region västerbotten

REVISORERNAS BEDÖMNINGAR

2026-04-20 REV 37-2025

Regionstyrelsen
Hälso- och sjukvårdsnämnden

Granskning av informationssäkerhet

Det finns betydande risker och sårbarheter i Cosmic som innebär att regionen inte uppfyller interna och externa riktlinjer och lagkrav inom informationssäkerhetsområdet. Vi 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.

En stor del av bristerna var identifierade och kända innan Cosmic driftsattes. Regionstyrelsen har löpande tagit del av uppföljning och information från FVIS-programmet inför driftsättningen av systemet. Utifrån styrelsens ansvar för regiongemensamma system, bedömer vi att det är en allvarlig brist att styrelsen inte efterfrågat underlag eller rapportering över att riskerna var på en acceptabel nivå innan systemet togs i drift.

Granskningen visar att hälso- och sjukvårdsnämnden inte var delaktig i beslutet att påbörja personuppgiftshanteringen i Cosmic. Utifrån nämndens personuppgiftsansvar för informationen som hanteras i Cosmic, bedömer vi att det är en allvarlig brist att nämnden inte tagit del av information och beretts möjlighet att ta ställning till de risker och konsekvenser som föreligger med den personuppgiftsbehandling och journalföring som sker i Cosmic.

Trots att det fanns dokumenterade risker och sårbarheter av betydande karaktär när Cosmic driftsattes, visar granskningen att inga konkreta förbättringsinsatser har genomförts efter systemet började användas i april 2025. Styrelsen och nämnden har inte heller säkerställt att några kompensatoriska åtgärder vidtagits tills en varaktig lösning är implementerad. Oklara samarbetsformer mellan regionen, Sussa och leverantören har sannolikt bidragit till styrelsens och nämndens passiva hantering av bristerna. Regionen har i hög grad förlorat kontroll över centrala delar inom informationssäkerhetsområdet som inte kan delegeras vidare.

Revisorerna har enhälligt ställt sig bakom dessa bedömningar och slutsatser. I en bilaga lämnar revisorerna sina rekommendationer till regionstyrelsen och hälso- och sjukvårdsnämnden. Revisorerna lämnar denna skrivelse samt underliggande rapport (nr 6/2025) till styrelsen och nämnden för yttrande. Yttrande med uppgifter om verkställda och planerade åtgärder ska lämnas till revisionskontoret senast den 2 oktober 2026.

För regionens revisorer

Edward Riedl
Ordförande

Bert Öhlund
Vice ordförande

Bilaga Revisorernas rekommendationer och instruktioner för yttrande

Revisorernas rekommendationer

Vi rekommenderar regionstyrelsen och hälso- och sjukvårdsnämnden att:

- Säkerställa att Cosmic uppfyller tillämpliga interna krav och lagkrav. För att åtgärda detta behöver regionens process för krav mot leverantören formaliseras.
- 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.
- 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.
- 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.
- Säkerställa att styrande dokument som ingår i ledningssystem för informationssäkerhet är uppdaterade och kompletta för att motsvara interna och externa krav.

Instruktioner för yttrande

Det ska vara enkelt att utläsa vilka åtgärder som styrelsen och nämnden vidtagit eller planerar att vidta. Tänk därför på detta när ni svarar:

- Lämna ett svar för varje rekommendation som revisorerna lämnat. Det ska finnas en tydlig koppling mellan rekommendationerna och de åtgärder som vidtagits eller planeras vidtas.
- Svara så konkret som möjligt. Ange gärna hur åtgärderna ska genomföras, vem som ska genomföra dem och när.
- Om styrelsen och nämnden inte tänker vidta några åtgärder, motivera varför.
- Om styrelsen och nämnden inte kan svara på utsatt tid, kontakta undertecknad.
- Inkommet yttrande kommer att publiceras på www.regionvasterbotten.se/revision. Tänk på att yttrandet ska vara tillgänglighetsanpassat för att publiceras på regionens webbplats.

Vid frågor kontakta

Malin Hedlund
Revisionskontoret
090-785 73 70
Malin.k.hedlund@regionvasterbotten.se