Forvaltningsrevisjon av informasjonssikkerhet - prosjektplan

Behandles i utvalg	**Møtedato**	**Saknr**
Kontrollutvalget i Melhus kommune	07.09.2023	40/23

Saksbehandler Eva J. Bekkavik
Arkivkode FE-217, TI-&58
Arkivsaknr 23/94 - 7

Forslag til vedtak
Kontrollutvalget slutter seg til problemstillingene, leveringstidspunkt og ressursrammen revisjonen har foreslått i prosjektplanen

Vedlegg
Prosjektplan, oppdatert med ny leveringsdato
Brev til Revisjon Midt-Norge SA om kontrollutvalgets vedtak i sak18/23

Saksopplysninger
Datatilsynet har satt i gang et større tilsynsarbeid med nærmere hundre norske kommuner og fylkeskommuner sin ivaretakelse av personopplysningssikkerheten. Tilsynsarbeidet vil gjennomføres i to faser. Fase 1 består av dokumentgjennomgang og fase 2 blir et stedlig tilsyn og vil være som en forvaltningsrevisjon. Melhus kommune ble trukket ut til fase 1.

Kontrollutvalget fikk prosjektplanen til behandling på sitt møte 4. mai (sak 18/23), men vedtok å sette behandlingen "på vent" inntil Datatilsynet tok en beslutning om hvilke kommuner som ble trukket ut til fase 2. Kontrollutvalget fattet følgende vedtak:
Kontrollutvalget avventer å behandle prosjektplanen til Datatilsynet har bestemt hvilke kommuner som vil være med i fase 2.

Melhus kommune ble ikke trukket ut til fase 2 i Datatilsynets undersøkelse, derfor legges prosjektplanen frem for kontrollutvalget i dagens møte.

Kontrollutvalget og kommunestyret har gjennom utarbeidelsen og vedtak av plan for forvaltningsrevisjon for 2020 - 2024, lagt premissene for forvaltningsrevisjonsarbeidet ut 2024.
På kontrollutvalgets møte 16. februar 2023, i sak 6/23, bestilte utvalget en forvaltningsrevisjon av datasikkerhet.

Kontrollutvalget protokollerte følgende:
Kontrollutvalget ønsker svar på følgende spørsmål:
- Hva gjør kommunen for å forebygge, oppdage og håndtere digitale angrep?
- Hva gjør kommunen hvis systemene blir helt utilgjengelige eller ikke til å stole på?
- Hvordan forvaltes kommunens kontroll over persondata?
- Hvordan forvaltes teknologien og hvordan understøtter den kommunale tjenester på kort og lang sikt?
- Hvilke rutiner er etablert for sikring av kommunes data?
- Hvordan følger kommunens sikkerhetstiltak lover, forskrifter og annet regelverk med tanke på backup, personvern, kriseløsninger, hacking med mer?
- Hvordan fungerer de fastlagte rutinene for informasjonssikkerhet i praksis?
- I hvilken grad er organiseringen av informasjonssikkerhetsarbeidet tilfredsstillende og i tråd med lovkrav?
- Hvilke systemer har kommunen for kontroll og etterprøving av informasjonssikkerhet?
- Hvordan blir kontroll og etterprøving gjennomført?

Kontrollutvalget fattet følgende vedtak:
1. Kontrollutvalget viser til plan for forvaltningsrevisjon for 2020-2024 og bestiller en forvaltningsrevisjon av datasikkerhet.
2. Prosjektplan med ressursramme og tidspunkt for ferdig rapport oversendes kontrollutvalgets sekretariat innen 17.04.2023 og legges frem for kontrollutvalget på utvalgets møte 04.05.2023.
3. Kontrollutvalget gir sekretariatet fullmakt til å følge opp prosjektet på vegne av utvalget.

Revisor har avklart begrepene "datasikkerhet" og "informasjonssikkerhet" på side 3 og 4 i prosjektplanen, og sier at det er begrepet "informasjonssikkerhet" som er brukt i spørsmålene som kontrollutvalget ønsker svar på. På bakgrunn av dette så vil revisor bruke begrepet informasjonssikkerhet videre i denne forvaltningsrevisjonen.

Revisjonen har foreslått 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?

Forvaltningsrevisjonen gjennomføres med et timeforbruk på inntil 300 timer. Revisor vil ta et oppstartsmøte med administrasjonen i starten av november 2023 og datainnhentingen vil være ferdig i midten av februar 2024. For å svare ut problemstillingene har revisor planlagt å bruke intervju og en dokumentgjennomgang. Ferdig rapport oversendes kontrollutvalgets sekretariat i slutten av april 2024.

Oppdragsansvarlig forvaltningsrevisor, Hanne Marit Ulseth Bjerkan, vil orientere om problemstillinger og gjennomføring av forvaltningsrevisjonen på møtet 7. september. Kontrollutvalget må da benytte anledningen til å stille spørsmål, samt å gi innspill til eventuelle endringer og/eller tillegg.

Vurdering
Revisor har satt opp en oversikt på side 10 i prosjektplanen som viser hvilken av problemstillingene som svarer ut de ulike spørsmålene kontrollutvalget ønsker svar på.

Ferdig rapport skal leveres kontrollutvalgets sekretariat i slutten av april 2024, det vil si at kontrollutvalget kan behandlet rapporten på sitt siste møte før sommeren i 2024.

Kontrollutvalgets sekretariat har endret tittel på forvaltningsrevisjonen fra Datasikkerhet til Informasjonssikkerhet på bakgrunn av revisors forklaring av begrepene.

Konklusjon
Kontrollutvalgets sekretariat anbefaler at kontrollutvalget slutter seg til problemstillingene, leveringstidspunkt og ressursrammen revisjonen har foreslått i prosjektplanen.