Regionstyrelsen

2026-09-08

Uppföljning - Regionstyrelsens redovisning av åtgärder med anledning av regionfullmäktiges anmärkning

Sammanfattning

Detta ärende utgör en uppföljning av de åtgärder som har genomförts och planeras för att hantera identifierade risker och brister i journalsystemet Cosmic. Regionstyrelsen kommer vid sammanträdet i september 2026 att informeras om genomförda åtgärder samt om det fortsatta arbetet.

Uppföljningarna kommer också att ligga till grund för ett samlat ärende i regionstyrelsen (RS 460-2026), utifrån det uppdrag som regionfullmäktige har gett regionstyrelsen genom beslut den 28 april 2026, § 63 (RS 364-2026). Uppdraget innebär att regionstyrelsen, tillsammans med hälso- och sjukvårdsnämnden, ska redovisa genomförda och planerade åtgärder för att hantera identifierade risker och brister i journalsystemet Cosmic. Uppdraget ska återrapporteras till regionfullmäktige vid sammanträdet i november 2026.

Revisorernas granskning visar på brister i styrelsens och nämndens styrning och kontroll inför driftsättningen av systemet. Styrelsen och nämnden säkerställde inte att förberedelserna varit tillräckliga innan systemet började användas. Exempelvis visar granskningen att utbildningen till vårdens medarbetare inte varit tillräcklig. Utbildningen förberedde inte medarbetarna i tillräcklig grad för att kunna använda Cosmic.
Granskningen visar också att flera riskanalyser som var genomförda innan Cosmic driftsattes identifierade allvarliga och väsentliga risker, trots detta vidtog styrelsen och nämnden inte några konkreta åtgärder för att hantera eller minimera riskerna.
Revisorernas granskning visar att det finns betydande risker och sårbarheter i Cosmic som innebär att regionen inte uppfyller interna och externa riktlinjer och lagkrav inom informationssäkerhetsområdet. De bedömer att dessa sårbarheter innebär en betydande risk för regionens IT-säkerhet. Bristerna som granskningen uppmärksammat skulle också kunna få allvarliga konsekvenser för patienter och medborgare.

Genomförda åtgärder

Revisorerna rekommenderar i Fördjupad granskning nr 5-2025 (RS 409-2026) regionstyrelsen och hälso-och sjukvårdsnämnden att;
- Utvärdera införandet av Cosmic.
- Tydliggöra och fastställa ansvar och roller.
- Säkerställa att systemet utvecklas efter verksamheternas behov samt att verksamheterna får förutsättningar att använda systemet på ett sådant sätt att

nyttoeffekter uppstår.

Regionstyrelsens förvaltning har genomfört en uppföljning i samband med programmets avslutande och upprättandes av FVIS slutrapport (RS 118-2025). Objektägare för VISA ansvarar för uppföljning av indikatorer för genomförda verksamhetsförändringar och initierar via regionens planerings-, budget- och uppföljningsprocess ytterligare verksamhetsförändringar som behövs för att realisera förväntade nyttor.

Arbetet med att säkerställa att systemet utvecklas efter verksamheternas behov bedrivs enligt en nyttorealiseringsplan för kontinuerligt förbättringsarbete. Det inkluderar att arbeta med organisationen, regionalt i objektet och i SUSSA samverkan.

Revisorerna rekommenderar i Fördjupad granskning nr 6-2025 (RS 410-2026) att regionstyrelsen och hälso- och sjukvårdsnämnden säkerställer att;
- Cosmic uppfyller tillämpliga interna krav och lagkrav
- Tydliggöra ansvarsfördelningen mellan regionen, Sussa och Cambio
- Fastställa och förankra interna roller och ansvar inom informationssäkerhet, dataskydd objektförvaltning
- Stärka riskhanteringsarbetet genom riktlinjer och ansvarsfördelning
- Säkerställa att styrande dokument som ingår i ledningssystemet för informationssäkerhet är uppdaterade.

Regionstyrelsens förvaltning arbetar med att ta fram en struktur för löpande avtalsuppföljning. I samband med den nya cybersäkerhetslagen och tillhörande föreskriften ska roller och ansvarsfördelning ses över, styrdokumenten uppdateras och kommuniceras till berörda parter.

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.

Den behörighetsproblematik som funnits inom systemet är nu åtgärdad. Vilket har resulterad i en förbättrad styrning av behörigheter och åtkomst. Säkerhetskraven har integreras i förvaltningen av systemet samt vidareutveckling.

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.

Planerade åtgärder

Extern granskning av Cambio avseende cybersäkerhet planeras inom en treårsperiod och görs gemensamt i Sussa.

Pågående riskanalysarbete inför ny objektplan 2027. VISA-objektet arbetar med att revidera riskanalys, konsekvensbedömning, lämplighetsbedömning, handlingsplan KLASSA, följa upp säkerhetstesterna samt de externa granskningarna

Lyft behov av fortsatta resurser inom VISA objektet gällande användarstöd.

Förslag till beslut

Informationen är delgiven.