Västerås stads revisorer

SENASTE NYTT Nr 5 – 2022

Granskning av IT- och informationssäkerhet

Granskningens inriktning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Iakttagelser och slutsatser

Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation. Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, ”Granskningsprogram Cyber- och Informationssäkerhet” (GCI), särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 57 punkter på en ordinarie skala från 1 (begynnande) till 5 (optimerad) inom de respektive områdena. Representanter för kommunens informationssäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

Rekommendationer

I granskningen har ett antal förbättringsområden identifieras och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Revisionen har överlämnat revisionsrapporten till kommunfullmäktige. Rapporten är publicerad på stadens hemsida www.vasteras.se
För ytterligare information, kontakta revisionens ordförande Asta Matikainen Lecklin tfn: 076-896 43 86 eller revisionssekreterare Christel Modin tfn: 076-569 48 43.