Granskning av införande av nytt vårdinformationssystem

Region Norrbotten

Januari 2025

Charlotte Arnell, projektledare

Agnes Westerlund, projektmedarbetare

Kristian Damlin, kvalitetssäkrare

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Norrbotten genomfört en granskning av införandet av nytt vårdinformationssystem. Granskningens syfte har varit att bedöma om regionstyrelsen har säkerställt att implementering av nytt vård-informationssystem sker i enlighet med gällande lagstiftning och på ett ändamålsenligt sätt.

2019 tecknade regionen avtal med Cambio om att införa ett nytt vårdinformationsstöd. Upphandlingen gjordes tillsammans med åtta andra regioner och samordnat under SUSSA-samverkan, som är en sammanslutning av de regioner som ska byta till nytt vårdinformationsstöd. Systemet driftsattes den 23 november 2024 i Region Norrbotten.

Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen **inte helt** har säkerställt att implementering av nytt vårdinformationssystem skett i enlighet med gällande lagstiftning och på ett ändamålsenligt sätt.

Granskningen bedömer att riskanalyser, konsekvensbedömningar och lämplighets-bedömningar följer lagkrav och branschstandard samt att dessa utförts grundligt och uppdaterats i takt med ändrade förutsättningar. Det finns även en godtagbar planering för uppföljning av leverantör och avtal. Avseende förberedande utbildning samt rutiner, vägledningar och liknande för användningen av systemet, bedöms att dessa är i allt väsentligt tillräckliga. De primära bristerna avser personuppgiftsbiträdesavtalet samt bristande testning av systemet innan driftsättning.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar, se respektive revisionsfråga i rapporten.

Revisionsfrågor	Bedömning	
Har ändamålsenliga riskanalyser, konsekvensbedömningar och lämplighetsbedömningar genomförts?	Delvis	
Har ändamålsenliga risk- och behovsanalyser avseende behörighetstilldelning genomförts?	Delvis	
Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av systemet?	Delvis	
Har ändamålsenliga tester av systemet genomförts?	Delvis	
Finns ändamålsenlig planering för uppföljning av leverantör och avtal?	Ja	
Finns ändamålsenlig utbildningsplan för vårdinformationssystemets användare?	Ja	
Finns ändamålsenliga regler, rutiner och vägledning som reglerar och stödjer användningen av det nya systemet?	Ja	

Rekommendationer

Regionstyrelsen rekommenderas att:

- Säkerställa att riskanalyser avseende informationssäkerhet, konsekvensbedömningar avseende dataskydd samt lämplighetsbedömningar avseende sekretess, påbörjas i ett tillräckligt tidigt skede i framtida upphandlingar och införanden av IT-system och -tjänster,
- Säkerställa att de höga risker som inte kunnat reduceras innan driftsättning, snarast följs upp och åtgärdas,
- Säkerställa att de handlingsplaner (inklusive ytterligare tester och fortsatta externa granskningar av leverantören) som överlämnas från projektet till förvaltningen av vårdinformationssystemet genomförs,
- Säkerställa att slutgiltiga beslut avseende beslut om driftsättning, fastställande av riskanalyser, lämplighetsbedömning och liknande motiveras skriftligt.

Innehållsförteckning

Förkortningar och begrepp

I rapporten används olika begrepp som alla syftar på vårdinformationssystem. Dessa begrepp är journalsystem, informationssystem och vårdinformationsstöd.	
BP	Ett förutbestämt tillfälle där beslut fattas om ett projekts fortsatta verksamhet. Begrepp som används inom Region Norrbotten och som står för beslutspunkt.
Cambio Cosmic	Cambios vårdinformationssystem. I rapporten refereras systemet främst till som Cosmic.
FVIS	Framtidens Vårdinformationsstöd
GDPR	Den allmänna dataskyddsförordningen EU (2016/679)
HSLF-FS 2016:40	Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården
Informations-säkerhet	Det finns ingen legal eller formellt fastslagen definition av informationssäkerhet. En vedertagen beskrivning däremot är att informationssäkerhet utgörs av en uppsättning administrativa och tekniska åtgärder för att bevara informationens konfidentialitet, riktighet och tillgänglighet. Konfidentialitet innebär att informationen endast är tillgänglig för behöriga personer. Riktighet innebär att informationens innehåll är korrekt och inte kan ändras av obehöriga. Tillgänglighet innebär att informationen är tillgänglig när den behövs.
IMY	Integritetsskyddsmyndigheten
ISO27000-serien	Internationell standardserie för informationssäkerhet, cybersäkerhet och dataskydd.
IT-säkerhet	Det finns ingen legal eller formellt fastslagen definition av IT-säkerhet. En vanlig beskrivning är att IT-säkerhet avser de tekniska delarna av informationssäkerhet, både avseende IT och fysisk säkerhet. IT-säkerhet handlar om allt från vpn-förbindelser och antivirus till intrångsdetektering och säkerhetskopiering.
MSBFS 2018:8	Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster.
OSL	Offentlighets- och sekretesslag (2009:400)
PUA	Personuppgiftsansvarig
PUB	Personuppgiftsbiträde
SOA	Statement of applicability (“uttalande om tillämplighet”), en inventering av organisationens arbete med informationssäkerhet.
SUSSA	Strategisk utveckling av sjukvårdsstödjande applikationer

Inledning

Bakgrund

Regionerna har ett av det svenska samhällets mest komplexa uppdrag, detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. En avgörande del av detta uppdrag innebär att hantera information, och framförallt personuppgifter, av olika slag. I många fall kan uppgifterna vara både sekretessbelagda och känsliga, och i stora volymer. Brister i hantering av personuppgifter och skyddet för enskildas integritet kan leda till ett försämrat förtroende för både den enskilda regionen men även offentlig sektor och välfärdssystemet i allmänhet. Förtroende tar lång tid att bygga upp, men kan snabbt raseras av en enskild incident. Brister kan också leda till skada för organisationen och/eller individerna som drabbas, och i sin tur ge negativa ekonomiska konsekvenser för regionen.

2019 tecknade regionen avtal med Cambio om att införa ett nytt vårdinformationsstöd. Upphandlingen gjordes tillsammans med åtta andra regioner och samordnat under SUSSA samverkan, som är en sammanslutning av de regioner som ska byta till nytt vårdinformationsstöd. Systemet driftsattes den 23 november 2024.

Det nya vårdinformationssystemet består av ett kärnsystem (journalsystem) och olika komponenter. Behovet av ett nytt informationssystem är stort och om allt går som tänkt så kommer det att innebära möjlighet att utveckla effektiva vårdprocesser. Införandet av ett nytt vårdinformationsstöd är dock en stor investering för regionen och innebär stora verksamhetsmässiga risker. År 2021/2022 genomförde revisorerna en förstudie avseende införande av nytt vårdinformationssystem. I förstudien lämnas sex förslag på fördjupade granskningar, lämpliga att genomföra de kommande åren.

Regionens revisorer har mot bakgrund av ovanstående, samt efter genomförd väsentlighets- och riskbedömning, beslutat att granska införandet av nytt vårdinformationssystem, med fokus på hanteringen av informations- och IT-säkerhet samt personuppgiftshantering.

Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om regionstyrelsen har säkerställt att implementering av nytt vårdinformationssystem sker i enlighet med gällande lagstiftning och på ett ändamålsenligt sätt.

1. Har ändamålsenliga riskanalyser, konsekvensbedömningar och lämplighetsbedömningar genomförts?
2. Har ändamålsenliga risk- och behovsanalyser avseende behörighetstilldelning genomförts?
3. Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av systemet?
4. Har ändamålsenliga tester av systemet genomförts?
5. Finns ändamålsenlig planering för uppföljning av leverantör och avtal?

6. Finns ändamålsenlig utbildningsplan för vårdinformationssystemets användare?
7. Finns ändamålsenliga regler, rutiner och vägledning som reglerar och stödjer användningen av det nya systemet?

