Regionstyrelsen 2026-11-10 591321

**Regionstyrelsens redovisning av åtgärder med anledning av revisionens granskning av Cosmic**

**Bakgrund**
I revisionsberättelsen riktar revisonen anmärkning mot regionstyrelsen och ordförande i hälso - och sjukvårdsnämnden för passiv och bristande styrning och kontroll över identifierade risker i journalsystemet i Cosmic. Som underlag till denna anmärkning har två granskningar genomförts, en för själva införandet och den andra kopplat till IT-datasäkerhet. Dessa två går in i varandra och nämnderna har yttrat sig i granskningarna till revision.

Yttrande för anmärkningarna gavs till fullmäktige i Juni både från regionstyrelsen och ordförande i hälso och sjukvårdsnämnden, den huvudsakliga åtgärden var att respektive nämnd löpande följer upp framdriften och planerade åtgärder, vilket är gjort. I beslutet från fullmäktige ska sammantaget av åtgärderna återrapporteras i november.

Införande och utveckling i samverkan gemensamt med övriga regioner och en leverantör är en komplex process. Tidsplanen har var utmanande och svåra prioriteringar genomfördes för att möta tidsplanen. Införandet gick över förväntan men behovet av vidareutveckling av grundkonfigurationen var tydligt och det är nog inte så konstigt heller.

Åtgärder kopplat till revisionsgranskningarna och yttranden till fullmäktige.

**Införandegranskningen och dess åtgärder**

**Utvärdering av projektet. (RS409-2026)**
En slutrapport är redovisat och viktiga lärdomar är identifierade (RS 118-2025)
Slutrapport på SUSSA nivå är genomfört och återrapporterat
Portföljförvaltare för Utvecklingsportföljen följer upp och rapporterar nyttor och effekter under minst 5 år utifrån nyttokalkyl och fastställda indikatorer.
Portföljen kan föreslå ytterligare utveckling av arbetssätt och teknik för att förväntade nyttor ska uppnås.

Objektägare ”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

**Tydliggör roller och ansvar mellan olika förvaltningar**
Den grundläggande ansvarsfördelningen är klargjort sedan tidigare av fullmäktige, förenklat är styrelsen ansvarig för själva systemet och dess innehåll, kontakter mot SUSSA och leverantör. Hälso-sjukvårdsnämnden är ansvarig för att rapportera avvikelser och behovsställare, det klargörs också i objektet VISA som är bemannat med både teknik och verksamhet.
Objektet VISA ständigt förbättrar sitt arbetssätt, roller och ansvar

**Säkerställa att systemet utvecklas efter verksamheternas behov samt att verksamheten får förutsättningar att använda systemet på ett sådant sätt att nyttorna uppstår.**

En nyttorealisering plan är skapat, beslutad och löpande följs upp av såväl förvaltning som av regionstyrelsen.
Extra utbildningsstöd efter införandet är genomfört, löpande torsdagsutbildningar.
Grundutbildning för nyanställda, kliniskt kunskapsstöd och beslutstöd är infört (UpToDate)

**Stöd till ledning och styrning**
•Objektet har deltagit på olika chefsmöten
•Rapportering till Hälso- och sjukvårdens ledningsgrupp.
•Objektets styrgrupp bemannas av flera chefer inom Hälso- och sjukvården
•Arbete med att uppnå effektiv uppföljning av kvalitet och produktion genom flexibel utdata i samarbete med Objekt Data och Analys samt Objekt Ekonomi
•Styrande dokument från Sussa samverkan publiceras i ledningssystemet
•Kliniskt Rekommendarionsråd (KRR)
•Deltagande i Styrgruppen för Hälsoinformatik i Region Västerbotten
•Kvalitetsforum hanterar samtliga ändringsbegäran

**Organisation**
•Etablering av förvaltning för Cosmic med tydlig samverkan mellan vårdverksamhet och teknik i enlighet med regionens objektmodell.
•Samverkan mellan objekt via objektteam med olika ansvarsområden

**Sussa samverkan**
•Objektet VISA bemannar Sussa vårdstöds Utvecklingsforum, Ändringsråd och Change Advisory Board (CAB) samt en antal andra forum och grupperingar

**Regionstyrelsen beslutade 2026-04-17 att genomföra ett SUSSA gemensamt förbättringsprojekt som löpande följs upp i regionstyrelsen.**
SUSSA som samverkansorgan behöver gå från en utveckling/implementationsorganisation till en leveransorganisation, de frågorna drivs av den sk beställargrupp inom SUSSA , regiondirektören är regionens representant.
Objektet VISA jobbar med en utvecklingsplan för att ta ytterligare steg

**Granskningen IT säkerhet och dess åtgärder.RS 410-2026**

**För hög behörighet för vissa medarbetare**
Införande av behörigheter sker enligt rutin efter individuellt behov och riskanalys
Säker inloggning genom dubbel autentisering i Cosmic
Systemstöd för samtyckeshantering i sammanhållen journalföring införd

**Säkerställa att Cosmic uppfyller tillämpliga interna krav och lagkrav. För att åtgärda detta behöver regionens process för krav mot leverantören formaliseras.**
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. SUSSA planerar en ytterligare revision

**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**.
I samband med den nya cybersäkerhetslagen och tillhörande föreskriften ska rollerna ses över, styrdokumenten uppdateras och kommuniceras till berörda parter.
Införande av behörigheter.
Kontinuerligt cybersäkerhetsarbete inom objektet med stöd av genomförd klassning och tillhörande handlingsplan

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

**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**.
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.