Til kontrollutvalgene i IKT Fjellregionen IKS sine eierkommuner

29.november 2022

Kontrollutvalget i Tynset kommune inviterer til en mulig forvaltningsrevisjon av IKT-sikkerhet og personvern i IKT Fjellregionen IKS (FARTT)

På samlingen for kontrollutvalgene i FARTT-samarbeidet den 14.november ble det luftet mulige samarbeid om forvaltningsrevisjoner både på lang og kort sikt. Ut fra signalene i møtet så vedtok kontrollutvalget i Tynset at de ønsker å invitere til en felles forvaltningsrevisjon for IKT-sikkerhet og personvern. Det ble behandlet i sak 41/22 «Vurdering av ny forvaltningsrevisjon». Saken og behandlingen(møteprotokoll) er i lenken: https://konfjell.no/kontrollutvalg/tynset-kommune/

IKT-sikkerhet er et område som har høy vesentlighet og risiko ut fra vurderinger knyttet til konsekvenser for kommunene dersom noe skulle gå galt. Kontrollutvalget i Tynset har forespurt BDO som er deres selskap for forvaltningsrevisjoner, om et forslag til hvordan en slik forvaltningsrevisjon kan gjennomføres slik at en har et bedre grunnlag å ta stilling ved et eventuelt samarbeid. Forslaget følger nedenfor.

Område og avgrensning

FARTT ivaretar både felles programmer (Microsoft) og mange fagsystemer for sine fem kommuner. FARTT har også et eget IKT-sikkerhetsutvalg som indikerer at IKT-sikkerhet er ivaretatt. Personvern blir også i stor grad ivaretatt gjennom IKT-sikkerhetsrutiner. Det tas derfor utgangspunkt i at en forvaltningsrevisjon om IKT-sikkerhet og personvern omfatter denne siden av personvernet. Hvordan kommunene ivaretar personvern i sine prosedyrer, er en annen og mye mer omfattende revisjon. Det er derfor ikke lagt inn i denne forvaltningsrevisjonen.

Forslag til problemstillinger

BDO sine forvaltningsrevisjoner av IKT-sikkerhetsprosjekter bygger på en risikobasert revisjon basert på standardene ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet (Nasjonal Sikkerhetsmyndighet). **Ifølge disse, kontrolleres både må- og bør-krav til IKT-sikkerhet**.
BDO har på derfor utarbeidet følgende forslag til følgende problemstillinger som legges til grunn:

1. Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?
2. Blir sikkerhetsrisikoer identifisert og håndtert?
3. Blir informasjon og informasjonssystemer beskyttet i henhold til beste praksis?
4. Hvordan oppdages avvik og mulige trusler mot virksomheten?
5. Blir hendelser håndtert på en tilfredsstillende måte?

Både ledelse og styringssystem for informasjonssikkerhet vil bli kontrollert, samt de forebyggende tiltakene og kapasitet for hendelseshåndtering. Tilnærmingen omfatter både menneskelige, organisatoriske og teknologiske sikkerhetstiltak.

Sikkerhetstesting

Det er ikke uvanlig å inkludere en sikkerhetstesting som en del av sikkerhetsrevisjonen, og dette vil i kombinasjon med revisjonen gi tilstrekkelig verifikasjon av sikkerhetstilstanden i virksomheten. Sikkerhetstestene skal simulere angrepsteknikker som brukes av trusselaktører for å oppnå uautorisert tilgang til informasjonssystemer, eller for å påvirke tilgjengeligheten eller integriteten til systemer og data. Hensikten med testingen er å avdekke sårbarheter som utnyttes til misbruk og datakriminalitet, samt foreslå eventuelle forebyggende tiltak. For de aktuelle systemene vil BDO i samråd med selskapet finne hensiktsmessige testscenarioer. Dette må gjøres basert på systemenes verdier, trusler og mulige sårbarheter som er kartlagt i den innledende risikovurderingen. For å identifisere og simulere de mest sannsynlige trusselscenarioene vil nøyaktig omfang av sikkerhetstestingen utarbeides i samarbeid med selskapet. Resultatene fra sikkerhetstesting vil gi et godt grunnlag for å vurdere reelle angrepsvektorer og faktisk risiko, samt for å anbefale og implementere konkrete tiltak.