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

- Offentlighet- och sekretesslag (2009:400)
- Allmänna dataskyddsförordningen (EU) 2016/679, "GDPR"
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, HSLF-FS 2016:40

Avgränsning

Granskningsobjekt är regionstyrelsen. Granskningen är avgränsad till områdena informationssäkerhet, IT-säkerhet och personuppgiftshantering.

Granskningen är också avgränsad till perspektivet om gällande regelverk och etablerad praxis efterlevts avseende processen för införandet av nytt vårdinformationssystem. Exempelvis har vi granskat om riskanalyser har genomförts, och på det sättet och till den omfattning som regelverk och praxis anvisar. Däremot har vi inte granskat de materiella avvägningar och beslut som tagits, exempelvis om det var rätt eller fel att driftsätta det nya vårdinformationssystemet vid det tillfället som det skedde, eller om analysen i exempelvis lämplighetsbedömningen var korrekt eller ej.

Metod

Granskningen har genomförts genom intervjuer och dokumentstudier. Insamlingen har gjorts av framförallt dokumenterade riskanalyser och bedömningar, beslut, avtal, samt interna styrande och stödjande dokument (se Bilaga 1). Digitala intervjuer har genomförts med regiondirektör, IT/MT-direktör, informationssäkerhetschef och informationssäkerhetsresurs samt huvudprojektledare. De intervjuade har beretts möjlighet att sakgranska rapporten.

Granskningsresultat

Beskrivning av FVIS

Region Norrbottens arbete med nytt vårdinformationsstöd organiseras i projektet FVIS. Projektet leds av en styrgrupp med anknuten klinisk referensgrupp, en projektledare och biträdande projektledare. Vid staben ingår de sju uppdragen: Avtal och juridik, Informationssäkerhet, Förändringsledning, Kommunikation, Ekonomi, HR och IT/MT. Vid tidpunkten för granskningen ingick de fyra delprojekten Teknik, Datalager/utdata, Avveckla VAS och övriga system samt Verksamhetens införande och utbildning.

I januari 2024 fastställdes datumet för driftsättning av det nya vårdinformationssystemet till vecka 48 år 2024, enligt *Tidslinje - FVIS-projektet Region Norrbotten* (odaterad), och beslut om att driftsätta det nya journalsystemet togs den 18 november 2024, *Beslut om driftsättning av journalsystemet* (2024-11-18). Den 23 november 2024 införde Region Norrbotten det nya vårdinformationssystemet, Cambio Cosmic.

Region Norrbottens införande av det nya vårdinformationsystemet har delats upp i olika faser, så kallade beslutspunkter, från beslutspunkt noll (BP0) till beslutspunkt sex (BP6). Vid beslutspunkt fyra (BP4), som ägde rum i augusti 2024, fattades beslut om den så kallade "Pre Go live"-fasen. BP5 inträffade i oktober samma år. Den sista beslutspunkten, BP6, där rekommendationer avseende "Go Live" (beslut om driftsättning) förmedlades, inträffade i november 2024.

Riskanalyser

Revisionsfråga 1: Har ändamålsenliga riskanalyser, konsekvensbedömning och lämplighetsbedömning genomförts?

Utgångspunkter

Riskanalyser

Riskanalyser avseende informationssäkerhet (och därför också avseende personuppgiftshantering och integritetsskydd) är en process som syftar till att identifiera och hantera potentiella hot och sårbarheter som kan påverka en organisations informationstillgångar. Kravet att genomföra riskanalyser avseende informationssäkerhet framgår av flera lagstiftningar och föreskrifter, bland annat av lag om informationssäkerhet för samhällsviktiga och digitala tjänster samt socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. Vidare framgår det av MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster att en leverantör ska identifiera, analysera och värdera risker för organisationens information, nätverk och informationssystem.

Inför en upphandling eller innan ett system börjar användas behöver en riskanalys genomföras. Syftet är att tydliggöra vilka krav som behöver ställas och att klarlägga vilka

säkerhetsåtgärder som behöver vidtas för att uppnå ett adekvat skydd. Om riskanalyser inte genomförs på ett ändamålsenligt sätt kan organisationen misslyckas med att uppfylla sina skyldigheter att skydda informationen, vilket i sin tur kan ge upphov till risker för både organisationen och enskilda individer (primärt patienter och anställda i en hälso- och sjukvårdsverksamhet).

Att genomföra (och dokumentera) riskanalyser, och systematiskt arbeta med åtgärdandet av identifierade risker, är också ett sätt att uppfylla principen om ansvarsskyldighet enligt GDPR. Principen innebär att den personuppgiftsansvarige ska kunna visa att behandlingen är förenlig med GDPR och att lämpliga tekniska och organisatoriska åtgärder har vidtagits för att skydda de registrerades rättigheter och friheter (det vill säga kunna visa hur detta går till).

Konsekvensbedömning
Av artikel 35.1 i dataskyddsförordningen följer att den personuppgiftsansvarige ska utföra en dataskyddskonsekvensbedömning om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Bedömning av vad som sannolikt innebär en hög risk ska göras utifrån den förteckning som är framtagen av Integritetsskyddsmyndigheten (IMY) i enlighet med GDPR.72. Exempel på sådana behandlingar kan vara när stora mängder av personuppgifter behandlas, när känsliga personuppgifter behandlas, när de registrerade är i beroendeställning till den personuppgiftsansvarige eller när ny teknik används. Syftet med en konsekvensbedömning är att förebygga risker för registrerades personliga integritet innan de uppkommer. För att identifiera eventuella höga risker behöver som regel en riskanalys föregå en konsekvensbedömning.

Det är den personuppgiftsansvarige som ansvarar för att genomföra en konsekvensbedömning, och konsekvensbedömningen ska som huvudregel utföras innan en behandling påbörjas. Konsekvensbedömningen ska enligt GDPR åtminstone innehålla en systematisk beskrivning av personuppgiftsbehandlingen, bedömning av behovet och proportionaliteten, bedömning av riskerna för de registrerades rättigheter och friheter, samt de planerade skydds- och säkerhetsåtgärderna. Det är också obligatoriskt att konsultera dataskyddsombudet. Om kvarstående sannolika höga risker återstår efter genomförd konsekvensbedömning, ska förhandssamråd begäras hos Integritetsskyddsskyddsmyndigheten.

Lämplighetsbedömning
I samband med utkontraktering av IT-drift till privata tjänsteleverantörer tillgängliggörs i regel en stor mängd information. En myndighet är ytterst ansvarig för att den information som hanteras av, eller på uppdrag av, myndigheten får ett ändamålsenligt skydd och i övrigt hanteras i enlighet med gällande rätt. Enligt den sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL hindrar sekretess inte att en uppgift lämnas till en tjänsteleverantör som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. En myndighet behöver inför ett utlämnande göra en

lämplighetsbedömning för att avgöra om uppgifterna kan tillgängliggöras för en tjänsteleverantör på ett rättsenligt, säkert och lämpligt sätt. Bestämmelsen om lämplighetsbedömning kom 2023 och det finns därmed ännu inte helt tydlig praxis eller vägledning kring vad den ska innehålla eller genomföras.

lakttagelser

Riskanalyser

På uppdrag av regiondirektör genomfördes i maj 2024 en övergripande riskanalys utifrån Region Norrbottens införandeplan för införandet av Cosmic, se *Uppdragsbeskrivning riskanalys för införande av Cosmic* (februari 2024). Riskanalysen genomfördes ur ett patientsäkerhetsperspektiv och inkluderade informationssäkerhet, IT-säkerhet och cybersäkerhet, *Införandet av nytt journalsystem: Övergripande riskanalys ut perspektiven: Informationssäkerhet och patientsäkerhet* (maj 2024).

