Forvaltningsrevisjonsrapport - Informasjonssikkerhet

Behandles i utvalg	**Møtedato**	**Saknr**
Kontrollutvalget i Namsos kommune	30.08.2022	22/22

Saksbehandler Einar Sandlund
Arkivkode FE-217, TI-&58
Arkivsaknr 21/234 - 7

Forslag til vedtak:

1. Kontrollutvalget slutter seg til forvaltningsrevisjonsrapporten Informasjonssikkerhet.
2. Saken oversendes kommunestyret med slik innstilling til vedtak:

1) *Kommunestyret tar forvaltningsrevisjonsrapporten Informasjonssikkerhet til orientering.*
2) Kommunestyret ber kommunedirektøren følge opp rapportens anbefalinger:

• Inkludere informasjonssikkerhet i helhetlig ROS.
• Utarbeide målsettinger og strategi for informasjonssikkerhet separat eller i forbindelse med andre plandokumenter.
• Om organisering og ansvar for informasjonssikkerhet er tydelig og hensiktsmessig.
• Få på plass et internkontrollsystem.
• Iverksette gjennomganger for å avvikle tilganger til personer som har sluttet.
• Sikre at behandlingsoversikter kommer på plass i henhold til personopplysningsloven.
• Løfte fokuset på informasjonssikkerhet som et ledd i å bygge en sikkerhetskultur.
3) Kommunestyret ber kommunedirektøren innen 01.03.22 om skriftlig rapport til kontrollutvalget på hvordan anbefalingene er fulgt opp.

Vedlegg
Forvaltningsrevisjonsrapport informasjonssikkerhet

Saksopplysninger
Kommunelovens § 23-3 sier at det skal gjennomføres forvaltningsrevisjon i kommunen.
Kommunestyret behandlet den 29.10.20 i sak 155/20 plan forvaltningsrevisjon 2020-2024.

Ut fra prioriteringen i planen gjorde kontrollutvalget i sak 21/21 slikt bestillingsvedtak:
1. Kontrollutvalget bestiller forvaltningsrevisjon området IKT, datasikkerhet, GDPR.
2. Kontrollutvalget gir følgende innspill på følgende problemstillinger/spørsmål:
· Sikkerhet , drifting og dublering av system,
· Samordning mellom enhetene på bruk av digitale plattformer, effektivisering.
· Fremtidig lagring og tilgang. Kompatibilitet av system, rettsdokumentasjon,
3. Revisor bes å utarbeide prosjektplan i henhold til neste møte, 23.11.21.

Kontrollutvalget behandlet prosjektplanen i sak 27/21 og fattet slikt vedtak:
1. Prosjektplan datert 04.11.21 godkjennes.
2. Rapporten forventes levert 01.06.22 og innenfor den angitte ressursbruk på 400 timer.
3. Kontrollutvalget bes å bli orientert underveis for å kunne ta stilling til evt. behov for endringer i prosjektplanen.

Følgende problemstillinger er besvart i rapporten, jfr. vedtatt prosjektplan :
1. Hvordan ivaretar Namsos kommune informasjonssikkerhet?
2. Hvordan har kommunen sikret integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene?

Endelig rapport ble oversendt 07.07.22. Kommunedirektøren har rapporten til høring og avgitt høringssvar 27.05.22, jfr. vedlegg 2 i rapporten. Etter oppstartsmøtet ble det klart at den andre problemstillingen om sikring av integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene, burde tones ned. Dette skyldes at de sammenslåtte kommunene, Overhalla kommune og Flatanger kommune har hatt et samarbeid innenfor IT siden 2002. Revisor har derfor valgt å lage et beskrivende svar på denne problemstillingen, uten revisjonskriterier.

Metodene brukt for å samle data i denne forvaltningsrevisjonen, nærmere beskrevet i kap. 1.3., er gjennomført med intervjuer og dokumentgjennomgang. Til intervjuene ble det laget tilpassede intervjuguider. Det er skrevet referat fra alle intervjuene, som er verifiserte. Noen av de som er intervjuet har fått tilleggsspørsmål på e-post i etterkant. I dokumentgjennomgangen er sentrale politiske dokumenter slik som samfunnsplan og beredskapsplan, dokumenter og referater fra informasjonssikkerhetsutvalgets arbeid og rutiner fra kvalitetssystemet m.v. Det er revisors oppfatning at de data som er samlet inn gir et tilstrekkelig grunnlag for å belyse arbeidet med informasjonssikkerhet i Namsos kommune

Hvordan ivaretar Namsos kommune informasjonssikkerhet?
Konklusjon er at Namsos kommune mangler en forankring for arbeidet med informasjonssikkerhet i kommunens mer overordnede risikovurderinger og planer. Videre mangler kommunen blant annet internkontroll og kontroll med brukertilganger. Kommunen har en del forebyggende og oppdagende sikkerhetstiltak. Korrigerende tiltak er i stor grad på plass for IT-enheten, men ikke andre deler av kommunen. Det mangler en overordnet risikovurdering for informasjonssikkerhet i Namsos kommune, som kan legge premissene for informasjonssikkerhetsarbeidet, men det er gjort enkelte risikovurderinger innenfor området.

