Fördjupad granskning 6/2025

Granskning av informationssäkerhet

April 2026
Jenny Thörn, Helena Olsson
Azets Revision & Rådgivning
Diarienummer: REV 37-2025

region västerbotten

Granskning av informationssäkerhet

Rapport

Region Västerbotten

2026-03-10

Antal sidor: 25

1 INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING

Azets Revision & Rådgivning har av Region Västerbottens revisorer fått uppdraget att granska regionens följsamhet till interna och externa krav inom informationssäkerhet efter införandet av nytt vårdinformationssystem. Uppdraget har även avsett granskning av organisation och ansvarsfördelning vid övergång från projekt till förvaltning med fokus på informationssäkerhetsarbetet.

Granskningen har syftat till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt följsamhet till interna och externa krav inom informationssäkerhet för nytt vårdinformationssystem. Granskningen har även haft som syfte att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden hörsammat tidigare lämnade rekommendationer i granskning av informationssäkerhet.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt följsamhet till interna och externa krav inom informationssäkerhet för nytt vårdinformationssystem.

Vår samlade bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden endast delvis har hörsammat tidigare lämnade rekommendation i granskning av informationssäkerhet.

Den samlade bedömningen grundar sig i att Region Västerbotten, sedan driftsättning av Cosmic, inte har vidtagit nödvändiga åtgärder för att utveckla eller stärka området. Trots att det finns dokumenterade risker och sårbarheter av betydande karaktär har inga konkreta förbättringsinsatser kunnat verifieras under granskningen.

Vidare konstaterar vi att det visserligen finns styrande dokument och arbetssätt inom området men att det inom regionen, utifrån de intervjuer vi genomfört, i praktiken inte förefaller finnas en tydlig förståelse för ansvarsfördelningen. Samarbetsformerna mellan regionen, SUSSA och Cambio framstår som oklara, vilket har lett till att regionen i hög grad har blivit beroende av SUSSA och därigenom förlorat kontroll över centrala delar som ej kan delegeras vidare.

Vad gäller uppföljning av den tidigare granskningen så baserar vi vår samlade bedömning på att informationssäkerhetsarbetet inom flera områden fortfarande är bristfälligt i relation till de rekommendationer som lämnades. Bland annat är styrande dokument utgångna eller inte samstämmiga vad gäller benämning av ansvar och roller och nyckelfunktioner som deltar i det operativa arbetet saknas i beskrivningarna i de styrande dokumenten. Det finns en uppföljning i form av årsberättelse som tas fram på regionövergripande nivå. Det saknas dock ännu former för uppföljning avseende efterlevnad av att regionen efterlever lagkrav och interna krav inom informationssäkerhet.

I det följande redovisas bedömning av respektive revisionsfråga:

Granskningen avser att besvara om regionstyrelsen och hälso- och sjukvårdsnämnden:	
Säkerställt att risker och sårbarheter som kvarstod vid driftsättning åtgärdats så att dessa är på en acceptabel nivå och efterlever lagkrav?	Nej
Säkerställt att etablerade säkerhetsåtgärder utvärderats genom penetrationstest eller andra it-säkerhetsanalyser internt hos regionen eller hos leverantören?	Nej
Säkerställt att systemet har en ändamålsenlig åtkomsthantering som säkerställer följsamhet till lagkrav?	Nej
Säkerställt att beslutade behörighetsmodeller finns som utgår från risk- och behovsbedömning, samt att tilldelade behörigheter följs upp genom regelbundna loggkontroller?	Nej
Säkerställt en tydlig ansvarsfördelning mellan styrelse och nämnd samt mellan regionen, SUSSA och systemleverantören som säkerställer ett ändamålsenligt informationssäkerhetsarbete?	Nej
Säkerställt att åtgärder vidtagits i relation till tidigare lämnade rekommendationer?	Endast delvis

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Utifrån våra iakttagelser och bedömningar rekommenderar vi regionstyrelsen och hälso- och sjukvårdsnämnden att:

- **Säkerställa att styrande dokument som ingår i ledningssystem för informationssäkerhet är uppdaterade och kompletta för att motsvara interna och externa krav**
  Vi rekommenderar att styrdokumenten ses över och ger förutsättningar för regionens verksamhet att efterleva de informationssäkerhetskrav som ställs på regioner. Regionen bör därtill säkerställa att ledningssystemet för informationssäkerhet är strukturerat och kan utgöra ett tydligt ramverk för det arbete som verksamheterna ska utföra.

- **Fastställa och förankra interna roller och ansvar**
  Vi rekommenderar att Region Västerbotten säkerställer en tydlig och gemensam förståelse för samtliga roller och det ansvar som respektive funktion bär. Alla berörda, regionstyrelsen, hälso- och sjukvårdsnämnden samt berörda tjänstepersoner, bör ha en klar uppfattning om vad som förväntas av dem samt deras respektive åtaganden inom informationssäkerhet och dataskydd.
- **Tydliggöra ansvarsfördelningen mellan regionen, SUSSA och Cambio**
  Vi rekommenderar att ansvar, befogenheter och mandat formaliseras och kommuniceras på ett strukturerat sätt mellan Region Västerbotten, SUSSA och Cambio. Detta för att säkerställa att Region Västerbotten självständigt kan initiera, driva och följa upp frågor som krävs för att uppfylla tillämpliga lagkrav. Detta innefattar även att etablera en tydlig process för återkoppling från SUSSA och Cambio av inrapporterade fel och brister, inklusive tidsramar för när åtgärder förväntas vara genomförda.
- **Säkerställa att det systemstöd som används uppfyller tillämpliga interna krav och lagkrav**
  Vi rekommenderar att organisationen säkerställer att det systemstöd som används inom området är ändamålsenligt och uppfyller relevanta lagkrav. Detta inkluderar att systemet möjliggör korrekt hantering av åtkomst för användare i enlighet med gällande regelverk. För att åtgärda detta behöver regionens process för krav mot leverantören formaliseras.
- **Stärka riskhanteringsarbetet genom tydligare riktlinjer och ansvarsfördelning**
  Vi rekommenderar att riktlinjen för riskhantering i Region Västerbotten implementeras för att tydliggöra krav på genomförande av riskanalyser och åtgärder samt process för att acceptera risker. Den interna kontrollen behöver därtill stärkas i syfte att säkerställa att identifierade risker och sårbarheter dokumenteras i åtgärdsplaner och löpande följs upp till dess att riskerna kan bedömas som acceptabla.

2 BAKGRUND

Azets Revision & Rådgivning har av Region Västerbottens revisorer fått uppdraget att granska regionens följsamhet till interna regler inom informationssäkerhet efter införande av nytt vårdinformationssystem. Uppdraget har även avsett granskning av organisation och ansvarsfördelning vid övergång från projekt till förvaltning med fokus på informationssäkerhetsarbetet. Uppdraget ingår i revisionsplanen för år 2025.