Analysen omfattade samtliga verksamheter och befintliga processer som berördes av införandet. Syftet med riskanalysen var att ligga till grund för val av ändamålsenliga och proportionella tekniska och organisatoriska säkerhetsåtgärder, enligt uppgifter från regionen. Den dokumenterade övergripande riskanalysen, tillsammans med en rapport för riskanalysen, överlämnades till huvudprojektledare i maj 2024. Enligt rapporten för riskanalysen, *Slutrapport - Övergripande riskanalys driftsättning av Cosmic* (augusti 2024), bedömdes de risker som identifierats vid den övergripande riskanalysen allvarligt påverka patientsäkerheten.

I oktober 2024 genomfördes en uppföljning av den övergripande riskanalysen, vilken redovisats i *Övergripande riskanalys driftsättning av Cosmic - uppföljning* (november 2024). Vid den uppföljande riskanalysen identifierades fortsatt allvarliga risker ur ett patientsäkerhetsperspektiv och ett flertal risker innebar bristande lagefterlevnad och betydande patientsäkerhetsrisker, inklusive röjande av patientuppgifter och brister i konfidentialitet och sekretess. I den uppföljande riskanalysen konstaterar analysteamet att åtgärder behöver vidtas innan systemet tas i drift.

Analysteamet för den övergripande och den uppföljande riskanalysen har bestått av medlemmar från FVIS-projektet, inklusive delprojektledare, teamledare och uppdragsledare, samt kompetenser från regionen inom patientsäkerhet, informationssäkerhet, IT-säkerhet och cybersäkerhet. Genomförda riskanalyser baserades på Sveriges kommuner och regioners handbok *Utredning av risker – Handbok för metoden riskanalys*, 2022. Vid genomförandet har risker och riskernas bakomliggande orsak identifierats och riskbedömningarna har gjorts med metoden “allvarlighetsgrad och sannolikhet”. Förslag på åtgärder för att minska riskernas konsekvenser har tagits fram för risker som bedömts vara mycket allvarliga eller allvarliga, eller då det varit relevant av andra skäl.

Beslut om införande hade planerats till den 11 november men beslut fattades om att senarelägga beslutet till den 18 november, med anledning av att detaljer behövde utredas, enligt *Beslut angående införande av journalsystemet Cosmic* (november 2024). Det framkommer i presentationsunderlaget inför beslut om driftsättning den 18

november att höga risker fortsatt kvarstod och att regiondirektören fattar beslut om driftsättning (BP6) med handlingsplan för att hantera identifierade risker, *20241112 Scenarion riskanalys* (november 2024). Det framgår av presentationsunderlaget att kvarstående risker överlämnas i form av en handlingsplan till mottagande förvaltningsorganisation. Det framgår inte resonemang kring hur de kvarstående riskerna värderas och varför beslut om att gå vidare till införande ändå fattas.

Konsekvensbedömning

Konsekvensbedömningen har genomförts utifrån en mall framtagen av Kompetenscenter välfärdsteknik, Sveriges kommuner och regioner (2022). Den är gjord i flera versioner utifrån att den uppdaterats i takt med att bedömningar har ändrats för att återspegla olika typer av vidtagna åtgärder (exempelvis säkerhetshöjande åtgärder).

I augusti 2024 genomfördes en konsekvensbedömning*, Konsekvensbedömning avseende dataskydd enligt art. 35 GDPR för vård- och omsorgsverksamhet, Framtidens vårdinformationssystem, Cosmic journalsystem, version 0.2*. Ansvarig för genomförandet av konsekvensbedömningen var regiondirektören i sin roll som projektägare, med stöd av FVIS styrgrupp. Enligt *Delprojektrapport status inför BP4 i FVIS-projektet Driftsättningsplanering* (augusti 2024) stöttade uppdraget informationssäkerhet projektet i arbetet genom att ta fram underlag till konsekvensbedömningen. Synpunkter från aspekterna patientsäkerhet, IT-säkerhet och juridik återfinns i konsekvensbedömningen, vilken också inkluderar dataskyddsombudets utlåtande (bedömning och rekommendationer). Underlaget för konsekvensbedömningen överlämnades i en första version samt sammanfattades och ingick som en del i rapporteringen inför BP4 till projektledning.

Den sammantagna bedömningen av genomförd konsekvensbedömningen var att ett flertal risker identifierades och att dataskyddets rekommendation var att inte påbörja behandlingen av personuppgifter innan identifierade risker åtgärdats.

En uppdaterad version av konsekvensbedömningen, *Konsekvensbedömning avseende dataskydd enligt art. 35 GDPR för vård- och omsorgsverksamhet, version 1.0*, genomfördes och överlämnades till projektledningen inför inför beslut om “Go Live” (BP6) i november 2024. Enligt den sammantagna bedömningen var dataskyddsombudet rekommendation fortsatt att inte påbörja behandlingen innan de identifierade riskerna åtgärdats. I huvudsak är det samma risker som nämns i riskanalyser avseende informationssäkerhet och lämplighetsbedömning.

I december 2024 kompletterades konsekvensbedömningen med slutlig bedömning och godkännande. Trots de rekommendationer som framfördes av dataskyddsombudet i bedömningen, fattades beslutet att gå vidare med behandlingen. Detta beslut motiverades med att framsteg avseende de identifierade riskerna hade skett, samt att arbetet ska fortsätta i enlighet med handlingsplaner och överenskommelser. Beslutet, och fastställandet av konsekvensbedömningen, är daterad den 6 december 2024, alltså cirka två veckor efter driftsättningen.

Lämplighetsbedömning

En första version av lämplighetsbedömningen överlämnades till projektledningen inför BP4. Av de resurser som deltog i arbetet att ta fram underlag till bedömningen ingick bland andra informationssäkerhetschef samt informationssäkerhetsresurs och IT-säkerhetsansvarig.

Av den första versionen av lämplighetsbedömningen*, Lämplighetsbedömning vid utkontraktering av IT-drift (*odaterad*),* framgår att risken för röjande av patientuppgifter, brister i konfidentialitet, sekretess och spärrhantering anses vara betydande ur ett patientsäkerhetsperspektiv. Vidare konstateras att bristerna i kontinuitetshantering och incidenthantering för journalsystemet är betydande och att utkontrakteringen av Region Norrbottens patientjournaler därför bedöms vara riskfylld. En uppföljande extern granskning rekommenderas genomföras inför “Go Live”, enligt bedömningen. I delprojektrapport inför BP4 framgår att informationssystemet Cosmic avråds från driftsättning till dess att de områden som identifierats i rapporten är åtgärdade.

En uppdaterad version av lämplighetsbedömning överlämnades till projektledning inför BP6. Utifrån den samlade bedömningen i *Lämplighetsbedömning vid utkontraktering av IT-drift (*december 2024) framgår att samtliga, nödvändiga säkerhetsåtgärder inte bedöms vara vidtagna och att utkontraktering, med beaktande av informationsklassning, riskanalys och/eller konsekvensbedömning, inte anses vara lämplig. Av dokumentet framgår att beslut om utkontraktering bedöms vara tillräckligt bra för att kunna ske, trots identifierade risker.

Båda versionerna av bedömningen innehåller allsidiga bedömningspunkter, där flera olika perspektiv har undersökts och analyserats. Exempelvis bedöms kontraktsvillkoren, som är ett perspektiv som nämns i förarbetet till lagstiftningen och som kan påverka utkontrakteringens lämplighet.

Bedömningen avslutas med en samlad bedömning där utkontrakteringen bedöms som lämplig, trots att merparten av bedömningarna i övrigt i dokumentet lutar åt att utkontrakteringen är olämplig. Dokumentet är fastställt den 6 december 2024, vilket är cirka två veckor efter driftsättningen.

