Regionstyrelsen 2025-06-16

Yttrande – Fördjupad granskning nr 6/2025 av informationssäkerhet *(RS 410-2026)*

Sammanfattning

Regionstyrelsen har fått i uppdrag att besvara revisionens granskning dnr REV 37-2025.

Underrubrikerna i detta yttrande motsvarar de rekommendationer som lämnas i granskningsrapporten, och svaret redovisas nedan utifrån dessa.

Säkerställa att Cosmic uppfyller tillämpliga interna krav och lagkrav. För att åtgärda detta behöver regionens process för krav mot leverantören formaliseras.

Regionstyrelsen vidtar följande åtgärder:

Struktur för att arbeta löpande med avtalsuppföljning finns på plats. Det har tillsatts en regional avtalsgruppering som samordnas av objektledningen för VISA-objektet. Regionalt avtalsansvarig finns även representerad i SUSSAs avtalsgruppering. Där följs alla avtalade krav upp, inkluderat säkerhetskrav och andra lagkrav.

Inom VISA objektet arbetas det löpande med krav utifrån klassning av informationstillgångarna, vilket är ett kontinuerligt arbete.

Tydliggöra ansvarsfördelningen mellan regionen, Sussa och Cambio. Styrelsen behöver säkerställa att regionen självständigt kan initiera, driva och följa upp frågor som krävs för att uppfylla tillämpliga lagkrav.

Regionstyrelsen vidtar följande åtgärder:

Regionen har det fulla ansvaret för informationssäkerhet och regelefterlevnad. SUSSA fungerar som gemensam beställar- och samordningsfunktion mellan regionerna. Cambio ansvarar för systemets säkerhet och leverans enligt avtal.

Detta uppnås genom att definiera fastställda roller och tydligt kommunicera respektive ansvarsområden.

Fastställa och förankra interna roller och ansvar inom informationssäkerhet, dataskydd och objektsförvaltning. Det behöver finnas en tydlig och gemensam förståelse för samtliga roller och det ansvar som respektive funktion har.

Regionstyrelsen vidtar följande åtgärder:

I samband med den nya cybersäkerhetslagen och tillhörande föreskriften ska rollerna ses över, styrdokumenten uppdateras och kommuniceras till berörda parter.

Stärka riskhanteringsarbetet genom tydligare riktlinjer och ansvarsfördelning. Detta inkluderar att stärka den interna kontrollen i syfte att säkerställa att identifierade risker och sårbarheter dokumenteras i åtgärdsplaner och följs upp till dess att riskerna kan bedömas som acceptabla.

Regionstyrelsen vidtar följande åtgärder:

Riskhanteringsarbetet sker i linje med den övergripande styrningen för riskhantering. Riskhantering är en del av det systematiska cybersäkerhetsarbetet och ligger till grund för de säkerhetsåtgärder som beslutas under ledningens genomgång. Uppföljningsstrukturen för beslutade säkerhetsåtgärder har reviderats och förändring med löpande ledningsförankring har genomförts.

Det systematiska cybersäkerhetsarbetet inkluderat riskhantering ska förtydligas ytterligare genom processbeskrivning i ledningssystemet.

Säkerställa att styrande dokument som ingår i ledningssystem för informationssäkerhet är uppdaterade och kompletta för att motsvara interna och externa krav.

Regionstyrelsen vidtar följande åtgärder:

Under januari 2026 har en översyn av samtliga dokument inom ledningssystemet för cybersäkerhet genomförts. Arbetet med revidering har initierats i syfte att säkerställa att dokumenten uppfyller krav enligt aktuell lagstiftning och kommande föreskrifter.

Eftersom de nya föreskrifterna ännu inte är fastställda behöver Region Västerbotten invänta dessa innan beslut om ny styrning kan fattas.