvalget lød blant annet som følger:

> Kontrollutvalget bestiller en forvaltningsrevisjon om beredskap og IT-sikkerhet med følgende tema:
>
> - å se om det er utarbeidet beredskapsplaner for IT-området som er kjent i hele organisasjonen
> - å se i hvilken grad det blir gjennomført nødvendig opplæring og øvelser knyttet til kommunens IT-beredskap
> - å se om kommunen har tilfredsstillende løsninger for hvordan kommunens virksomhet opprettholdes og gjenopprettes ved bortfall av saks- og arkivsystem, samt helsejournaler

I bestillingen er det beredskap for *IT-området* som kontrollutvalget ønsker å se på, ikke all beredskap i kommunen. Revisor tolker andre del av bestillingen som *nødvendig, systematisk opplæring* og øvelser innen IT-beredskap (informasjonssikkerhet). Den tredje delen tolker vi som om kommunen har *tilfredsstillende løsninger* for å opprettholde virksomheten ved bortfall av saks- og arkivsystem og helsejournaler. Videre tolker vi den tredje delen som om kommunen har tilfredsstillende løsninger for å *gjenopprette disse systemene* ved bortfall.

Revisor mener at det kan være fornuftig at prosjektet omfatter *informasjonssikkerhet*, da det omfatter mer enn IT, men henger mye sammen med IT-sikkerhet. Informasjonssikkerhet er det begrepet som brukes i risiko- og vesentlighetsanalysen.

2.2 Bakgrunnsinformasjon

Informasjonssikkerhet er satt med høy risiko i risiko- og vesentlighetsanalysen (ROV)[1] som skal ligge til grunn for planen for forvaltningsrevisjon i Vefsn kommune. I ROV-rapporten er det gjort følgende vurderinger rundt IKT-sikkerhet:

> **Generelt** er sannsynligheten for ondsinnede handlinger mot IKT-systemer økende i samfunnet. Kommunene er komplekse organisasjoner som er avhengig av IKT på de

fleste områder. Hvis IKT-systemet rammes av en hendelse som setter det ut av funksjon, er konsekvensen at kommunens virksomhet blir skadelidende på ulike måter. Økende grad av digitalisering gir effektive løsninger, men det er sannsynlig at bevisstheten omkring IKT-sikkerhet ikke er til stede i hele organisasjonen, med eksempelvis den konsekvens at brukere trykker på en lenke som gir uvedkommende tilganger. IKT-sikkerhet er relatert til personvernforordningen og håndtering av personopplysninger, eksempelvis med den konsekvens at personopplysninger kommer på avveie.

Risikoene som er beskrevet ovenfor gjelder også **Vefsn kommune**. Styrken til kommunen er at kommunen har en IT-avdeling av en viss størrelse i egen organisasjon, med stabile ansatte.

IKT-sikkerhet og beredskap er et av områdene med høyest risiko i hele kommunesektoren og samfunnet ellers.

Revisjon Midt-Norge har gjennomført forvaltningsrevisjonen på dette området i flere kommuner:

I juni 2024 ble det lagt fram en rapport for kontrollutvalget i Melhus[1][2] kommune med følgende problemstillinger:

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

I juni 2023 ble det lagt fram en rapport i Rennebu kommune[3]. Forvaltningsrevisjonen hadde de samme problemstillingene som i forvaltningsrevisjonen i Melhus kommune.

I 2024 har Revisjon Midt-Norge også gjennomført forvaltningsrevisjon, med samme problemstillinger som ovenfor, for Bodø kommune (på oppdrag fra Salten kommunerevisjon, Bodø kommunes revisor).

Revisor mener at disse problemstillingene dekker det som kontrollutvalget i Vefsn kommune er opptatt av.

[1] Se utdyping i vedlegg

2.3 Kommunens organisering

Vefsn kommune har IKT-tjeneste i egen organisasjon. Tjenesten hører under økonomisjefens ansvarsområde, og ledes av en IKT-leder. Tjenesten har fire ansatte i tillegg til IKT-leder.

3 PROSJEKTDESIGN

Dette kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 Problemstillinger

1) Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

   Problemstillingen vil ivareta:

   - Overordna system for informasjonssikkerhet
   - Organisering av informasjonssikkerhet
   - Personvern
   - Internkontroll som ivaretar informasjonssikkerhet (risikovurderinger, avvikshåndtering)
   - Opplæring

2) Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

   - Tiltak for å håndtere risiko
   - Tiltak for å beskytte og opprettholde nødvendig drift
   - Tiltak for regelmessige tester og øvelser, tiltak for å avdekke, håndtere og gjenopprette system ved hendelser

Den siste problemstillingen vil spesielt rettes inn mot saks- og arkivsystem og helsejournaler.