Intervjuer

Vid intervjuer framgår att det övergripande perspektivet på riskhanteringsarbetet (avseende informationssäkerhet och IT-säkerhet) introducerades förhållandevis sent i FVIS-projekt, vilket intervjuade menar har inneburit att ledningen och andra nyckelaktörer inte tidigt nog integrerat dessa aspekter i beslutsfattandet. Det uppges att det inte finns några dokumenterade riskanalyser avseende informationssäkerhet genomförda före hösten 2023. Vid det tillfället genomfördes en SUSSA-gemensam analys riskanalys, som låg till grund för den som regionen genomförde under våren 2024.

Det framgår vid intervjuer att regionen inte genomfört någon second opinion eller liknande avseende analysteamens rekommendationer avseende konsekvens- och

lämplighetsbedömning. Däremot har arbetssättet generellt varit så att slutsatser och rekommendationer har stämts av inom SUSSA samverkan.

Av intervjuer framgår också att den slutliga avvägningen mellan risker och fördelar med att driftsätta systemet som planerat, skedde på muntlig basis utifrån det ovan beskrivna presentationsunderlaget till BP6.

Bedömning

Har ändamålsenliga riskanalyser, konsekvensbedömning och lämplighetsbedömning genomförts?

Delvis.
Riskbedömningen följer en etablerad standard, flera olika kompetenser och perspektiv är genomgående representerade och det har även systematiskt genomförts uppdaterade bedömningar över tid. Den har ett gediget innehåll och alla frågor har fått väl utvecklade svar. Avseende konsekvensbedömningen följer den branschstandard i och med att SKR:s mall används. Konsekvensbedömningen är omfattande och alla frågor har fått väl utvecklade svar. Avseende lämplighetsbedömningen bedömer vi att den följer branschstandard. Den innehåller mycket information och framstår som väl genomarbetad med omfattande analyser.

I alla tre bedömningar och analyser saknas en dokumenterad och utvecklad motivering kring varför fortsatt införande ändå väljs, trots redovisade höga risker och rekommendationer att avbryta införandet. Det saknas även en tydlig redovisning av hur riskerna kan hanteras och därmed reduceras, för att motivera ett införande. Av intervjuer framgår att muntliga resonemang fördes men det är inte tillräckligt för att upprätthålla transparens och spårbarhet avseende beslut. Det är inte ett obligatoriskt krav att inkludera exempelvis ett resonemang om varför dataskyddsombudets rekommendation inte följs, men det skulle minska risken att konsekvenbedömningen blir underkänd av tillsynsmyndigheten och det ökar transparensen generellt. Det bedöms även som en brist att konsekvensbedömning och lämplighetsbedömning är fastställda efter att driftsättning är genomförd eftersom det indikerar att analysen inte var färdigställd innan beslut om “Go Live”.

Generellt, och framförallt i konsekvensbedömning och lämplighetsbedömning, bedömer vi att det saknas analys över de positiva förändringar som införandet av ett nytt vårdinformationssystem kan innebära. Exempelvis lyfts det i konsekvensbedömningen fram risker med att tjänsten levereras som molntjänst. I sammanhanget hade också kunnat lyftas fördelar med molntjänst som driftsform, såsom möjlighet till ökad säkerhet.

Vi bedömer det också som problematiskt att det strukturerade och ändamålsenliga riskarbetet (avseende de områden som är relevanta i denna granskning) har påbörjats för sent (speciellt utifrån att den ursprungliga tidsplanen stipulerade driftsättning under våren 2024). Det går inte att utesluta att, om detta arbete hade påbörjats tidigare, hade diskussionerna med leverantören kunna påbörjats tidigare och därmed hade möjligtvis fler brister kunnat vara åtgärdade vid införandet.

Behörighetstilldelning

Revisionsfråga 2: Har ändamålsenliga risk- och behovsanalyser avseende behörighetstilldelning genomförts?

Utgångspunkter

Flera lagstiftningar och föreskrifter reglerar hur patienters uppgifter ska skyddas vid behörighetstilldelning. Bestämmelser om vårdgivarens ansvar för tilldelning och begränsning av behörigheter för åtkomst till uppgifter om patienter finns i patientdatalagen. Det framgår av Socialstyrelsens föreskrifter och allmänna råd 2016:40 att vårdgivaren ska ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgift och att beslut om tilldelning ska föregås av en behovs- och riskanalys. Vidare ska vårdgivaren ta fram rutiner för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella.

Iakttagelser

Dokumentation

I beslutsunderlag inför BP4 rekommenderades att säkerställa att tilldelning av behörighet till Cosmic sker på individnivå och föregås av behovs- och riskanalys i enlighet med HSLF-FS 2016:40, 4 kap 2§, enligt uppgifter från regionen. Ansvarig för uppföljning av rapportering av status i arbetet är avsedd gruppering inom projektet.

I delprojektrapport *Delprojektrapport, säkerhet status inför BP6 i FVIS-projektet, Driftsättningsplanering* (november 2024) lämnas rekommendationen från den juridiska analysen att inte driftsätta journalsystemet eftersom bedömningen är att systemet inte uppfyller kraven på att vårdpersonal endast ska ha behörighet till information som är nödvändigt för att utföra deras arbetsuppgifter. Det framförs även att Cambio muntligen lämnat uppgift om att systemet förbättrats under hösten 2024, men det är oklart om så verkligen är fallet. Det hänvisas även till information från Region Örebro (som driftsatte Cosmic innan Region Norrbotten) där man har reagerat på att man ser för mycket information. Den samlade rekommendationen som framförs i rapporten, till beslutsfattare, är att följa upp ovan beskrivna farhåga med ytterligare tester.

I rutinen *Behörighet till Cosmic* (september 2024, version 7.0) beskrivs att före beslut och tilldelning av personalens behörighet måste en behovs- och riskanalys göras. Behovs- och riskanalys ska därefter ske löpande minst en gång per år. Arbetet med genomförd risk- och behovsanalys avseende behörighetstilldelning för behörigheter i den nya vårdinformationssystemet har utgått från en regionalt framtagen rutin och dokumenterades i för ändamålet framtagen mall, *Behovs- och riskanalys - behörigheter i Cosmic* (odaterad).

Inom ramen för granskningen har vi tagit del av mallen för behovs- och riskanalysen och tillhörande rutin. Av dokumenten framgår tydligt att de är anpassade till det nya journalsystemet och till nya roller som tillkommit i och med detta.

Intervjuer

Vid intervjuer uppges att samordnare inom avsedd gruppering inom projektet rapporterar att all verksamhet inom Region Norrbotten har inkommit med en behovs- och riskanalys innan någon behörighet i Cosmic tilldelades, enligt framtagen rutin.

Vid intervju i slutet av granskningen uppges att frågan om brister i systemet avseende behörighetsstyrning drivs vidare gentemot leverantören inom ramen för SUSSA samverkan. Ansvarig region inom SUSSA är Region Västernorrland.

Bedömning

Har ändamålsenliga risk- och behovsanalyser avseende behörighetstilldelning genomförts?

Delvis.
Granskningen bedömer att ändamålsenliga risk- och behovsanalyser avseende behörighetstilldelning genomförts. Vi ser att regionen har en utarbetad process för behörighetstilldelning i Cosmic och det bekräftas att all verksamhet inom Region Norrbotten har inkommit med en behovs- och riskanalys innan någon behörighet i Cosmic tilldelats.

Däremot är det tydligt att frågan om den reella åtkomsten till patientuppgifter, oaktat den formella behovs- och riskanalysen, är ett riskområde som inte fått en tillfredsställande lösning innan driftsättningen. Den eventuella praktiska risken riskerar att underminera behovs- och riskanalyserna, och därför är det viktigt att åtgärda den uppkomna osäkerheten. För att balansera denna brist, hade det varit önskvärt med en mer konkret plan för uppföljning och ytterligare testning, vid tiden för driftsättning.

Tjänste- och personuppgiftsbiträdesavtal

Revisionsfråga 3: Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av systemet?