Regionstyrelsen och hälso- och sjukvårdsnämnden har i tidigare fördjupningsgranskningar fått kritik för brister i sitt informationssäkerhetsarbete. Granskningarna påvisade brister inom styrning, organisation samt kontroll och uppföljning. Därtill saknades etablerade processer för riskhantering. I denna granskning har en översiktlig uppföljning av tidigare lämnade rekommendationer genomförts som del i den fördjupade granskningen.

Under de senaste åren har ett omfattande arbete genomförts i syfte att byta journalsystem i Region Västerbotten. Arbetet har samordnats med ytterligare åtta regioner i den så kallade SUSSA[1] - samverkan. I april 2025 införde Region Västerbotten systemet. Regionerna har etablerat en gemensam objektsförvaltningsorganisation vilken syftar till att möjliggöra en säker och kostnadseffektiv regiongemensam styrning av systemförvaltning, support och it-drift.

Revisorerna har sedan år 2021 löpande följt arbetet i regionen med att införa Cosmic. I granskningarna har revisorerna identifierat stora risker förknippade med införandet av systemet. Risker och sårbarheter har identifierats inom flera områden, exempelvis funktionalitet, säkerhet och juridik. Revisorerna bedömer att det finns risk för att identifierade risker och avvikelser inte har följts av relevanta åtgärder så att risker nått en acceptabel nivå.

Revisorerna såg därför ett behov av att granska om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att informationssäkerhetsarbetet efter införandet efterlever interna regelverk och tillämpliga lagkrav. Revisorerna såg även behov av att följa upp de rekommendationer som lämnades i granskning av informationssäkerhet 2022.

[1] Strategisk utveckling av sjukvårdsstödjande applikationer

3 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

Granskningen syftar till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt följsamhet till interna och externa krav inom informationssäkerhet för nytt vårdinformationssystem.

Granskningen syftar även till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden hörsammat tidigare lämnade rekommendationer i granskning av informationssäkerhet.

Granskningen avser att besvara om regionstyrelsen och hälso- och sjukvårdsnämnden:

1. Säkerställt en tydlig ansvarsfördelning mellan styrelse och nämnd samt mellan regionen, SUSSA och systemleverantören som säkerställer ett ändamålsenligt informationssäkerhetsarbete?
2. Säkerställt att risker och sårbarheter som kvarstod vid driftsättning åtgärdats så att dessa är på en acceptabel nivå och efterlever lagkrav?
3. Säkerställt att etablerade säkerhetsåtgärder utvärderats genom penetrationstest eller andra it-säkerhetsanalyser internt hos regionen eller hos leverantören?
4. Säkerställt att systemet har en ändamålsenlig åtkomsthantering som säkerställer följsamhet till lagkrav?
5. Säkerställt att beslutade behörighetsmodeller finns som utgår från risk- och behovsbedömning, samt att tilldelade behörigheter följs upp genom regelbundna loggkontroller?
6. Säkerställt att åtgärder vidtagits i relation till tidigare lämnade rekommendationer?

3.1 AVGRÄNSNING

Granskningen avser regionstyrelsen och hälso- och sjukvårdsnämnden och avgränsats till Region Västerbottens interna arbete.

Revisionsfrågorna 1–5 avser endast informationssäkerhetsarbetet i relation till nytt vårdinformationssystem Cosmic.

Revisionsfråga 6 avser det övergripande informationssäkerhetsarbetet i regionen men avgränsas till de rekommendationer som presenteras i granskningsrapport från 2022.

4 REVISIONSKRITERIER

Granskningen har utgått från nedanstående revisionskriterier:

- 6 kap. 6 § kommunallagen (2017:725), KL
- Tillämpbara interna regelverk och beslut
    - Informationssäkerhetspolicy
    - Reglementen för regionstyrelsen och hälso- och sjukvårdsnämnden

- Delegationsordning för regionstyrelsen och hälso- och sjukvårdsnämnden

Det finns ett flertal lagkrav och föreskrifter som måste beaktas när information hanteras i digitala informationssystem. Vi redogör för gällande revisionskriterier översiktligt för att underlätta läsbarhet i rapporten men vill poängtera att kraven är både komplexa och omfattande och kan bestå av ytterligare reglering än den som presenteras i rapporten.

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster[2]

Hälso- och sjukvård har varit en av de sektorer som omfattats av lagen sedan 2018. Inspektionen för vård och omsorg (IVO) utgör tillsynsmyndighet för regionernas arbete och följsamhet till lagen.

Enligt lagen ska organisationer ha ett ledningssystem för informationssäkerhet som säkerställer ett systematiskt och riskbaserat arbete. Arbetet ska som minst uppnå eller motsvara kraven enligt standarden ISO 27001 och 27002. Standarden reglerar organisatorisk säkerhet, personalsäkerhet, it-säkerhet och fysisk säkerhet. Det ställs särskilda krav på att etablera säkerhetsåtgärder för att skydda informationstillgångarnas konfidentialitet, riktighet, tillgänglighet och spårbarhet.

- Dataskyddsförordningen (GDPR)

Dataskyddsförordningen består av 99 artiklar och 173 beaktandesatser som utgör bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter. Nedan presenteras några i urval som vi särskilt bedömt väsentliga i den här granskningen.

Artikel 24: Den personuppgiftsansvariges ansvar

Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen.

Artikel 28: Personuppgiftsbiträden

Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.

Artikel 35: Konsekvensbedömning avseende dataskydd
Om en typ av behandling, särskilt vid användning av ny teknik, sannolikt leder till en hög risk för fysiska personers rättigheter, ska den personuppgiftsansvarige göra en

[2] Lag och föreskrift har upphävts 2026-01-15 genom SFS 2025:1507 Cybersäkerhetsförordning som kompletterande bestämmelser utifrån Cybersäkerhetslagen (2025:1506).

konsekvensbedömning av den planerade behandlingens inverkan på skyddet av personuppgifter (DPIA).

Artikel 36: Förhandssamråd
Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten (IMY) innan behandling påbörjas om en konsekvensbedömning (art. 35) visar att behandlingen skulle leda till en hög risk om inga åtgärder vidtas för att minska risken.

- Patientdatalagen (2008:355)
- Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården

I såväl Patientdatalagen (PDL)[3] som Socialstyrelsens förskrifter om journalföring och behandling av personuppgifter i hälso-och sjukvården[4], finns reglering gällande journalsystem. I Socialstyrelsens föreskrift framgår det att vårdgivaren ska, genom ledningssystemet där journalsystemet är en integrerad del, säkerställa att:

1. dokumenterade personuppgifter hos vårdgivaren är åtkomliga och användbara för den som är behörig (tillgänglighet),
2. personuppgifterna är oförvanskade (riktighet),
3. obehöriga inte ska kunna ta del av personuppgifterna (konfidentialitet), och
4. åtgärder kan härledas till en användare (spårbarhet) i informationssystem som helt eller delvis automatiserade.

5 METOD

Granskningen har genomförts genom dokumentstudier, intervjuer och stickprovsgranskning. Dokumentstudierna har syftat till att ge en översiktlig bild av nuläget i regionen och få information om hur styrning, beslutsfattande och uppföljning etablerats vid införande av nytt vårdinformationssystem.