Disse problemstillingene ivaretar kontrollutvalgets føringer, slik de kommer fram i bestillingsvedtaket.

3.2 Kilder til kriterier

- Lov om nasjonal sikkerhet (Sikkerhetsloven)[4]
- Lov om behandling av personopplysninger (Personopplysningsloven)[5]
- Virksomhetsikkerhetsforskriften[6]
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), § 15 om internkontroll på informasjonssikkerhetsområdet[7]
- https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/hva-og-hvorfor-er-det-viktig[8]
- Nasjonal sikkerhetsmyndighet NSM grunnprinsipper[9]
  - Sikkerhetsstyring
  - IKT-sikkerhet

3.3 Metoder for innsamling av data

Metodene for å samle inn og analysere data styres av problemstillingene. Alle forvaltningsrevisjoner begynner med et oppstartsmøte, hvor vi møter ledelsen og nøkkelpersoner innenfor det reviderte området. I oppstartsmøtet vil vi få overordna informasjon om det vi spør om i de to problemstillingene.

For å belyse den første problemstillingen vil vi etterspørre informasjon om og system for internkontroll av informasjonssikkerhet og tilhørende dokumenter. Her vil vi sjekke om de inneholder de bestemmelsene, prosedyrene og rutinene som bør være til stede for å ha tilfredsstillende IKT-sikkerhet.

Når det gjelder den andre problemstillingen vil den bli belyst gjennom intervjuinformasjon med nøkkelpersoner innenfor informasjonssikkerhet, i tillegg til systemansvarlige for saks- og arkivsystem og helsejournaler. Skriftlig dokumentasjon på beredskap og tiltak vil også bli etterspurt og gjennomgått.

Dokumenter som omhandler sikkerheten, kan være unntatt offentligheten. Dette vil bli håndtert i tråd med unntaksbestemmelser i offentlighetsloven.

For den andre problemstillingen kan det være aktuelt å få innsyn i hvor vidt det gjennomføres regelmessige tester.

De metodene og kildene som er beskrevet ovenfor er de som revisor ser på som mest gyldige for å belyse problemstillingene. Revisor vil, i tråd med sitt selvstendige ansvar for å følge god kommunal revisjonsskikk i valg av metoder og kilder, kunne gjøre endringer.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig revisor	Anna Ølnes
Prosjektmedarbeider	Hanne Marit Ulseth Bjerkan
Kvalitetssikrer	Margrete Haugum
Kvalitetssikrer	Cathrine Berg Mortensen

4.2 Milepælsplan

Bestillingsdato	10.05.2024
Prosjektplan til sekretær	30.08.2024
Oppstartsmøte	September 2024
Datainnsamling ferdig	Februar 2025
Rapport til uttalelse	Februar 2025
Rapport til sekretær	Februar/mars 2025

Trondheim,

Anna Ølnes

Oppdragsansvarlig revisor

KILDER

1. Revisjon Midt-Norge SA Revisors Risiko- Og Vesentlighetsvurdering (ROV) for Vefsn Kommune. **2024**.
2. Revisjon Midt-Norge SA Informasjonssikkerhet i Melhus Kommune. **2024**.
3. Revisjon Midt-Norge SA IT-Sikkerhet i Rennebu Kommune. **2023**.
4. Justis- og beredskapsdepartementet Lov Om Nasjonal Sikkerhet (Sikkerhetsloven). **2018**.
5. Justis- og beredskapsdepartementet Lov Om Behandling Av Personopplysninger (Personopplysningsloven). **2021**.
6. Justis- og beredskapsdepartementet Forskrift Om Virksomheters Arbeid Med Forebyggende Sikkerhet (Virksomhetssikkerhetsforskriften). **2018**.
7. Digitaliserings- og forvaltningsdepartementet Forskrift Om Elektronisk Kommunikasjon Med Og i Forvaltningen (EForvaltningsforskriften). **2004**.
8. Direktoratet for forvaltning og økonomistyring (DFØ) Miniveileder Om Oppfølging Av Informasjonssikkerhet i Styringsdialogen. **2024**.
9. Nasjonal sikkerhetsmyndighet (NSM) *NSM Grunnprinsipper*; 2020;

Revisjon Midt-Norge

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no