Utgångspunkter
Avseende tjänsteavtalet finns det i princip inga juridiska eller formella krav på innehållet eller utformandet avseende informationssäkerhet, dataskydd och integritetsskydd. Däremot finns det regelverk som omgärdar avtalet, exempelvis lag om offentlig upphandling som styr processen för köpet.

Det som styr om villkoren i avtalet är ändamålsenliga eller ej, är i vilken grad de tillförsäkrar regionen att de lagar och regler som gäller för regionen kan efterlevas även om tjänsten tillhandahålls av en extern part. Det kan handla om villkor av formell karaktär, men det kan också handla om kommersiella villkor som är avsedda att skapa bästa möjliga förutsättningar för att avtalet ska följas och hur olika typer av situationer som kan uppstå ska lösas (exempelvis om leverantören inte kan leverera som planerat).

När det gäller personuppgiftsbiträdesavtalet (PUB-avtalet) är det obligatoriskt enligt GDPR[1] när personuppgifter ska behandlas på uppdrag av en personuppgiftsansvarig (PUA). PUA behöver, både genom kravställning i upphandlingen och genom villkor i

[1] Artikel 28.

PUB-avtalet, förvissa sig om att personuppgiftsbiträdet (PUB) kan behandla personuppgifterna på ett sätt som är lagenligt och ger ett tillräckligt skydd för den enskildes personuppgifter. Utöver det behöver själva PUB-avtalet innehålla ett antal obligatoriska villkor och instruktioner, exempelvis vilka personuppgifter som får behandlas, hur länge de får behandlas och hur personuppgifter ska skyddas för att få ett fullgott skydd. Instruktionerna behöver vara relativt specifika och avgränsade. Syftet med detta är att den personuppgiftsansvariga (regionen i detta fall) ska kunna behålla kontrollen över personuppgiftsbehandlingen.

lakttagelser

Avtalsgranskning

Tjänsteavtal

Granskningen har tagit del av det huvudavtal som tecknats mellan SUSSA-regionerna (inklusive Region Norrbotten) och leverantören, *Framtidens vårdinformationsstöd Avtal köp - Avtalet* (signerad i juni 2020).

Avtalet innehåller sedvanliga villkor såsom avtalstid, beskrivning alternativt bilagor som beskriver tjänsterna som upphandlas och dess innehåll, villkor för hur underleverantörer får användas, villkor om leveranser skulle försenas, pris, upphovsrättsliga villkor, ansvarsreglering vid eventuella skador samt villkor för hävning och uppsägning.

I avtalet bestäms ordningen för hur olika handlingar/bilagor ska gälla i relation till varandra, i det fall innehåll skulle vara motstridigt. Personuppgiftsbiträdesavtalet ligger som nummer sex i ordningen, bland annat efter samverkansmodell och projektplan.

Avtalet innehåller inte något generellt villkor om att leverantören ska följa gällande rätt i sin leverans. Det ställs heller inte krav på att personer som kommer i kontakt med Region Norrbottens information, på leverantörens sida, som standard skriver under en sekretessbekräftelse eller liknande. Det ställs endast krav på att det ska göras på begäran av regionen och det finns inte heller något bilagt dokument som ska användas.

Vidare regleras att leverantören endast får “lämna ut beställarens data” i den utsträckning det är nödvändigt. Vad som avses med “lämna ut” framgår inte, det vill säga om det är data i allmänhet eller endast sådan information som är sekretessbelagd.

Det framgår också att de villkor avseende sekretess som finns under p.12 i tjänsteavtalet även gäller efter att avtalet har upphört att gälla.

Personuppgiftsbiträdesavtal
Bilagt till det ovannämnda huvudavtalet mellan SUSSA-regionerna och leverantören finns ett personuppgiftsbiträdesavtal, *Framtidens vårdinformationsstöd DU-avtal – bilaga DU7 Personuppgiftsbiträdesavtal* (juni 2020).

Avtalet, inklusive instruktionen för personuppgiftsbehandlingen, följer i allt väsentligt den struktur för personuppgiftsbiträdesavtal som Sveriges kommuner och regioner har tillgängliggjort som mall.

Personuppgiftsbiträdet (leverantören) förbinder sig i detta avtal att följa instruktionerna i avtalet, följa dataskyddslagstiftning samt hålla sig uppdaterad på gällande rätt inom området. Biträdet förbinder sig också att vidta åtgärder för att skydda personuppgifterna från alla slags behandlingar som inte är förenliga med avtalet och instruktionerna och dataskyddslagstiftning.

I personuppgiftsbiträdesavtalet (PUB-avtalet) framgår också att biträdet ska se till att samtliga personer som arbetar under dess ledning, underbiträden (underleverantörer) och dess personal, är under lagstadgad tystnadsplikt eller förbinder sig till sekretess genom avtal.

Vidare ger PUB-avtalet den personuppgiftsansvarige rätt att göra granskningar och revisioner hos biträdet. Avseende överföringar av personuppgifter utanför EU (så kallade tredjelandsöverföringar) får dessa inte göras utan den personuppgiftsansvariges skriftliga godkännande och instruktioner. I avtalet regleras också att den begränsning av ansvar för skada som finns enligt huvudavtalet, inte gäller om skadan avser personuppgiftsbehandling.

Instruktionen för biträdets behandling av personuppgifterna innehåller en beskrivning av ändamålet för behandlingen, där det beskrivs att ändamålet följer av huvudavtalet. Det beskrivs även att behandlingen inte är begränsad till support, underhåll, konsultsupport och kundnöjdhetsundersökningar. Avseende vilken typ av personuppgifter som får behandlas nämns ett antal, exempelvis namn, personnummer och “hälsorelaterad data” samt att det i huvudsak är patienter, närstående och anställdas personuppgifter som behandlas. Instruktionen innehåller ingen närmare anvisning om överföringar till tredje land utan hänvisar endast tillbaka till personuppgiftsbiträdesavtalet.

Avseende krav på skyddsåtgärder i instruktionen utgår dessa från kontrollmoment i ISO27002-standarden. Det beskrivs exempelvis att biträdet ska säkerställa att personuppgifterna skyddas av obehöriga, är åtkomliga för behöriga, att de hålls oförvanskade och att det ska finnas spårbarhet avseende tillgång till personuppgifterna. Avseende olika typer av fysiskt skydd beskrivs dessa åtgärder mer detaljerat, exempelvis att IT-system ska skyddas av brandväggar och antivirusprogram.

Övrig dokumentation

I presentationsunderlaget inför BP6 beskrivs att det ofullständiga personuppgifts-biträdesavtalet är en risk avseende patientsäkerhet.

I *Konsekvensbedömning avseende dataskydd enligt art. 35 GDPR för vård- och omsorgsverksamhet*, daterad 2024-11-04, beskrivs att leverantören har support för tjänsten i Sri Lanka, och därmed sker en tredjelandsöverföring i strid med personuppgiftsbiträdesavtalet.

Intervjuer

Vid intervju uppges att personuppgiftsbiträdesavtalets instruktion har bedömts vara i behov av uppdatering. Därför har det inom SUSSA samverkan arbetats med en ny version. Arbetet uppges ha pågått i flera års tid och vara nästan klart. Dock finns det inga beslut om en ny instruktion, eller överenskommelse med leverantören.

Bedömning

Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av systemet?

Delvis

Tjänsteavtalet bedöms i allt väsentligt följa branschstandard och innehålla relevanta villkor. Avseende villkoren för sekretess är dessa relativt otydligt formulerade. Exempelvis framgår inte vad “lämna ut beställarens data” innebär, vilket skapar en onödig otydlighet avseende hur sekretessbelagda uppgifter ska hanteras.

PUB-avtalet, exklusive instruktionen, bedöms i allt väsentligt följa branschstandard och innehålla relevanta villkor. Däremot är instruktionen varken fullständig eller korrekt.