Dokumentstudierna har omfattat ett stort antal underlag. Dessa har utgjorts av styrande dokument som ingår i regionens ledningssystem för informationssäkerhet, riskanalyser och säkerhetsrapporter för Cosmic. Vi har därtill tagit del av uppföljning genom protokoll från regionstyrelsen och hälso- och sjukvårdsnämnden samt exempelvis patientsäkerhetsberättelse och årsrapport för informationssäkerhet för åren 2024 och 2025.

Intervjuer har genomförts med tidigare programägare FVIS[5], objektägare, regionjurist, informationssäkerhetsstrateg, IT-säkerhetsansvarig, objektspecialister VISA[6]-objektet, IT-

[3] Patientdatalag 2008:355
[4] HSLF-FS 2016:40
[5] Framtidens vårdinformationssystem
[6] Vårdinformationsadministration

arkitekt, konsulter med uppgifter i arbetet med Cosmic eller informationssäkerhet i regionen.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.

Rapporten är faktakontrollerad av intervjuade personer.

6 RESULTAT AV GRANSKNINGEN

6.1 INLEDNING

Region Västerbotten driftsatte i april 2025 ett nytt vårdinformationssystem. Det förberedande arbetet har under åren 2020 – 2025 organiserats inom ramen för program Framtidens Vårdinformationssystem (FVIS). 2025-05-23 fattades beslut om överlämning från program till förvaltning. Under programperioden rapporterade programmet till Regionstyrelsen även om viss rapportering och informationsdelning gjordes till hälso- och sjukvårdsnämnden.

Den här granskningen tar sin utgångspunkt i arbetet med riskhantering och åtgärder efter att Cosmic driftsatts och systemet överlämnats till förvaltning.

6.2 ANSVARSFÖRDELNING

6.2.1 Informationssäkerhet

Enligt Riktlinjer Informationssäkerhet - förvaltning och drift[7] har regionstyrelsen och nämnderna ansvar för att regionens informationssäkerhetsarbete sker på ett ändamålsenligt sätt och i enlighet med fastställda riktlinjer. Regionstyrelsen ansvar för de informationssystem som stödjer regionens verksamhet.

Ansvar för informationssäkerhet följer verksamhetsansvaret vilket innebär att verksamhetschef eller motsvarande är informationsägare och ansvarig för informationssäkerheten inom sin verksamhet. För information som hanteras i gemensamma IT-system ska informationsägaren tillse att information som tillförs systemet uppfyller informationssäkerhetskraven samt ställa krav gentemot berörda systemägare så att systemen uppfyller informationssäkerhetskraven.

I riktlinjen för förvaltning och drift hänvisas till att förvaltning av it-system sker i enlighet med regionens förvaltningsmodell, denna beskrivs i avsnitt 6.2.3. Alla system i regionen ska ha en ägare. Systemägaren har ansvaret för respektive IT-systems säkerhet, är beställare av informationssystem med det yttersta ansvaret att tillse att ett förvaltningsobjekt fungerar på avsett sätt. Intervjuade beskriver att rollen systemägare inte är tydligt definierad i regionen. Flertalet intervjupersoner gör dock tolkningen att det är att likställa med rollen objektägare.

Intervjuade har även haft svårt att med tydlighet beskriva vem som är informationsägare inom hälso- och sjukvårdsförvaltningen. Hälso- och sjukvårdsdirektören har, via delegation, utsett rollen CMIO (Chief Medical Information Officer). Rollen beskrivs i dokumentet Informationsägarskap i hälso- och sjukvården[8] men saknas i övriga styrande dokument som ingår i regionens ledningssystem för informationssäkerhet. Underlaget redovisar rollens ansvar men anger även att hälso- och sjukvårdsdirektör, i rollen som förvaltningschef, är

[7] Regionstyrelsen (66149), giltigt tom 2024-02-11.
[8] Dokumentnr 74124, reviderat av hälso- och sjukvårdsdirektören 2026-01-08

taktisk informationsägare för den samlade vårdinformationen. Enligt underlaget är CMIO objektägare i objektet Data och Analys (DoA). Vi har genom intervjuer fått information om att funktionen innehar rollen objektägare i VISA-objektet, detta framgår dock inte av underlaget avseende informationsägare inom hälso- och sjukvården.

Baserat på vår dokumentgranskning av regionens styrande dokument gör vi tolkningen att hälso- och sjukvårdsdirektören är informationsägare utifrån sitt verksamhetsansvar. Det innebär således ansvaret för den information som hanteras i Cosmic och för att säkerställa att systemet uppfyller informationssäkerhetskraven. Vi har inte, genom dokumentation, kunnat spåra i vilka processer eller beslut som informationsägaren involverats i informationssäkerhetsarbetet efter att Cosmic driftsattes i april 2025.

Vi har inte heller, genom dokumentation, kunnat utläsa om ansvarsfördelningen mellan regionstyrelsen och hälso- och sjukvårdsnämnden ändrades på något sätt i samband med att Cosmic driftsattes och överlämnades i förvaltning. Som nämnts tidigare så hade regionstyrelsen uppdrag och ansvar inför driftsättning och erhöll rapportering från FVIS-programmet.

Vi kan dock genom granskning av regionstyrelsens och hälso- och sjukvårdsnämndens protokoll, efter datum för driftsättning, konstatera att varken styrelsen eller nämnden haft ärenden på sina sammanträden som handlar om informationssäkerhet kopplat till Cosmic.

6.2.2 Dataskydd

Enligt reglementet för hälso- och sjukvårdsnämnden är nämnden personuppgiftsansvarig för de register och andra behandlingar av personuppgifter som sker i nämndens verksamhet. Detta befästs även i regionens Riktlinje Struktur för dataskyddsarbetet[9].

Enligt riktlinjen kan personuppgiftsansvaret inte delegeras, ansvaret är långtgående och innebär att den personuppgiftsansvarige är ansvarig för samtliga led i behandlingen av personuppgifter, oavsett om den helt eller delvis utförs av någon annan, till exempel en leverantör. Leverantören är i dessa fall personuppgiftsbiträde (PuB). Region Västerbotten har PuB-avtal med Cambio.

Vi har inte, genom dokumentation, kunnat spåra i vilka processer eller beslut som personuppgiftsansvarig involverats i dataskyddsfrågorna efter att Cosmic driftsattes i april 2025. Hälso- och sjukvårdsdirektör vid tiden för införandet har därtill bekräftat i intervju att nämnden, i dess roll som personuppgiftsansvarig, inte involverades i ställningstagande av att påbörja personuppgiftsbehandling i Cosmic. Detta trots att dataskyddsombud och informationssäkerhetsfunktionen i regionen lämnat en avrådan att påbörja personuppgiftsbehandling i Cosmic. Detta med anledning av bedömningen att systemet inte uppnådde lagkraven enligt PDL och Dataskyddsförordningen.