Videre er det uklart om det finnes et mål for informasjonssikkerhet, det mangler en sikkerhetsstrategi og kommunen har ikke en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår. Internkontroll er ikke på plass og det arbeides med å få på plass et kvalitetssystem som grunnlag for internkontroll. Flere rutinebeskrivelser er på plass.

Kommunen har et system på opprettelse av brukere, men har ikke kontroll på å avvikle brukere som ikke skal ha tilgang til datasystemet lengre. Kommunen har en behandlingsoversikt i henhold til personopplysningsloven som ligger i dagens kvalitetssystem, men det er ikke oppdatert. Det gis opplæring i informasjonssikkerhet til nyansatte og skal gjennomføre årlige opplæringstiltak, men slik revisor ser det er det et forbedringspotensial i å bygge en sikkerhetsstruktur.

Det vurderer ikke IKT-risiko ved alle anskaffelser av datasystemer. Kommunen har systemer for for å overvåke datasikkerhet, sårbarheter, trafikkanalyse og det er gjennomført inntrengingstest i 2022. Likedan vurderer revisor det slik at kommunen har planer for gjenoppretting, hendelseshåndtering og enkelte hendelser, f.eks. ransomwareangrep.

Informasjonssikkerhet i overgangen til ny kommune
Overgangen til ny kommune medførte ikke store endringer siden samarbeidet på IT allerede var på plass og det var lite problemer knyttet til IT ved sammenslåingen av kommunene. Revisor har valgt å lage en beskrivende besvarelse på denne problemstillingen, fordi det er historie og lite aktuelt for revisjon. Kommunen leverer i dag mange IT-tjenester til Flatanger og Overhalla kommuner.

Revisors oppfatning er at integritet, konfidensialitet og tilgjengelighet for informasjon ble ivaretatt ved kommunesammenslåingen. Kommunene som ble sammenslått, hadde allerede et samarbeid og datasystemene var allerede koblet sammen, slik at jobben med overgangen handlet om å integrere like systemer. Historiske data fra sak- og arkivsystemet ble tatt vare på og tilgjengelig fra historiske databaser.

Imidlertid kommer det frem behov for at det utarbeides en ny IKT-strategi i forbindelse med etableringen av Nye Namsos og som kan være felles for alle kommunene, som fortsatt skal ha samdrift om IKT-infrastruktur. Revisor har ikke funnet at det er laget noen IKT-strategi etter kommunesammenslåinga.

Vurdering
Sekretariatet viser til den framlagte rapport og er av den oppfatning at den svarer ut de gitte problemstillinger i prosjektplanen.

Sekretariatet viser til at rapporten viser at kommunen har flere mangler vedrørende informasjonssikkerhet. Det gjelder forankringen av arbeidet med risikovurderinger, internkontrollsystem, og kontrollen med brukertilganger m.v. Målsettinger og strategi for informasjonssikkerheten bør utarbeides separat eller i forbindelse med andre planer. Videre kommer det frem at å sikre behandlingsoversikter iht. personopplysningsloven kommer på plass. Fokuset på informasjonssikkerhet for å bygge en sikkerhetskultur må økes.
En god del forebyggende og oppdagende sikkerhetstiltak er imidlertid på plass og innenfor IT-enheten er mange korrigerende tiltak på plass, men ikke i andre deler av kommunen.

Sekretariatet viser forøvrig til at kommunen leverer mange IT-tjenester til Flatanger og Overhalla kommuner.

Kontrollutvalget anbefales å slutte seg til rapporten. Saken anbefales videre lagt frem for kommunestyret med innstilling på å ta forvaltningsrevisjonsrapporten Informasjonssikkerhet til orientering og videre be kommunedirektøren følge opp anbefalingene i innstillingens pkt. 2. Kommunestyret anbefales til slutt å be kommunedirektøren innen 01.03.22 .22 gi skriftlig rapport til kontrollutvalget på hvordan anbefalingene er fulgt opp.