Avsnittet som beskriver ändamålet för personuppgiftsbehandlingen är otydligt formulerad. Det är möjligt att tolka skrivningen som att behandlingen avser support, underhåll, konsultsupport och kundnöjdhetsundersökningar. En sådan tolkning skulle innebära att instruktionen exkluderar huvuddelen, och den mest känsliga delen av behandlingen, nämligen lagringen och bearbetningen av patientuppgifter.

Utifrån övriga dokument drar vi slutsatsen att regionen har konstaterat att en överföring av personuppgifter kommer att ske till Sri Lanka, vilket innebär en tredjelandsöverföring. I och med att det helt saknas stöd för detta i instruktionen är det en överföring som strider mot det ingångna avtalet, vilket skapar konsekvenser för både regionen och leverantören avseende ansvarsförhållandena.

Instruktionen är en helt central del när ett biträde anlitas för att behandla personuppgifter, eftersom den styr vilka uppgifter som får behandlas, och hur det ska ske. Därför är det viktigt att instruktionen är både fullständig och korrekt, men också tydligt formulerad. Risken finns annars att personuppgifter överförs till biträdet, samt att denna behandlar uppgifterna, utan rättsligt stöd.

Det är vanligt att förutsättningarna för personuppgiftsbehandlingar förändras. Instruktionerna kan komma att behöva ändras både ofta och med relativt kort varsel. I detta fall bedömer vi att regionen och SUSSA samverkan har haft mycket gott om tid på

sig att både uppdatera instruktionen och komma överens med leverantören om en uppdaterad version.

Den 6 december 2024 undertecknades en ny instruktion avseende personuppgiftsbehandlingen som i allt väsentligt läker de ovan beskrivna bristerna. Dock är det fortfarande en brist att detta inte fanns på plats redan vid driftsättningen, särskilt eftersom det fanns så gott om tid inför driftsättandet att åtgärda instruktionen.

Systemtester

Revisionsfråga 4: Har ändamålsenliga tester av systemet genomförts?

Utgångspunkter

Enligt socialstyrelsens allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården ska ett informationssystem testas innan det tas i drift.[2]

Det framgår också av MSB:s vägledning avseende säkerhetsåtgärder i informationssystem att organisationen innan driftsättning av ett nytt informationssystem behöver göra tester för att upptäcka eventuella brister som kan påverka säkerheten i IT-miljön. Sådana kontroller kan göras på olika sätt, exempelvis genom säkerhetstester, granskning eller verifiering av dokumentation. I samband med utvecklingsarbete behöver det tas fram en testplan som beskriver behovet av tester under utvecklingsarbetet så att fel och brister upptäcks och kan rättas till före driftsättning. Det är lämpligt att testplanen beskriver vilka tester som ska utföras och när samt hur testerna ska genomföras.

Av MSB:s vägledning framgår vidare att innan ett informationssystem godkänns och förs över till produktionsmiljön, ska valda säkerhetsåtgärder inklusive säkerhetsfunktioner vara aktiverade samt brister som upptäcks i samband med tester, granskningar och verifiering av dokumentation vara åtgärdade. Om det finns brister som det inte går att göra något åt behöver dessa riskbedömas.

Iakttagelser

Dokumentation

Testrapport för Region Norrbotten leveransobjekt informationssäkerhet inom Framtidens VårdInformationsStöd (januari 2024, version 0.1) är en del av kvalitetssäkring och ingår i Region Norrbottens användaracceptanstest. Rapporten baseras på de funktionella tester som genomförts kopplade till lagkrav i två avtalade funktioner: journal och patientöversikt. Testerna har genomförts inom området informationssäkerhet i samarbete inom SUSSAs informationssäkerhetsgrupp. Tester och testrapporter för Region Norrbottens leveransobjekt informationssäkerhet inom FVIS har överlämnats till delprojektet Test. Testerna inom området omfattar test av aspekter inom informationssäkerhet med fokus på lagefterlevnad där tillräcklig testtäckning för att göra en kvalificerad bedömning av kvaliteten behöver uppnås. Ansvarig för uppföljning av rapportering av statusen för dessa tester är grupperingen Test inom FVIS-projektet i Region Norrbotten. I testrapporten identifieras många betydande risker. Bland annat

[2] 3 kap. 7 §.

identifieras risken att vårdpersonal behöver ta del av för mycket journalinformation, att sekretess inte kan upprätthållas och risk för att relevant information om patienten som finns hos annan vårdgivare missas.

Det framgår i *Delprojektrapport säkerhet status inför BP6 i FVIS-projektet Driftsättningsplanering* (november 2024) att uppdraget för test ingår i FVIS-delprojektet Teknik. Det framgår vidare att tester avseende vårdinformationssystemet har utförts på en kombinerad system- och acceptanstestnivå, där syftet är att säkerställa att Region Norrbotten kan driftsätta Cosmic journalsystem som en tjänst. Testfall, checklistor och felrapporter har hanterats i testverktyget ReQtest och testaktiviteterna har hanterats i verktyget JIRA. Alla felrapporter har hanterats i JIRA och leverantörens supportcenter.

Det framgår vidare i samma dokument att leverantören i augusti 2024 lämnade sin Statement of applicability (SOA) enligt ISO 27001:2022, vilken innehöll säkerhetsåtgärder från ISO 27002:2022 (DOCID-1488585834-140). SOA innehåller ett antal säkerhetsåtgärder som utgår från testning. För att undersöka hur Cambio arbetar med testning har Region Norrbotten, genom SUSSA samverkan, ställt kompletterande frågor till leverantören, vilket framgår av delprojektrapporten. Den 13:e november 2024 inkom Cambios uppgraderade certifiering till ISO 27001:2022.

I samma dokument framgår det också en rekommendation att följa upp tidigare tester och granskningar (bland annat avseende informationssäkerhet och integritetsskydd).

I presentationsunderlaget inför beslut om “Go Live” (november 2024), framgår att testning av vårdinformationssytemet har genomförts men inte med fullständigt godkända resultat (exempelvis avseende avgränsning av information, loggning och journalspärrar). De bristande testresultaten är inte uppföljda genom nya tester. Handlingsplan för att åtgärda de identifierade bristerna har efterfrågats från Cambio men inte erhållits.

Regiondirektörens beslut om driftsättning av Cosmic den 18 november 2024 innehåller en hänvisning till ovan nämnda rekommendation. Dock har det inte under granskningen identifierats någon mer konkret plan om uppföljande testning än ovannämnd rekommendation.

<u>Intervjuer</u>
Vid intervjuer framkommer att bristande resultat vid tester, samt i vissa fall utebliven testning, har varit ett betydande orosmoment under längre tid. Det beskrivs också hur dialog med leverantören förts under året, samt att externa granskningar har genomförts för att ytterligare skapa klarhet kring eventuella brister och för att tillförsäkra regionen korrekta beslutsunderlag.

Vid intervjuer beskrivs också vissa svårigheter att snabbt och flexibelt agera utifrån identifierade brister hos leverantören. Region Norrbotten är endast en av flera aktörer inom SUSSA samverkan och en gemensam koordination och prioritering behöver ske inom samarbetet. Det innebär vissa svårigheter att agera gentemot leverantören utifrån endast Region Norrbottens perspektiv och prioritering, samtidigt som det inför

driftsättning i just Region Norrbotten primärt är regionen som har risker att ta ställning till och hantera.

Bedömning

Har ändamålsenliga tester av systemet genomförts?

Delvis.
Vi bedömer att de krav som finns i allmänna råd och vägledningar är uppfyllda. Det är också positivt att testning och granskning har varit jämförelsevis omfattande, samt att regionen har varit aktivt pådrivande gentemot leverantören avseende åtgärdande av identifierade brister. Däremot är det tydligt att test- och granskningsresultaten inte är tillfredsställande och inte heller åtgärdade innan systemet driftsattes. För att balansera denna brist, hade det varit önskvärt med en mer konkret plan för uppföljning och ytterligare testning, vid tiden för driftsättning.