[9] Beslutad av regiondirektör, utgången 2024-10-27

6.2.3 Objektstyrning

Region Västerbottens Riktlinje Objektsarkitektur (OA)[10] beskriver vilka objekt i objektverksamheten som finns. Objekten i regionen är indelade i tre områden:

1. Kärnverksamhetens objekt
2. Stödverksamhetens objekt
3. Teknikobjekt

Kärnverksamhetens objekt består av objekt som stödjer hälso- och sjukvårdens processer. Ett av de objekt som ingår i kärnverksamhetens objekt är Vårdinformationsadministration (VISA) där Cosmic, efter överlämning från program till förvaltning, placerats. Objektet hette tidigare Vårdstöd Bas men bytte under hösten 2025 namn till VISA.

Riktlinje för Rollbeskrivning Modell för objektstyrning i Region Västerbotten[11] beskriver ansvar och roller i objektstyrningen. Dokumentet beskriver att objektstyrgrupp kan eskalera portföljstyrgruppen. I intervjuer framkommer att objektet inte eskalerat någon risk eller avvikelse sedan driftsättningen.

Det saknas dokumenterad reglering hur eskaleringstrappan i objektstyrningen ska fungera i relation till styrelser och nämnder. I granskningen av dokument från hälso- och sjukvårdsnämndens sammanträden 2025 noterar vi att det saknas ärenden relaterat till arbetet i VISA-objektet dit kvarstående arbete överlämnats.

Förvaltningsledning i objekten utgörs av rollerna objektägare, objektägare teknik, objektledare[12] och objektledare teknik. Enligt intervjuade ingår i VISA-objektet ca 40 utsedda funktioner på olika nivåer, dessa är jämnt fördelade mellan verksamhet och teknik. Intervjuade beskriver att en utmaning efter överlämningen till förvaltning är att flertalet funktioner objektet inte varit delaktiga inom FVIS-programmet varpå kunskap och förståelse om åtgärdsarbetet i Cosmic varierar.

Gränsdragning mellan objektstyrningen och det ansvar som regleras i regionens styrdokument för informationssäkerhet och dataskydd är inte tydligt reglerat. Det framgår inte heller i överlämningsdokumentationen från FVIS till förvaltning på vilka sätt informationsägare, systemägare och personuppgiftsansvariga har informerats och involverats inför överlämning av det kvarstående arbetet.

6.2.4 Samverkan mellan Region Västerbotten, SUSSA och systemleverantören

Samstämmigt framförs i intervjuer att beslutsfattandet inte kan delegeras till SUSSA utan kvarstår i respektive region. Det är samtidigt tydligt att kommunikation till systemleverantören ska gå via SUSSA. Detta för att erhålla en samordning och samsyn vid påtryckningar och förfrågningar. Processerna beskrivs av intervjuade som långdragna och omständliga på grund av detta.

[10] Dokumentnr 66182
[11] Dokumentnr 74477, utgånget 2025-02-17, saknas enligt uppgift revidering eller beslut om ny riktlinje.
[12] Dokumentet 74477 använder begreppet objektledare men ordet förvaltningsledare förekommer i samma dokument.

Region Västerbotten har tillsammans med övriga regioner (genom SUSSA) efterfrågat dokumentation som verifierar att Cambio lever upp till de krav inom informationssäkerhet som ställts i avtal. Ingen sådan dokumentation har levererats enligt de intervjuade. Det uppges därför finnas få konkreta underlag på efterlevnad av informationssäkerhetskrav hos Cambio. [redacted]

6.2.5 Bedömning

Vår bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden **inte** säkerställt en tydlig ansvarsfördelning mellan styrelsen och nämnden så att informationssäkerhetsarbetet varit ändamålsenligt.

Vår bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden **inte** säkerställt en tydlig ansvarsfördelning mellan regionen, SUSSA och systemleverantören så att informationssäkerhetsarbetet varit ändamålsenligt.

Vi baserar vår bedömning på att det finns dokumenterad ansvarsfördelning inom informationssäkerhet, dataskydd och objektsförvaltning. Vi bedömer dock att beskrivningar av ansvaret i olika styrdokument är otydligt vilket vi även kan bekräfta i praktiken. Vi noterar till exempel att sammanblandning har gjorts avseende ansvar för driftsättning av systemet i relation till informationsägarens ansvar, systemägarens ansvar och personuppgiftsansvaret. Dessa otydligheter har kvarstått efter driftsättning där vi konstaterar att frågor och ärenden inte har eskalerats till styrelsen och nämnden så att de beretts möjlighet att ta ställning till risker och konsekvenser. Detta har i sin tur inneburit att styrelsen och nämnden inte säkerställt ett ändamålsenligt informationssäkerhetsarbete i enlighet med ansvar enligt reglementen och den ansvarsfördelning som anges i styrande dokument inom informationssäkerhet och dataskydd.

Vi bedömer att det är tydligt att varje region är avtalsansvarig i relation till Cambio. Samtidigt konstaterar vi i granskningen att nuvarande samverkansformer inom ramen för SUSSA innebär att Region Västerbotten inte självständigt kan initiera, driva och följa upp frågor som krävs för att uppfylla tillämpliga lagkrav. Mot bakgrund av att varken styrelsen eller nämnden agerat i förhållande till Cambio, trots de betydande brister som identifierats, bedömer vi att de inte säkerställt en tydlig ansvarsfördelning så att informationssäkerhetsarbetet varit ändamålsenligt.

6.3 ÅTGÄRDSARBETET FÖR IDENTIFIERADE RISKER OCH SÅRBARHETER

6.3.1 Identifierade risker och sårbarheter

I dokumentation inför beslut[13], daterat dagen innan driftsättning, framgår att några av projektets områden signalerat att det fanns allvarliga brister och lämnat rekommendationer att inte driftsätta systemet innan bristerna åtgärdats. Bristerna som beskrivs finns inom områdena informations- och IT-säkerhet samt ekonomi. Dessa hade identifierats genom både interna och externa riskanalyser, säkerhetsanalyser och tester. Vi har tagit del av rapporternas innehåll. Med hänvisning till att de är sekretessbelagda beskriver vi inte ytterligare detaljer om innehållet.

Beslut om överlämning från program till förvaltning har dokumenterats i Överlämning – FVIS till förvaltning[14] där genomförda leveranser, kvarstående arbete och mottagare i ordinarie förvaltning beskrivs. Enligt underlaget för överlämning hade verksamhetschef CIMT[15] samt programägaren beslutat att samtliga leveranser skulle lämnas över. Kvarstående arbete skulle klassificeras som återstående utveckling eller förbättringsområde. Dokumentet hänvisar till underlag, exempelvis konsekvensbedömning, säkerhetsrapporter och tester som beskriver risker och sårbarheteter med Cosmic ur informations- och it-säkerhetsperspektiv.

Överlämningen innebar således att samtliga tidigare identifierade risker och brister för Cosmic överlämnades till objekt Vårdstöd Bas/VISA. Av dokumentationen framgår att arbetet ingår i objektens löpande systematiska arbete med att säkerställa säkerheten för systemen.

