# Fördjupad granskning 2024

**Revisionen**

**2024-07-05**

# Granskning av informationssäkerhet (Dnr 2024/9003)

### Granskning av informationssäkerhet

Kommuner har ett av det svenska samhällets mest komplexa uppdrag, detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. Brister i hantering av information leder till ett försämrat förtroende för tjänster och bakomliggande aktörer. Förtroendet för en organisation tar lång tid att bygga upp, men kan snabbt raseras av en enskild informationssäkerhetsincident.

Det övergripande syftet med informationssäkerhet är att säkerställa att information för medarbetare, medborgare och andra intressenter hanteras med utgångspunkt i tillgänglighet, riktighet, konfidentialitet och spårbarhet. Med dagens snabba digitalisering blir informationssäkerhet allt viktigare. Klassning av informationstillgångar är viktigt för att säkerställa att den mest skyddsvärda informationen verkligen får det skydd som krävs.

Information är värdefull och behöver många gånger skyddas. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering, vilket i sin tur skapar förtroende både internt och externt samt är en förutsättning för att organisationen ska kunna leverera ett fullgott skydd.

Utmaningar gällande informationssäkerhet har även resulterat i NIS-direktivet, som i korthet innebär krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga och vissa digitala tjänster, både för privata och offentliga aktörer. Förslaget på det direktivet, NIS 2, inkluderar bl.a. hårdare säkerhetskrav samt ett sanktionssystem.

Revisorerna har i sin riskanalys för år 2024 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att det finns en god informationssäkerhet inom kommunen och har därför gett PwC ett uppdrag att granska området.

### Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Revisionsfrågor:

- Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning?

- Finns styrande informationssäkerhetsdokumentation och är dessa väl implementerade i verksamheten?
- Finns ett ledningssystem för informationssäkerhet implementerat?
- Sker kommunens arbete med informationssäkerhet systematiskt?
- Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet i verksamheterna?
- Finns en god struktur för behörighetshantering implementerad?

**Metod**

Granskningen genomförs med hjälp av intervjuer av identifierade nyckelpersoner i kommunen, samt inläsning och genomgång av tillgänglig dokumentation.