Västra Mälardalens Kommunalförbund

2023-12-11

För yttrande: Direktionen
För kännedom: Kommunfullmäktige Arboga
Kommunfullmäktige Köping
Kommunfullmäktige Kungsör
Kommunfullmäktige Surahammar

Uppföljande granskning av it-säkerhet

Västra Mälardalens kommunalförbunds förtroendevalda revisorer har genomfört en uppföljande granskning av it-säkerheten. Uppdraget ingår i revisionsplanen för år 2023.

KPMG har av Västra Mälardalens kommunalförbunds revisorer fått i uppdrag att följa upp resultatet av en tidigare genomförd granskning av it-säkerhet från 2021. Revisorerna följer regelbundet upp tidigare genomförda revisionsgranskningar som ett led i att granska om genomförda granskningsinsatser bidragit till att verksamheterna utvecklas.

Utifrån genomförd uppföljning är vår sammanfattande bedömning att förbundsdirektionen delvis hörsammat de rekommendationer som lämnades i samband med granskningen av it-säkerhet från 2021.

I den tidigare granskningen bedömdes att förbundet till viss del hade processer, rutiner och kontroll över it-säkerheten, men att arbetet inte bedrevs med ett tillräckligt riskbaserat förhållningssätt. Granskningen rekommenderade därför ett antal åtgärder med syfte att tillse att vidtagna säkerhetsåtgärder utgår från behov och riskbild.

Vi har genom den uppföljande granskningen delgivits ett antal vidtagna förbättringsåtgärder. Bland annat har en informationssäkerhetspolicy beslutats, vilken reglerar uppföljning samt roller och ansvar för det övergripande arbetet.

Dock anser vi att arbetet med riskanalyser har fortsatta utvecklingsbehov. Vi bedömer att förbundsdirektionen inte i tillräcklig omfattning efterfrågat riskanalyser eller bedömt informationssäkerhetsrisker. Vår bedömning är att förbundet i vissa väsentliga avseenden saknar ett systematiskt arbete med riskanalyser och informationsklassningar, vilket riskerar medföra att etablerade it-säkerhetsåtgärder inte motsvarar faktiska behov och aktuell hotbild.

Vi rekommenderar direktionen att:

- Föra dialog med medlemskommunerna om gränsdragning mellan medlemskommunerna och förbundet avseende informationssäkerhetsarbetet och systemförvaltningsorganisationen.

- Revidera riktlinjen för systemförvaltning med avseende på att tydliggöra vikten av att riskanalyser och informationsklassning genomförs som delar i ett riskbaserat it-säkerhetsarbete.

- Införa en modell/metod för riskanalys avseende it-infrastruktur som löpande uppdateras för att möta nya risker och hot.

- Förtydliga digitaliseringsrådets roll och ansvar i styrande dokument.

- Genomföra en riskanalys som inkluderar informationssäkerhetsrisker för förbundet och utifrån behov vidta åtgärder för att minimera eller eliminera risker för förbundet.

Kommunalförbundets revisorer begär yttrande från direktionen över bifogad rapport senast den 29 februari 2024.

Yttrandet översändes till samtliga revisorer via e:post samt till Karin Helin Lindkvist, KPMG, karin.helin-lindkvist@kpmg.se.

För revisorerna

DocuSigned by:
Lars Wigström
BC9D07A1CAE745...
Lars Wigström
Revisor, Kungsör

DocuSigned by:
Rodney Adahl
6A8BFB50FC8546D...
Rodney Adahl
Revisor, Surahammar

DocuSigned by:
Eva Leonardsson
2E2350B353AC405...
Eva Leonardsson
Revisor, Köping

DocuSigned by:
Bertil Bresell
2EC927EB5FED427...
Bertil Bresell
Revisor Arboga