Intervjuade lyfter att överlämningen gjordes utan beaktande av vilka resurser, ekonomiska eller personella, som behövde tillföras objektet så att förutsättningar fanns att ta vid det kvarstående arbetet som överlämnades.

Riktlinje för Rollbeskrivning Modell för objektstyrning i Region Västerbotten[16] beskriver att utsedda roller i modellen leder förvaltnings- och utvecklingsarbetet enligt det uppdrag som beslutats i objektplanen. Objektplan för VISA-objektet saknas för 2025. Vi har inte heller tagit del av annan sammanställning med planering eller prioritering för det kvarstående arbete som överlämningsdokumentet hänvisar till.

Några av de aktiviteter som enligt överlämning från FVIS till förvaltning då var kvarstående var att ta del av resultat från extern granskning, uppdatera handlingsplan informationssäkerhetsklassning, uppdatera konsekvensbedömning, uppdatera lämplighetsbedömning samt ta del av och följa upp arbetet med tilldelade aktiviteter i genomförd riskanalys och slutligen följa upp identifierade brister i genomförda tester.

Vi har inte kunnat ta del av någon dokumentation som styrker vilka åtgärder som regionen, SUSSA eller leverantören vidtagit utifrån identifierade brister och enligt de intervjuade har

[13] RS 402-2025 Beslutsunderlag GoLive
[14] RS 2153 72-2024
[15] Centrum för informationsteknik och medicinsk teknik
[16] Utgånget 2025-02-17, saknas enligt uppgift revidering eller beslut om ny riktlinje.

åtgärderna som framgår av överlämningsdokumenten inte genomförts. Vi har inte heller tagit del av dokumentation eller beskrivning avseende åtgärder som regionen vidtagit i syfte att möta riskerna tills åtgärder i systemet vidtagits, så kallade kompensatoriska åtgärder i syfte att sänka risk och sannolikhet tills en varaktig lösning finns som leder till att risken helt kan accepteras.

Bilden som ges i intervjuer är att regionen uppfattar att den inte internt har rådighet över åtgärdshantering för att komma till rätta med identifierade risker och sårbarheter. Detta då dessa härrör till bristande leveranser från systemleverantören. Nuvarande system bedöms inte uppnå de krav som ställts i upphandling och avtal. [redacted] I flera intervjuer beskrivs att fel och brister inte får rapporteras direkt till leverantören utan ska gå via SUSSA. Enligt intervjuade har regionens företrädare löpande rapporterat behov och krav via SUSSA. SUSSA har sedan eskalerat frågor från regionerna till systemleverantören.

Som vi nämnt i föregående avsnitt uppfattas kommunikation och samverkan mellan regionerna, SUSSA och leverantören som bristfälliga där åtgärder inte vidtas i en takt som företrädare från Region Västerbotten bedömer som acceptabla. Samstämmiga uppgifter i intervjuer är att det finns en bristande hantering av de synpunkter som regionerna lämnar samt bristande återkoppling om hur åtgärdsarbetet framskrider.

6.3.2 Utvärdering av säkerhetsåtgärder genom penetrationstest eller andra it-säkerhetsanalyser

Region Västerbotten, SUSSA samt andra regioner som ingår i SUSSA-samverkan har genomfört tester och analyser av säkerheten i systemet innan driftsättning som vi beskrivit i tidigare avsnitt. Dessa har visat sårbarheter med systemet. Enligt intervjuade har sårbarheterna kommunicerats till SUSSA. I intervjuer framgår det inte vilka åtgärder som SUSSA alternativt Cambio vidtagit. Det framgår inte heller när bristerna ska vara åtgärdade.

Då det saknas underlag över vilka åtgärder som vidtagits av leverantören för att komma till rätta med identifierade brister så har inte penetrationstest och it-säkerhetsanalyser kunnat göras i syfte att utvärdera åtgärdernas effektivitet.

Region Västerbottens egna IT-funktioner har efter införandet av systemet genomfört ytterligare säkerhetstester[17]. Dessa genomfördes i juni 2025. Testerna både fördjupar och breddar den ursprungliga riskbilden, snarare än att bara *sammanfalla* med de tidigare identifierade riskerna och som överlämnats till VISA-objektet. De har även ingått i rapportering till SUSSA för vidare hantering i relation till leverantören.

Region Västerbotten saknar återkoppling för hur dessa sårbarheter har hanterats av leverantören.

[17] RS 965:29–2024 (Sekretessbelagd) och RS 965:29–2024 (Sekretessbelagd)

6.3.3 Bedömning

Vår bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden **inte** säkerställt att risker och sårbarheter åtgärdats.

Åtgärder har inte vidtagits sedan driftsättning vilket medför att utvärdering genom penetrationstest eller it-säkerhetsanalyser **inte** varit relevanta att göra.

Vi baserar vår bedömning på att det saknas dokumenterade underlag som redogör för hur regionstyrelsen och hälso- och sjukvårdsnämnden följt upp att tidigare kommunicerade risker och sårbarheter åtgärdats eller på annat sätt hanterats efter att Cosmic driftsattes.

Enligt reglementet för regionstyrelsen har de ansvar för regiongemensamma system och har även varit mottagare av rapportering från FVIS-programmet inför driftsättning, där de varit mottagare av information om identifierade risker och sårbarheter. Vi bedömer därigenom att det är en allvarlig brist att regionstyrelsen inte efterfrågat underlag och rapportering över att risker var på en acceptabel nivå innan systemet togs i drift.

Hälso- och sjukvårdsnämnden är personuppgiftsansvarig för informationen som hanteras i Cosmic vilket inte kan delegeras. Interna bedömningar och analyser visar att Cosmic inte efterlever lagkrav och att allvarliga säkerhetsbrister föreligger. Mot bakgrund av detta är vår bedömning 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.

Det saknas dokumentation över vilka formella krav på åtgärder som kommunicerats från Region Västerbotten till SUSSA och systemleverantören. Det saknas även krav på tidsplan för när åtgärder förväntas vara levererade. Vi bedömer att detta kan försvåra för regionen att, vid behov, ställa krav på juridiska och ekonomiska påföljder gentemot leverantören.

6.4 Åtkomst och behörigheter i Cosmic

Flertalet av de risker som identifierats i riskanalys, informationsklassning och konsekvensbedömning, se avsnitt 6.2.5, rör åtkomst och behörigheter i Cosmic.

Patientdatalagen reglerar vårdgivares behandling av personuppgifter inom hälso- och sjukvården. Lagen fastställer hur informationshantering inom hälso- och sjukvård ska vara organiserad så att den bland annat tillgodoser krav på patientsäkerhet. Vidare beskrivs att personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem. Enligt 4 kap. 1 § PDL får personal endast ha åtkomst till patientuppgifter om de behöver uppgifterna för att kunna utföra sitt arbete. Enligt 4 kap. 2 § PDL ska varje användare ha individuell åtkomst.

