Prosjektplan for forvaltningsrevisjon av IT-sikkerhet og personvern

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Tynset kommune	21.03.2023	15/23

Saksbehandler Ragnhild Aashaug
Arkivkode FE-217, TI-&58
Arkivsaknr 23/105 - 3

Forslag til vedtak
Kontrollutvalget godkjenner den framlagte prosjektplanen av forvaltningsprosjektet «Forvaltningsrevisjon avIKT-sikkerhet i IKT Fjellregionen IKS for kontrollutvalgene i eierkommunene.»
Oppstart igangsettes etter beskjed fra Kontrollutvalget i Tynset kommune

Vedlegg
BDO - Prosjektplan forvaltningsrevisjon av IKT-sikkerhet

Kontrollutvalget godkjenner den framlagte prosjektplanen av forvaltningsprosjektet «Forvaltningsrevisjon avIKT-sikkerhet i IKT Fjellregionen IKS for kontrollutvalgene i eierkommunene.»
Oppstart igangsettes i henhold til prosjektplanen.
Behandling:
Fra BDO AS deltok: prosjektansvarlig oppdragsrevisor Øyvind Sunde, Irene Aasen og Jonas Strisland. De hadde en gjennomgang av prosjektplanen.
Formålet med forvaltningsrevisjonen er å belyse IT-sikkerheten i IT-selskapet.
Gjennomgangen vil ha hovedfokus på IT-sikkerhet, men også omfatte personvern i relasjon til god informasjonssikkerhet.
Prosjektet er avgrenset til å omhandle programvare som FARTT har ansvar for.
Revisjonen vil forgå i henhold til nyeste standard (kommet ny i 2022).

Det legges opp til at rapporten primært kan gjennomgås som en felles presentasjon for kontrollutvalgene, og en presentasjon i det enkelte kommunestyre.

Sekretariatet informerte om at Ikt Fjellregionen IKS og de respektive kommunene er medlem i Kommune-CSIRT fra mars 2021. Kommune-CSIRT støtter norske kommuner og fylkeskommuner med sikkerhetsgjennomgang, sikkerhetsdokumenter, relevant informasjon og rådgivning rundt trusler, hendelser og sårbarheter i det digitale domenet.

Prosjektplanen er i henhold til bestillingen, og rapporten kan leveres i inneværende periode om det igangsettes etter påske. Kontrollutvalget ønsker derfor at forvaltningsrevisjonen igangsettes selv om det mangler vedtak fra de respektive kommuner om bevilgning, og tar risikoen ved eventuelle manglende bevilgninger. Sekretariatet henvender seg til kontrollutvalgene som ønsker å delta og informerer om igangsetting og ønske om svar på bevilgning. Dersom noen utvalg har innspill til prosjektplanen, så bes det om snarlig tilbakemelding.

Kontrollutvalget fremmet følgende endringsforslag på siste setning:
Oppstart igangsettes i henhold til prosjektplanen.

Forslag til vedtak enstemmig vedtatt.

Vedtak:

Kontrollutvalget godkjenner den framlagte prosjektplanen av forvaltningsprosjektet «Forvaltningsrevisjon av IKT-sikkerhet i IKT Fjellregionen IKS for kontrollutvalgene i eierkommunene.»
Oppstart igangsettes i henhold til prosjektplanen.

Saksopplysninger
Kontrollutvalget vedtok den 20.02.23 i sak 7/23 en bestilling av forvaltningsrevisjon på området IT-sikkerhet og personvern. Kontrollutvalget gjorde følgende vedtak:

1. Kontrollutvalget bestiller en prosjektplan på IKT sikkerhet og personvern i IKT Fjellregionen IKS ut fra den foreskrevne henvendelsen til de samarbeidende kontrollutvalgene.
2. Eierandelen legges til grunn for fordelingen av kostandene, og Tynset tar kostnaden for Folldal kommune sin eierandel.
3.

Timerammen på forvaltningsrevisjonen ble satt på 250 - 300 timer i bestillingen, og det kommer her ut med 270 timer. Det er inkluderer fysisk oppmøte én gang for å presentere rapporten, eksempelvis for kommunestyret. Øvrige møter, intervjuer og lignende foreslås gjennomført digitalt. Revisjonen oppgir at det dersom det ikke er ønskelig med presentasjon for alle kontrollutvalgene, kan rammen reduseres med 5 timer, eller omdisponeres til tid brukt på kartlegging og rapportering.

Fremdriftsplanen viser at arbeidet kan startes opp umiddelbart, og ferdigstilles innen sommerferien. Fremdriftsplanen er laget med forbehold om oppstart kort tid etter kontrollutvalgsmøte 21. mars 2023. Ved lengre utsettelse av igangsetting, kan høringsutkast utsettes til uke 32. Rapporten vil da fortsatt kunne behandles i kontrollutvalgets møte 4. september 2023.
Revisor vil gi løpende orientering om fremdrift underveis i prosjektet.

Problemstillinger

1. Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?
   Dette sees opp mot informasjonssikkerheten. Det kartlegges hvilke styrende dokumenter selskapet har utarbeidet, og hvordan roller og ansvar er definert.
   Disse kriteriene legges til grunn:
   a. Selskapet har etablert et styringssystem for informasjonssikkerhet.
   b. Selskapet har definert roller og ansvar knyttet til arbeid med informasjonssikkerhet.
   c. Selskapet har utarbeidet styrende dokumenter for informasjonssikkerhet.