Budsjett

Det er skissert et budsjett på 250-300 timer. BDO tar forbehold om å komme tilbake med mer eksakt anslag når/hvis kontrollutvalgene går videre med ideen om en felles forvaltningsrevisjon på dette området. De må også vurdere tidsestimatet(forbruk av tid) for om sikkerhetstesting skal inkluderes eller ikke.

OPPSUMMERING FRA SEKRETARIATET

På møtet den 14.november ble det diskutert å gjennomføre en forvaltningsrevisjon både av selskapet og av samhandlingen mellom FARTT og kommunene. Det er i denne omgang fokusert på det som skjer i selskapet FARTT. Samhandlingen med kommunene og hvordan det jobbes med personvern i kommunene er altså ikke inkludert.
Ut fra sekretariatets vurdering, så kan det være mest hensiktsmessig å starte med selskapet for å se hvordan «grunnmuren» fungerer. Det kan gi en pekepinn på om det er flere momenter som bør undersøkes i samhandlingen med kommunene på et senere tidspunkt. Da kan den enkelte kommune følge opp med en forvaltningsrevisjon på samhandlingen mellom selskapet og den enkelte kommune gjennom sine revisjonsselskap. Dersom noen utvalg ønsker at samhandlingen med kommunene skal inngå i en eventuell forvaltningsrevisjon, så ber vi om tilbakemelding på om det er ønskelig at det skal inngå i felles forvaltningsrevisjon med BDO, og hvilke avgrensninger dere ønsker.

Dersom det er flere som ønsker at samhandlingen med kommunene skal inngå kan vi sjekke ut om det vil gi gevinster dersom de ulike revisjonsselskapene gjennomfører en slik prosess samtidig. Gevinsten kan være at de kan samarbeide om gjennomføringen, og dermed samarbeide om innhenting av informasjon, tolking av informasjon, osv.

Et budsjett på 250 -300 timer vil i praksis bety en kostnad på ca. 300 000 – 360 000 kr. Når det gjelder fordeling av kostnader så er det erfaringsmessig mest vanlig at eierandelen i selskapet legges til grunn. Tynset ønsker innspill på hvordan dere ser for dere en fordeling, og i dette tilfellet ser sekretariatet tre måter som fordelingen kan gjøres ut fra:

1. Lik fordeling mellom kommunene
2. Fordeling ut fra eierandel i selskapet

3. Ut fra fordelingsnøkkel for årlige kostander

Eierandelen i selskapet slik:

- Tynset kommune 30%
- Alvdal kommune 19%
- Rendalen kommune 18%
- Tolga kommune 17%
- Folldal kommune 16%

Fordelingsnøkkelen for årlige kostnader fordeles slik:

- 40% deles likt mellom kommunene
- 60% fordeles etter antall lisenser som den enkelte kommune har.
  Hva som er antall lisenser for den enkelte kommune har vi ikke undersøkt, men vi har forstått at det varierer en del.

Tynset legger opp til en bestilling av en prosjektplan i sitt møte den 23.februar, slik at en gjennomføring av revisjonen kan bli ferdig i inneværende periode. **Vi spør derfor om dere kan ta stilling til følgende innen den 12.februar:**

- Ønsker dere å delta på en felles forvaltningsrevisjon av IKT-sikkerhet og personvern i IKT Fjellregionen IKS (FARTT)?
- Innspill til foreslåtte problemstillinger
- Ønske om andre områder eller avgrensninger
- Er det ønskelig at samhandlingen med kommunene skal omfattes i en eventuell forvaltningsrevisjon? I tilfelle hvordan?
- Innspill/krav til fordeling av kostander

På vegne av kontrollutvalget i Tynset

Ragnhild Aashaug
sekretariat

KONTROLLUTVALG FJELL IKS