I regionens riktlinje, för informationssäkerhet – förvaltning och drift, beskrivs att varje verksamhetschef ansvar för att dennes personal har rätt behörighet. Det inkluderar ansvar för att begränsa behörigheter i journalsystem och andra system med känsliga personuppgifter till det som behövs för att fullgöra arbetsuppgifter och inte är mer omfattande än vad som är nödvändigt. Dokumentet beskriver även att det ska finnas dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter i samtliga IT-system.

Regiondirektören har fastslagit bestämmelser för behörighetsstyrning i en riktlinje[18]. Dokumentet hänvisar till lagar och krav enligt nedan:

- Artikel 5 i dataskyddsförordningen
- SS-EN ISO/IEC 27002:2022
- HSLF:FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.

Riktlinjen anger exempelvis att behovs- och riskanalys ska genomföras innan tilldelning av behörigheter. Varje användare ska tilldelas en individuell behörighet för att komma åt personuppgifter. Åtkomsten ska begränsas till vad varje anställd behöver för att kunna utföra sina arbetsuppgifter, d.v.s. minsta möjliga behörighet och hänsyn ska tas till riskerna med en alltför vid behörighet, och alltför snäv behörighet. Rutiner behövs för att säkerställa korrekt tilldelning, granskning och förändring samt avregistrering av behörigheter samt beskrivning av vilka åtkomstmöjligheter respektive behörighet innebär. Process för hantering beskrivs i rutin för åtkomsträttigheter och säker autentisering[19].

Intervjuade beskriver att Region Västerbotten har haft ett dedikerat arbete i syfte att stärka arbetet med åtkomst och behörigheter. Detta avser både dokumenterade rutiner och processer, och tekniska implementationer och regler för en säker hantering. Behörighetstilldelning beskrivs av intervjupersonerna ske på ett formaliserat sätt, i enlighet med styrdokumenten så långt det är möjligt. Det finns ett stort antal grundkonfigurationer för anställda inom regionen som baseras på funktioner och organisationstillhörighet. För dessa har en behovs- och riskanalys genomförts och godkänts av ansvariga chefer. Vid beställning av behörigheter måste chefer godkänna tilldelningen vilket intervjuade anger blir en bekräftelse på att tilldelningen följer tidigare bedömning av behov av åtkomst för den specifika medarbetaren. Om en funktion avslutas så avslutas även samtliga behörigheter som tilldelats.

I intervjuer framkommer det att behörighetshanteringen i Cosmic är relativt statisk vilket gör att det i praktiken inte går att efterleva principen ”minsta möjliga behörighet” enligt regionens interna regelverk. Detta innebär i praktiken att användare tilldelas en behörighet

[18] Dokumentnr 87158
[19] Dokumentnr 87172

utifrån roll och vårdenhet men trots detta kan ta del av betydligt mer information om patienter än vad deras arbetsuppgifter kräver.

Intervjupersonerna beskriver att detta påpekats under lång tid till SUSSA och Cambio men problemet har inte åtgärdats. Vidare beskriver intervjupersonerna att Region Västerbotten, SUSSA och Cambio inte delar synen på hur funktionaliteten gällande behörigheter bör utformas, det vill säga tolkar kraven på olika sätt.

6.4.1 Loggkontroll

I patientdatalagen regleras hur kontroll av åtkomst ska hanteras. Av 4 kap. 3 § framgår att vårdgivaren ska dokumentera och kontrollera åtkomst. Kontrollen ska vara systematisk och återkommande för att säkerställa att inte obehörigen kommer åt uppgifter.

Regionen har en fastställd rutin för loggkontroller i Cosmic[20] där det framgår att varje verksamhetschef ansvarar för att det finns lokala rutiner för loggkontroller och att rutinerna följs. Rutinen beskriver att varje verksamhet ska göra systematisk stickprovskontroll varje månad med hjälp av regionens loggverktyg LogPoint. Vidare ska varje användare granskas minst en gång per år. All loggranskning ska enligt rutinen dokumenteras och sparas i LogPoint. Om kontrollen visar att obehörig användning skett ska utredningen och beslutet diarieföras samt dokumenteras i Platina.

I intervjuer framkommer det att LogPoint används som regionens centrala verktyg för logginsamling, logghantering och logguppföljning kopplat till journalsystemet Cosmic, i enlighet med rutinen. Det är ett nytt verktyg men ska, enligt intervjuer, vara implementerat i samtliga verksamheter. Verktyget används för att samla in, strukturera och analysera

[20] Dokumentnr 99149

loggdata i syfte att säkerställa spårbarhet, stärka informationssäkerheten samt möjliggöra uppföljning av efterlevnad av tillämpliga lagar och interna styrande dokument.

I intervjuerna framkommer att LogPoint implementerades i december 2025. I patientsäkerhetsberättelsen 2025[21] beskrivs att av de enheter som rapporterat in har de flesta genomfört systematiska stickprovskontroller på loggar i journalsystemen fram till tidpunkten för införandet av Cosmic. Vidare beskrivs det att rutiner och utbildning i ett nytt kontrollsystem som inte är implementerat behövs för att återuppta arbetet i nytt journalsystem. Detta indikerar att loggkontroller inte genomförts mellan driftstart av Cosmic och införande av Logpoint.

6.4.2 Bedömning

Vår bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden **inte** säkerställt att systemet har en ändamålsenlig åtkomsthantering som säkerställer följsamhet till lagkrav.

Åtgärder har **inte** vidtagits sedan driftsättning vilket medför att systemet fortsatt har brister i åtkomsthantering.

Vi baserar vår bedömning på att det saknas underlag som styrker att åtkomsthanteringen för Cosmic inom Region Västerbotten följer lagkrav. Vår stickprovsgranskning har bekräftat brister i åtkomsthanteringen.

Vår bedömning är att beslutade behörighetsmodeller **inte** utgår från behovs- och riskanalys, samt att behörigheter **inte** följs upp regelbundna loggkontroller.

Åtgärder har **inte** vidtagits sedan driftsättning vilket medför att systemet fortsatt har brister i behörighetshantering och loggkontroll.

Vi baserar vår bedömning att det visserligen finns beslutade behörighetsmodeller och att de utgår från behovs- och riskanalys men att behörighetsmodellen inte tillämpas i systemet då den tekniska lösningen inte medger det.

Gällande loggkontroller finns styrdokument, verktyg och arbetssätt framtagna. Dessa har dock implementerats 2026.Vi har efterfrågat men inte tagit del av underlag som verifierar att de tillämpas i verksamheterna på ett konsekvent och avsett sätt. Vi har inte heller tagit del av aggregerad information om antal loggkontroller som genomförts eller eventuella avvikelser som framkommit.

[21] HSN 1642–2025

6.5 UPPFÖLJANDE GRANSKNING AV TIDIGARE LÄMNADE REKOMMENDATIONER

Regionens revisorer genomförde 2022 en granskning av regionens IT- och informationssäkerhetsarbete[22]. Granskningen syftade till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att arbetet med IT-och informationssäkerhet bedrevs på ett ändamålsenligt sätt och om den interna kontrollen var tillräcklig inom området.

