Hälso-och sjukvårdsnämnden

2026-10-05 HSN 1343-2026

Hälso-och sjukvårdsnämndens redovisning av åtgärder med anledning av revisionens granskning av Cosmic

Sammanfattning

Hälso- och sjukvårdsnämnden (HSN) har, tillsammans med regionstyrelsen, fått i uppdrag av regionfullmäktige att till fullmäktiges sammanträde i november 2026 redovisa genomförda och planerade åtgärder för att hantera de risker och brister som identifierats i journalsystemet Cosmic.

Uppdraget till hälso-och sjukvårdsnämnden följer av regionfullmäktiges beslut den 28 april 2026, § 63 (RS 364-2026), där anmärkning riktades mot hälso- och sjukvårdsnämndens ordförande för passiv och bristande styrning och kontroll av identifierade risker och brister i systemet.

Hälso- och sjukvårdsnämnden har fortlöpande informerats om arbetet vid sammanträdena i juni, september och oktober. Detta underlag innehåller en samlad redovisning av de åtgärder som genomförts sedan april samt de fortsatta åtgärder som planeras för att hantera identifierade risker och brister.

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.

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.

Vilken roll och vilket ansvar nämnden har i de frågor som granskningen berör

Nämnderna ska var och en inom sitt område se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten.
De ska också se till att den interna kontrollen är tillräcklig för att förebygga fel och oegentligheter i verksamheten, och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt, enligt kommunallagen 6 kap. 6 §.

Detsamma gäller när skötseln av en kommunal angelägenhet med stöd av 10 kap. 1 § har lämnats över till någon annan.

Enligt regionstyrelsens reglemente 2.2 styrelsens övergripande uppgifter:
5. ha hand om regionkommunens personaladministrativa system, ekonomisystem, dokument- och ärendesystem, epostsystem, IT-system, kommunikationssystem, skaderapporteringssystem, passersystem och förtroendepersons register och andra regionövergripande system.

Det vill säga att regionstyrelsen har förvaltningsansvar för Cosmic precis som alla andra system inom RV. HSN är användare av Cosmic och ansvarar för att anmäla brister och incidenter till förvaltningen.

Vilka åtgärder nämnden avser att vidta med anledning av granskningen

Fortlöpande rapportering av eventuella brister och incidenter för att säkerställa att verksamheten bedrivs på ett tillfredsställande sätt för att förebygga fel och oegentligheter.

Hur de föreslagna åtgärderna ska genomföras samt när och hur nämnden ska följa upp åtgärderna

Fortlöpande rapportering av eventuella brister och incidenter. Uppföljning genom löpande återrapportering.

Hälso-och sjukvårdsnämnden 22 oktober 2026, § 145