Kommunstyrelsen

Ulf Aspelin | Informationssäkerhetssamordnare
0734-64 70 27 | ulf.aspelin@bollebygd.se

Dnr : **KS2023/107-6**

Revisionen

Revisionsrapport; Granskning av informationssäkerhet - yttrande

Sammanfattning av ärendet

Öhrlings Pricewaterhousecoopers AB (PwC) fick i uppdrag av de förtroendevalda revisorerna i Bollebygds kommun, att genomfört en granskning av kommunens styrning av informationssäkerhetsarbetet.

Syftet med granskningen var att bedöma hur kommunstyrelsen säkerställer styrningen av informationssäkerhetsarbetet och om det sker med tillräcklig intern kontroll.

Granskningen har gått till genom att läsa och granska styrdokument, beslut och beslutsunderlag samt samtal/intervjuer med kommundirektören, IT-samordnaren och informationssäkerhetssamordnaren.

PwC:s bedömning är att kommunstyrelsen inte helt säkerställer den styrning och uppföljningen av informationssäkerhetsarbetet, samt den interna kontrollen av densamma som förväntas.

Granskning har utgått från fyra frågor, som var och en fått en bedömning av hur kommunen uppfyller dessa. Frågorna var;

- Finns ändamålsenlig styrande informationssäkerhetsdokumentation? — Delvis uppfyllt

- Finns en informationssäkerhetsorganisation med tydlig roll- och ansvarsfördelning? Delvis uppfyllt

- Sker uppföljningen av informationssäkerhets-arbetet på ett ändamålsenligt sätt? Ej uppfyllt

- Finns ett ändamålsenligt ledningssystem för informationssäkerhet? Ej uppfyllt

PwC rekommenderar efter den genomförda granskningen att kommunstyrelsen genomför följande uppdrag för att stärka kommunens systematiska informationssäkerhetsarbete.

Nedan redovisas rekommendationer:

- Policy och riktlinjer bör kompletteras och konkretiseras för att bli ändamålsenliga.
- Tydliggöra roller och ansvar.
- Identifiera och klassa information.
- Genomföra riskanalyser.
- Riskanalyserna och informationsklassningarna bör vara styrande för det operativa IT-arbetet
- Etablera och färdigställa kontinuitetsplaner för kritiska delar av verksamheten.
- En systematisk och årlig uppföljning av kommunens och förvaltningarnas informationssäkerhetsarbete.

Yttrande

Kommunstyrelsen svarar följande:

Att arbeta med de sju rekommendationerna samtidigt kommer att vara svårt, därför föreslår kommunstyrelsen en följande prioritering av arbetet med rekommendationerna;

1. **En systematisk och årlig uppföljning av kommunens och förvaltningarnas informationssäkerhetsarbete.**

   Vi har idag ett pågående arbete och vi kommer vidareutveckla vårt systematiska informationssäkerhetsarbete ska anpassas för verksamhetens förutsättningar och finnas med som en del i verksamhetsplanen. Detta arbete ska vara en del av kommunens och förvaltningarnas årshjulen utifrån behov, och vara integrerat till 2023.

   Systematiskt informationssäkerhetsarbete är att arbeta förebyggande och att kontinuerligt anpassa skyddet utifrån organisationens behov och risker. Det handlar även om att förhindra att vår information läcker ut, förvanskas eller förstörs. Som stöd i detta arbete används material från Myndigheten för Samhällsskydd och Beredskap (MSB); www.informationssakerhet.se

   Arbetet kommer starta under hösten 2023 och vara del i kommunens säkerhetsarbete från januari 2025.

1. **Identifiera och klassa information.**

   Informationsklassning är ett tillvägagångssätt som hjälper kommunens verksamheter att välja rätt åtgärder för att skydda sin information. Att identifiera förvaltningarnas information och sedan klassa den har påbörjats, men sker inte systematiskt eller etablerat.

   Som stöd i detta arbete kommer SKR:s verktyg KLASSA v4 användas. Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder för att skydda information.

Arbetet kommer starta under hösten 2023.

2. **Genomföra riskanalyser.**

   Riskanalyser kommer att görs för att förstå vilka händelser som kan påverka våra verksamhetssystem negativt, vilka konsekvenser det får och hur sannolikt det är att det händer. Resultatet från analysen blir att införa åtgärder som tar bort, minskar eller minskar konsekvensen om den inträffar. Vi kan under vissa omständigheter välja att acceptera risken som den är. De identifierade riskerna tas fram genom en systematisk process.

   Arbetet kommer starta senast kvartal 2 2024 och beräknas vara klart i december 2024

3. **Riskanalyserna och informationsklassningarna bör vara styrande för det operativa IT-arbetet.**

   Framtagande och införande av ett Ledningssystem för informationssäkerhet (LIS) som är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter med policy, riktlinjer och rutiner. Syftet med LIS är att bedöma informationens värde och känslighet. Informationsklassning och riskanalys är de fundamentala komponenterna i detta sammanhang.

   Klart i Q1 2025.

4. **Etablera och färdigställa kontinuitetsplaner för kritiska delar av verksamheten.**

   Vi har ett pågående arbete med kontinuitetsplaner. Detta arbete är ständigt pågående och utvecklas hela tiden. Arbetet ingår i vårt Risk och Sårbarhetsanalysarbete, RSA. Arbetet börjar med

att identifiera vilka delar av verksamheten som är mest kritisk och behöver fungera oavsett störning.

Beräknas vara klart Q1 2024.

5. **Policy och riktlinjer bör kompletteras och konkretiseras för att bli ändamålsenliga.**

   Förvaltningarnas arbete med att skapa sina rutiner för sitt arbete med informationssäkerhet och dataskydd har slutförts hos en förvaltning och till vissa delar påbörjats under 2023, där förvaltningscheferna beslutar om rutinen i samverkan med sina chefer.

   Arbetet klart december 2023

6. **Tydliggöra roller och ansvar.**

   Grundprincipen är att ansvaret för informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret. Detta gäller ända från ledning ner till enskilda medarbetare. Denna princip innebär att den person som är ansvarig för ett visst verksamhetsområde också är ansvarig för informationssäkerheten inom det specifika området.

Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Därtill följer ett särskilt ansvar kopplat till roller och för olika yrkeskategorier.

I förvaltningarnas rutindokument finns alla roller beskrivna och vilket ansvar som vilar på rollen.

Klart december 2023.

Samlad bedömning

Syftet med granskningen har varit att bedöma om kommunstyrelsen säkerställer att styrningen av informationssäkerhetsarbetet är ändamålsenlig och om detta sker med tillräcklig intern kontroll. PwC bedömning är att kommunstyrelsen delvis säkerställer en ändamålsenlig styrning men att tillräcklig uppföljning och intern kontroll inte sker.

PwC har sett att arbetet med att införa ett systematiskt arbetssätt och ett LIS är påbörjat. De noterade även en berömvärd insikt om brister avseende informationssäkerhetsarbetet och om angelägenheten av ett väl fungerande sådant arbete. Dessa insikter ska konkretiseras i specifik styrning och uppföljning av området för att styrningen ska bli ändamålsenlig.

BOLLEBYGDS KOMMUN
Kommunstyrelsen

Ulf Rapp	Monica Holmgren
Ordförande	Förvaltningschef

Denna skrivelse har godkänts digitalt och saknar därför namnunderskrifter.