Den samlade bedömningen som gjordes i granskningen var att de granskade nämnderna hade en förhållandevis låg mognadsgrad inom informationssäkerhet jämfört med vad granskaren rekommenderar, givet den stora mängd information och andel information av känslig karaktär, som hanteras. Mognadsgraden bedömdes vara något högre inom förändringshantering, incidenthantering och nätverk. Lägst ansågs mognadsgraden vara inom policy, utbildning, informationsklassning och kontinuitetsplanering.

Granskningen resulterade i fyra rekommendationer till regionstyrelsen och hälso- och sjukvårdsnämnden som styrelsen och nämnden lämnat yttrande[23] över.

Vår uppföljning av regionens arbete och åtgärder i relation till lämnade rekommendationer har delvis försvårats mot bakgrund av att informationssäkerhetssamordnare, som i hög grad lett förbättringsarbetet i regionen, var föräldraledig vid tidpunkten för uppföljningen. Andra funktioner och representanter har bistått med uppgifter och underlag i den mån det gått att få tag i.

6.5.1 Rekommendation 1: Organisering för arbetet med IT- och informationssäkerhet

Se över organisationen för arbetet med IT- och informationssäkerhet. Säkerställ en tydlig ansvarsfördelning.

Yttranden

Regionstyrelsens och hälso- och sjukvårdsnämndens yttrande beskrev att ansvar och roller hade tydliggjorts genom nya styrdokument, exempelvis Riktlinje Informationssäkerhet - förvaltning och drift samt genom beskrivning av dataskyddsorganisationen.

Centrala roller hade tillsatts och utökats samt att hälso- och sjukvården hade utsett en informationsägare i syfte att tydliggöra ansvaret att säkerställa att informationen skyddas på avsett sätt.

Nuläge

Vi delar bilden i yttrandet att ansvarsfördelning tydliggjorts genom de styrande dokument som styrelsen och nämnden hänvisar till. Dock är de styrande dokumenten utgångna vid tid för uppföljningen. De styrande dokumenten saknar även reglering av bland annat rollen informationssäkerhetsstrateg[24], vilken vi uppfattar har en nyckelfunktion att leda och

[22] Granskning Nr 1/2022
[23] HSN 914–2023 samt RS 2023-01-02 (nr 471112)
[24] Rollen ändrade titulatur under 2025 från samordnare till strateg. Rollen beskrivs kortfattat i riktlinjen Struktur för dataskyddsarbete inom Region Västerbotten, Dokumentnr: 73581. Dokumentets giltighetstid har gått ut.

samordna regionens informationssäkerhetsarbete. Vi noterar även att styrande dokument inte är samstämmiga i benämning av rollen systemägare/objektägare vilket kan medföra oklarheter över vem som avses. Informationsägarens ansvar beskrivs i styrande dokument på en övergripande nivå, det är dock inte tydligt i vilka delar och hur informationsägaren ska ta sitt ansvar i det operativa arbetet på verksamhetsnivå, exempelvis avseende hantering och acceptans av risker. I tidigare avsnitt har vi även konstaterat att det finns en viss osäkerhet i vem som innehar rollen som informationsägare inom hälso- och sjukvården.

Det finns en etablerad organisation med centrala funktioner (informationssäkerhetsstrateg, dataskyddsombud, it-säkerhetsansvarig med flera) samt utsedda roller inom ramen för regionens objektsförvaltning (objektägare, objektägare teknik, objektledare, objektledare teknik med flera). Vi uppfattar att dessa roller på olika sätt är involverade och har uppgifter i det operativa informationssäkerhetsarbetet.

6.5.2 Rekommendation 2: Standardiserad process för riskhantering

Inför en standardiserad process för att identifiera risker inom IT- och informationssäkerhet.

Yttranden

I yttrandet anges att det för 2022 har beslutats om en övergripande riskanalys för informationssäkerhet med tillhörande åtgärdsplan. I samband med arbetet uppges att det finns en grund för en process för riskanalys som ska utvecklas. Regionstyrelsen avser, enligt yttrandet, att ta fram stöd och struktur för att identifiera, hantera och aggregera informationssäkerhetsrisker för att förbättra säkerhetsåtgärderna för informationstillgångar.

Nuläge

Vi har inte i granskningen erhållit något specifikt styrdokument i form av riktlinje eller rutin för riskhantering inom informationssäkerhet. Informationssäkerhetssamordnare har gjort en analys över regionens etablerade styrande dokument i relation till krav i den nya cybersäkerhetslagen. I arbetet har även dokumentansvariga kartlagts. I sammanställningen nämns Riktlinje för riskhantering. Den är dock i utkastform och har inte beslutats eller implementerats ännu[25].

I riktlinje informationssäkerhet – drift och förvaltning framgår att verksamhetschef i patientsäkerhetsberättelsen årligen ska rapportera de risker, analyser och åtgärder som vidtagits i verksamheten utifrån dess informationssäkerhetsansvar. I patientsäkerhetsberättelse 2025 beskrivs att införandet av Cosmic påverkat patientsäkerhetsarbetet då den har inneburit uppehåll, fördröjningar och genererat patientsäkerhetsrisker genom initiala handhavandeproblem. I bilaga 1 till patientsäkerhetsberättelsen, Informationssäkerhet 2025, beskrivs att det årligen genomförs en övergripande riskanalys med utgångspunkt i regionens roll som leverantör av samhällsviktig tjänst enligt 12 § i lag om informationssäkerhet för samhällsviktiga och

[25] Under faktakontroll framkommer att dokumentet är publicerat i ledningssystemet och gäller från och med 2026-02-11.

digitala tjänster[26]. Utifrån riskanalysen togs en åtgärdsplan fram vilken presenterades i Centrala ledningsgruppen i september 2025. Patientsäkerhetsberättelsen 2025 fastställdes av HSN 2026-02-18. Vi har efterfrågat riskanalys för 2025 med tillhörande åtgärdsplan men inte erhållit några underlag för att verifiera dess innehåll eller struktur.

6.5.3 Rekommendation 3: Styrdokument

Säkerställ att styrdokument är aktuella över tid och kända bland verksamheterna. Säkerställ att anställda får tillräcklig utbildning inom IT-och informationssäkerhet.

Yttranden

Enligt yttrandet pågick redan ett arbete med att följa upp dokumenterad information för att identifiera behov av utveckling och säkerställa nivån av dokumenterad information. Arbetet med att göra styrdokumenten kända kopplades även till tydliggörandet av roller och ansvar samt etablering av standardiserade processer för riskanalyser som nämnts ovan.

Nuläge

Vi noterar genom dokumentgranskning att flertalet styrdokument i regionens ledningssystem för informationssäkerhet inte är giltiga. Revidering har inte gjorts för att säkerställa att styrdokumenten är aktuella över tid. Det saknas dokumentation av på vilka sätt styrande dokument görs kända bland verksamheterna. Det pågår enligt intervjuade ett arbete, som leds av informationssäkerhetsstrategen, att inventera nuvarande styrning i relation till cybersäkerhetslagen och föreskrifter från Myndigheten för civilt försvar. När kraven i lag och föreskrift presenterats ska de styrande dokumenten ses över, revideras och kompletteras.