Uppföljning av avtal

Revisionsfråga 5: Finns ändamålsenlig planering för uppföljning av leverantör och avtal?

Utgångspunkter
Regionen har, i rollen som bland annat vårdgivare och personuppgiftsansvarig, ansvaret för att den information som hanteras används och skyddas på ett erforderligt sätt. I det fall uppgiften att hantera informationen lämnas över till en tredje part, exempelvis genom att köpa tjänsten vårdinformationssystem, gäller samma ansvar. Skillnaden blir i praktiken att istället för att göra uppföljningar och kontroller i den egna verksamheten, behöver uppföljningen möjliggöras genom kravställande i upphandling, villkor i avtal samt genomförande hos leverantör i praktiken.

Krav på uppföljning framgår bland annat genom GDPR. Den personuppgiftsansvarige får endast anlita biträden som ger "tillräckliga garantier" för att den enskildes integritet skyddas.[3] Europeiska dataskyddsstyrelsen har, i vägledning för hur kravet ska tolkas, uttalat att detta är en kontinuerlig förpliktelse som behöver följas upp av den personuppgiftsansvarige, genom exempelvis revisioner och inspektioner.[4]

Att planera för kontinuerlig uppföljning, och därefter genomföra den, är således avgörande både för att minimera risker och säkerställa att systemet är tillräckligt säkert, men också för att skydda enskildas integritet i enlighet med gällande lagkrav.

Iakttagelser
Avtal
I tjänsteavtalet kan vi inte identifiera villkor som avser uppföljning avseende informationssäkerhet, IT-säkerhet eller personuppgiftshantering. I PUB-avtalet regleras att biträdet minst en gång om året ska utföra en egenkontroll för att säkerställa att PUB-avtalet följs. Protokollet från egenkontrollen ska på begäran delges den personuppgiftsansvarige. PUB-avtalet medger också att den personuppgiftsansvarige själv, eller genom ombud, får följa upp biträdet, exempelvis genom

[3] GDPR art. 28.
[4] Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR Version 2.0, p. 99.

dokumentationsgranskning eller fysiskt i lokaler. Det framgår också att sådan revision normalt ska ske en gång per kalenderår men kan även ske oftare.

Övrig dokumentation

I *SUSSA vårdstöds samverkanshandbok* framgår att det i SUSSA samverkan finns ett gemensamt avtalsforum där representanter från regionerna deltar. I forumet följs avtal och leverantör upp.

I beslutsunderlaget inför BP6 lämnas ett antal rekommendationer som avser uppföljning, exempelvis avseende tjänsteleverans, ytterligare tester avseende bland annat behörighetsstyrning samt uppföljning av olika typer av säkerhetsåtgärder. Det framgår av samma underlag att handlingsplan överlämnas till mottagande förvaltningsorganisation. Inom ramen för denna granskning har vi inte tagit del av tidssatta planer för uppföljning.

Intervjuer

Under intervjuer beskrivs att utifrån de granskningar som ditintills genomförts av leverantören, förs diskussioner inom ramen för SUSSA samverkan där beslut fattas av styrgruppen.

Bedömning

Finns ändamålsenlig planering för uppföljning av leverantör och avtal?

Ja.

Genom villkoren i avtalen har regionen skapat formella förutsättningar för att kunna följa upp leverantören och leveransen, vilket är grundläggande. Mot bakgrund av att uppföljningar genomförts redan innan driftsättning bedömer vi det som rimligt att det vid tiden för granskningen inte finns tidssatta planer för uppföljning. Däremot framgår det att fler uppföljningar avser att genomföras, vilket också är viktigt att så sker och inte drar ut på tiden.

Sammantaget bedöms att planering för uppföljning i allt väsentlig är ändamålsenlig.

Utbildningsplan

Revisionsfråga 6: Finns ändamålsenlig utbildningsplan för vårdinformationssystemets användare?

Utgångspunkter

En ändamålsenlig utbildningsplan är avgörande för att säkerställa att ett vårdinformationssystem används effektivt och säkert. Enligt MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster ska leverantören (i detta fall regionen) ha interna regler och arbetssätt som säkerställer att medarbetarna har kunskap om säker hantering av information. Detta ska dels säkerställas genom att

medarbetarnas kompetens upprätthållas genom utbildning, informationsinsatser och övning, både regelbundet och utifrån identifierat behov.[5]

Ändamålsenlig och kontinuerlig utbildning och övning, som är ändamålsenlig för olika personalkategorier är också ett av kontrollmomenten i ISO-standard 27002:22.[6] Enligt ovannämnda föreskrifter ska informationssäkerhetsarbetet bedrivas med stöd av ISO-standarden, eller motsvarande. Det innebär i praktiken att kontrollpunkterna i ISO-standarden bör fungera som en utgångspunkt för arbetet med informationssäkerhet för Region Norrbotten.

Om användarna inte får en fullständig och ändamålsenlig utbildning kan det medföra flera betydande risker. Utan ordentlig utbildning kan personalen sakna förståelse för vikten av informationssäkerhet och omedvetet bryta mot lagar och förordningar. Kunskap och förståelse för hur systemet ska hanteras och användas är också indirekt viktiga aspekter av säkerhetsperspektivet; brister det i handhavandet riskerar även det säkraste systemet att hanteras på ett osäkert sätt som i sin tur kan skapa säkerhetsrisker för informationen i systemet.

Iakttagelser

Dokumentation

Det regionala arbetet med utbildningar sammanfattas i *Rapport FVIS delprojekt utbildning* (oktober 2024). Det framgår av rapporten att en regional utbildningsplan finns framtagen. Dokumentet ger ingående information om utbildningsorganisationen och beskriver att utbildningen sker i olika steg: E-learnings, utbildningsfilm, klassrumsdag, tilläggskurser och certifiering. Utbildningen består av en funktionell utbildning som bygger på olika moduler i informationssystemet. Medarbetaren går igenom e-learnings och utbildningsfilm innan denne tar del av övningsuppgifter i Cosmic utbildningsmiljö, vilken är en simulerad version av Cosmic, där användarna kan bekanta sig med systemet och testa olika funktioner. Övningsuppgifterna beräknas ta cirka sex timmar att genomföra. Det beskrivs också att det är olika utbildningsprogram för olika roller.

Det framgår av samma dokument att det finns en framtagen handledning för alla användarstöd och att information till vårdinformationssystemets användare finns tillgänglig på intranätet. I uppdraget Användarstöd, som ingår i förvaltningen, ingår ett långtidsuppdrag som syftar till att stödja enhetens användare i Cosmic. Det framgår av nämnda dokument att utbildning/repetition ska ha genomförts under hösten 2024 med stöd av *Cosmic Användarstöd Utbildning av medarbetare* (odaterad, version 2.0). Det framgår också att support (avseende både användning och tekniska problem) planerades att vara tillgänglig dygnet runt från driftsättning och en vecka framåt. Därefter planerades för att samma support skulle vara tillgänglig under kontorstid.

[5] 9 §.
[6] P. 6.3.

Det framgår av utbildningsplanen att vidare utbildningsinsatser överlämnas till förvaltning efter driftsättning av systemet, *Utbildningsplan - Införande Cosmic* (odaterad).

Inför BP6 genomfördes en sammanställning och uppföljning av identifierade risker - *Riskanalys Övergripande riskanalys driftsättning av Cosmic - uppföljning November 2024.* Där beskrivs att orsaksområdet "utbildning och kompetens" var en av de högst klassade riskerna vid analysen i maj 2024. Riskerna beskrivs bestå av bristande utbildning och möjlighet till repetition, samt att verksamheter kan ta fram egna rutiner vilket i sin tur kan leda till olika arbetssätt och bristande kvalitetssäkring. Riskerna beskrivs ha hanterats på olika sätt och därmed har riskpoängen sänkts till den uppföljande analysen i oktober 2024.