2. Blir sikkerhetsrisikoer identifisert og håndtert?
   Dette omhandler identifisering og håndtering av sikkerhetsrisikoer. Problemstillingen vil hovedsakelig bli kartlagt gjennom dokumentstudier, intervjuer og test av utvalgt materiale.
   Det foreslås å legge følgende kriterier til grunn for forvaltningsrevisjonen:
   a. Selskapet har kartlagt alle enheter og programvare som er i bruk.
   b. Selskapet har kontroll på alle identiteter og tilganger.
   c. Selskapet har utarbeidet, og reviderer jevnlig, risiko- og sårbarhetsanalyse av IKT-systemene.

3. Blir informasjon og informasjonssystemer beskyttet iht. beste praksis?
   Det vil undersøkes om det er etablert en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap om en hendelse skulle inntreffe. Dette vil undersøkes ved å gjennomgå
   Denne problemstillingen vil primært kartlegges gjennom dokumentstudier, intervjuer og test av utvalgt materiale for å se på prosesser og rutiner som er etablert for

sikkerhetskopiering og lagring av data.
Disse kriterier legges til grunn:

a. Selskapet har etablert et regime for sikker IKT-arkitektur og konfigurasjon.
b. Selskapet har oversikt og kontroll over hele livsløpet til de tjenestene som forvaltes på vegne av kommunen og som er tjenesteutsatt.
c. Selskapet har en plan for regelmessig sikkerhetskopiering av all virksomhetsdata for kommunene.

4. Hvordan oppdages avvik og mulige trusler mot virksomheten?
   Her sees det på om det er etablert sikkerhetsovervåking, rutiner for å oppdage sårbarheter/trusler og om det gjennomføres inntrengningstester på enkelte elementer. Dette kartlegges gjennom dokumentstudier, intervju og penetrasjonstesting.
   Disse kriteriene legges til grunn:
   a. Selskapet har etablert sikkerhetsovervåkning av utvalgte deler av IKT-systemet.
   b. Selskapet har rutiner for å oppdage og fjerne kjente sårbarheter og trusler.
   c. Selskapet har gjennomført inntrengningstester på utvalgte IKT-systemer.

5. Blir hendelser håndtert på en tilfredsstillende måte?
   Er virksomheten forberedt på uønskede hendelser? Denne problemstillingen kartlegges gjennom dokumentstudier, intervjuer og test av utvalgt materiale.
   Disse kriterier legges til grunn:
   a. Selskapet har et planverk for hendelseshåndtering og som revideres jevnlig.
   b. Selskapet har gjennomført regelmessige øvelser på informasjonssikkerhetshendelser.
   c. Selskapet har evaluert og implementert tiltak etter tidligere hendelser eller øvelse.

Avgrensning:
Revisjonen vil bygge på intervjuer, gjennomgang av dokumentasjon, test av utvalgte kontroller og penetrasjonstest gjennomført av BDO. Revisjonen vil i hovedsak omfatte felles infrastruktur som driftes hos IKT Fjellregionen IKS på vegne av kommunene i FARTT-samarbeidet. Revisjonen vil i utgangspunktet ikke omfatte infrastruktur som driftes av andre eksterne partner. Revisjonen vil ikke kunne gjennomgå alle applikasjonene som benyttes i kommunen, men vil ta utgangspunkt i de applikasjonene kontrollutvalget og administrasjonen anser som særskilt viktige. Dette avklares nærmere i planleggingsfasen av forvaltningsrevisjonen.

Vurdering og konklusjon
Planen viser hvordan forvaltningsrevisjonen er tenkt gjennomført, og samsvarer med den foreløpige prosjektbeskrivelsen som det ble bestilt når henvendelsen ble sendt ut til de andre eierkommunene. Personvern er ikke direkte berørt, men ut fra sekretariatets forståelse så er personvern inkludert gjennom at IKT-sikkerheten skal ivareta slike hensyn. Siden prosjektplanen harmonerer med utsendt beskrivelse, så legges det ikke opp til at prosjektplanen behandles i den enkelte kommune. Det er derimot viktig at rapporten kan behandles av alle, og det kan legges opp til en felles presetasjon for kontrollutvalgene. Men i det enkelte kommunestyre bør det gjøres individuelle presentasjoner, og dette kan gjøres digitalt.

Når det gjelder oppstart av prosjektet, så er bevilgning fra kommunestyrene i eierkommunene som ønsker å delta ikke avklart. Dersom kontrollutvalget vil avvente tilbakemelding på om kommunestyrene i Tolga, Alvdal og Rendalen bevilger midler til prosjektet, så er det litt usikkert når det kan behandles i kommunene. Det vil settes i gang en prosess mot kommunene når Tynset har behandlet denne prosjektplanen, og en kan jo håpe

på et svar innen den 1.mai. Kontrollutvalget må vurdere om de vil sette i gang og håpe på at det kommer midler eller om de vil utsette oppstart til tilsagnene er klare.