Vad avser utbildning så uppger intervjuade att det finns utbildningar att tillgå. Dock saknas tillräcklig funktionalitet för att följa upp genomförande och effekt av genomförda insatser. Det pågår ett utvecklingsarbete för att inkludera utbildning i regionens lärplattform som ett sätt att förbättra möjligheten till uppföljning. Utifrån de underlag och muntliga uppgifter vi fått i granskningen finns ingen tydlig uppfattning om deltagandet är tillräckligt för att skapa en säkerhetsmedvetenhet och säkerhetskultur inom informationssäkerhet.

6.5.4 Rekommendation 4: Uppföljning och kontroll

Säkerställ tillräcklig uppföljning och kontroll av verksamheternas arbete med IT och informationssäkerhet och att policyer, riktlinjer och rutiner följs.

Yttranden

Enligt yttranden tas en årlig informationssäkerhetsberättelse fram med uppföljning av verksamheternas arbete med informationssäkerhet på vissa områden. Regionen ska fortsätta utveckla sitt ledningssystem för informationssäkerhet med dess komponenter, där kontroll och uppföljning av verksamheternas informationssäkerhetsarbete är några av delarna.

[26] 2018:1174

Nuläge

Enligt Riktlinje informationssäkerhet – drift och förvaltning ska regionstyrelsen säkerställa att en årsrapport tas fram för informationssäkerhetsarbetet. Denna ska biläggas patientsäkerhetsberättelsen. Vi uppfattar från intervjuade att informationssäkerhetsstrateg upprättar årsrapporten men vi kan inte se att uppgiften är fördelad till denne i de styrande dokumenten. Som nämnts tidigare saknas beskrivning av informationssäkerhetsstrategens ansvar och uppgifter. Som tidigare nämnts innehåller Patientsäkerhetsberättelse 2025 ett avsitt om informationssäkerhet med tillhörande bilaga avseende informationssäkerhet. Patientsäkerhetsberättelsen har fastställts i HSN 2026-02-18.

Utöver rapporten har vi inte erhållit några underlag eller uppgifter som påvisar att det sker någon kontroll av efterlevnad av verksamheternas informationssäkerhetsarbete med grund i interna styrdokument eller lagkrav inom informationssäkerhet och dataskydd.

6.5.5 Bedömning

Vår bedömning är att regionen **endast delvis** omhändertagit tidigare lämnade rekommendationer

Vi baserar bedömningen på att vissa styrande dokumenten inom området informationssäkerhet är utgångna och därmed inte längre aktuella. Det förekommer även oklarheter kring roller och, i viss mån, ansvarsfördelning i organisationens arbete med informationssäkerhet.

Vidare har vi inte kunnat ta del av någon riktlinje för riskhantering kopplad till informationssäkerhet. Vi har inte heller kunnat verifiera att de styrande dokument som finns är implementerade i verksamheten på ett systematiskt sätt.

Vi kan inte bedöma om de utbildningsinsatser som erbjudits har resulterat i en ökad säkerhetsmedvetenhet eller en utvecklad säkerhetskultur i organisationen. I dagsläget saknas möjlighet att följa upp deltagandet på utbildningarna.

Det finns en uppföljning i form av årsberättelse som tas fram på regionövergripande nivå. Det saknas dock ännu former för uppföljning avseende efterlevnad av att regionen efterlever lagkrav och interna krav inom informationssäkerhet.

7 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

Granskningen har syftat till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt följsamhet till interna och externa krav inom informationssäkerhet för nytt vårdinformationssystem.

Granskningen har syftat till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden hörsammat tidigare lämnade rekommendationer i granskning av informationssäkerhet.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt följsamhet till interna och externa krav inom informationssäkerhet för nytt vårdinformationssystem.

Vår samlade bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden endast delvis har hörsammat tidigare lämnade rekommendation i granskning av informationssäkerhet.

Utifrån våra iakttagelser och bedömningar rekommenderar vi regionstyrelsen och hälso- och sjukvårdsnämnden att:

- **Säkerställa att styrande dokument som ingår i ledningssystem för informationssäkerhet är uppdaterade och kompletta för att motsvara interna och externa krav**
  Vi rekommenderar att styrdokumenten ses över och ger förutsättningar för regionens verksamhet att efterleva de informationssäkerhetskrav som ställs på regioner. Regionen bör därtill säkerställa att ledningssystemet för informationssäkerhet är strukturerat och kan utgöra ett tydligt ramverk för det arbete som verksamheterna ska utföra.
- **Fastställa och förankra interna roller och ansvar**
  Vi rekommenderar att Region Västerbotten säkerställer en tydlig och gemensam förståelse för samtliga roller och det ansvar som respektive funktion bär. Alla berörda, regionstyrelsen, hälso- och sjukvårdsnämnden samt berörda tjänstepersoner, bör ha en klar uppfattning om vad som förväntas av dem samt deras respektive åtaganden inom informationssäkerhet och dataskydd.
- **Tydliggöra ansvarsfördelningen mellan regionen, SUSSA och Cambio**
  Vi rekommenderar att ansvar, befogenheter och mandat formaliseras och kommuniceras på ett strukturerat sätt mellan Region Västerbotten, SUSSA och Cambio. Detta för att säkerställa att Region Västerbotten självständigt kan initiera, driva och följa upp frågor som krävs för att uppfylla tillämpliga lagkrav. Detta innefattar även att etablera en tydlig process för återkoppling från SUSSA och Cambio av inrapporterade fel och brister, inklusive tidsramar för när åtgärder förväntas vara genomförda.
- **Säkerställa att det systemstöd som används uppfyller tillämpliga interna krav och lagkrav**

Vi rekommenderar att organisationen säkerställer att det systemstöd som används inom området är ändamålsenligt och uppfyller relevanta lagkrav. Detta inkluderar att systemet möjliggör korrekt hantering av åtkomst för användare i enlighet med gällande regelverk. För att åtgärda detta behöver regionens process för krav mot leverantören formaliseras.

- **Stärka riskhanteringsarbetet genom tydligare riktlinjer och ansvarsfördelning**
  Vi rekommenderar att riktlinjen för riskhantering i Region Västerbotten implementeras för att tydliggöra krav på genomförande av riskanalyser och åtgärder samt process för att acceptera risker. Den interna kontrollen behöver därtill stärkas i syfte att säkerställa att identifierade risker och sårbarheter dokumenteras i åtgärdsplaner och löpande följs upp till dess att riskerna kan bedömas som acceptabla.

Datum som ovan

Azets Revision & Rådgivning AB

Jenny Thörn
Verksamhetsrevisor

Helena Olsson
Verksamhetsrevisor

Veronica Hedlund Lundgren
Certifierad kommunal revisor