Intervjuer

Vid intervjuer beskrivs att 2022 beslutades om en gemensam utbildningsstrategi inom SUSSA samverkan. Den har i sin tur resulterat i en utbildningsplan för regionen,vilken brutits ner i olika typer av konkreta utbildningsinsatser, där allt finns samlat på regionens intranät. Vidare beskrivs hur informationssäkerhetsperspektivet har inkorporerats i utbildningsinsatserna på flera sätt. Till exempel har informationssäkerhet, som nämnts ovan, förekommit som en del av utbildningen som genomförts, både i klassrum och i utbildningsfilmer.

Utöver det har utbildningsinsatser inom informationssäkerhet och riskanalys för angiven målgrupp genomförts inom ramen för FVIS under våren 2024, som framgår av *Delprojektrapport säkerhet status inför BP6 i FVIS-projektet Driftsättningsplanering* (november 2024). Syftet med utbildningsinsatsen var att höja medvetenheten om informationssäkerhet, IT-säkerhet, cybersäkerhet och dataskydd.

Bedömning

Finns ändamålsenlig utbildningsplan för vårdinformationssystemets användare?

Ja.

Granskningen visar att Region Norrbotten har genomfört en omfattande utbildning för det nya vårdinformationssystemet, vilket vi bedömer har skapat goda förutsättningar för att användarna ska ha kunskap om säker hantering av information. Genom att säkerställa att användarna har en god förståelse för systemet, läggs grunden för att de ska kunna använda det på ett säkert sätt och uppfylla kraven på informationssäkerhet. Det är särskilt positivt att utbildning och övning har kunnat ske i en simulerad system-miljö eftersom det ger en betydligt bättre möjlighet till förberedelse, jämfört med endast teoretiska övningar. Det är också fördelaktigt att informationssäkerhet har integrerats i utbildningen, det vill säga både direkt till användarna och indirekt genom att utbildarna själva har fått kompetensutveckling inför utbildningstillfällena.

Rutiner och vägledning

Revisionsfråga 7: Finns ändamålsenliga regler, rutiner och vägledning som reglerar och stödjer användningen av det nya systemet?

Utgångspunkter
Vid införandet av ett nytt journalsystem är det avgörande att ha tydliga regler, rutiner och vägledning på plats då dessa element säkerställer att systemet implementeras och används på ett effektivt och säkert sätt, samtidigt som det uppfyller gällande krav.

Det framgår av MSB:s vägledning av säkerhetsåtgärder i informationssystem att organisationen,[7] åtminstone i slutet av utvecklingsarbetet, behöver verifiera att det finns nödvändig dokumentation för att drift, förvaltning och användare ska kunna behandla information och informationssystem på ett säkert sätt.

Iakttagelser
Intervjuer
Vid intervjuer visas hur delprojektet *Verksamhetens införande* är uppbyggt. Delprojektet har en projektledare. För respektive vårddivision samt de övergripande områdena regionstöd och regiongemensamt har Införandeledare lett arbetet med införandet. Inom divisionerna och de övergripande områdena har det sedan funnits cirka 30 stycken Verksamhetsstöd. På enhetsnivå har det slutligen funnits Coacher, cirka 250 till antalet.

Alla dessa funktioner har tillsammans arbetat med att ta fram både rutiner och arbetssätt. När utkast till rutiner under hand blivit klara, har dessa godkänts (eller lämnats tillbaka för vidare arbete) av en klinisk referensgrupp som bestått av läkare. När rutinerna är godkända publiceras de på Vårdgivarwebben, och därefter har Införandeledare och Verksamhetsstöd ansvar för att sprida och förankra de nya rutinerna och arbetssätten. Utöver det har projektet även implementerat och visualiserat rutinerna på olika informationstillfällen digitalt (exempelvis intranätet) samt på chefsforum digitalt.

Vid driftsättningen av vårdinformationssystemet är det i första hand Coacher och Verksamhetsstöd som stöttar övriga användare med rutiner och arbetssätt. Region Norrbotten har upprättat en gemensam support där både IT- och verksamhetsfrågor ska besvaras.

Dokumentation
Inom ramen för denna granskning har stickprovskontroller genomförts på hemsidan Vårdgivarwebben. Kontrollen visar att det finns uppdaterade rutiner inom de flesta relevanta områdena. I de flesta fall indikerar dateringen på rutinen att det publicerats efter driftsättningen. Kontrollen visar exempelvis att rutiner för hur skyddade personuppgifter i Cosmic ska hanteras, diktering och transkribering i Cosmic samt vårddokumentation ska gå till (alla tre exempel på rutiner med särskild betydelse för informationssäkerhet och skydd för enskildas integritet).

Under granskningen har vi inte kunnat identifiera att en samlad utvärdering av rutiner och vägledningar genomförts.

[7] S. 35.

Bedömning

Finns ändamålsenliga regler, rutiner och vägledning som reglerar och stödjer användningen av det nya systemet?

Ja.

Granskningen visar att regler, rutiner och vägledningar har arbetats fram och godkänts av en för detta avsedd gruppering, där flera kompetenser har ingått. Rutinerna har därefter kommunicerats inom verksamheten, både genom digitala informationstillfällen och via öppen webbsida. Det är tydligt att det funnits en systematik för arbetssättet med en medvetenhet om vikten av förankring över hela organisationen.

Det är också positivt att det avsattes en utökad supportfunktion för både användningsfrågor och teknisk support för tiden för migrering och veckorna efteråt (så som redogörs för under fråga 6). I kombination med en välutvecklad struktur för instruktioner bedömer vi att det därigenom skapats ändamålsenliga förutsättningar för användningen av det nya vårdinformationssystemet. Bristen vi kunnat identifiera är avsaknaden av en samlad utvärdering av utbildningsupplägget. Dock skall denna brist ses i ljuset av andra insatser, där exempelvis utbildning, och risken för otillräcklig sådan, hanterats genom riskanalysen. Därför bedömer vi inte avsaknaden av en samlad utvärdering som avgörande i detta skede.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Norrbotten genomfört en granskning. Granskningens syfte är att bedöma om regionstyrelsen har säkerställt att implementering av nytt vårdinformationssystem sker i enlighet med gällande lagstiftning och på ett ändamålsenligt sätt. Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen **inte helt** har säkerställt att implementeringen skett i enlighet med gällande lagstiftning och på ett ändamålsenligt sätt.

Granskningen bedömer att riskanalyser, konsekvensbedömningar och lämplighetsbedömningar följer lagkrav och branschstandard samt att de utförts och uppdaterats i takt med ändrade förutsättningar. Vi bedömer det som en brist att konsekvens- och lämplighetsbedömning fastställdes efter driftsättning, och som problematiskt att det strukturerade riskarbetet påbörjades för sent. Granskningen bedömer vidare att ändamålsenliga risk- och behovsanalyser avseende behörighetstilldelning har genomförts. Däremot är det tydligt att frågan om den reella åtkomsten till patientuppgifter är ett riskområde som inte fått en tillfredsställande lösning innan driftsättningen. Det bedöms även som en generell brist att det saknas en dokumenterad och utvecklad motivering kring varför fortsatt införande ändå väljs, trots redovisade höga risker och rekommendationer att avbryta införandet. Det saknas även en tydlig redovisning av hur riskerna ska hanteras och därmed reduceras.

Avseende riskanalyserna vill vi understryka att de är i grunden väl genomförda, och att det är tydligt att det finns en grundläggande systematik i arbetet som är positiv. Det är framförallt den sista delen som avser analys och motivering kring varför risker och brister trots allt accepteras som behöver förbättras.

Tjänsteavtalet och PUB-avtalet, exklusive instruktionen, bedöms i allt väsentligt följa branschstandard och innehålla relevanta villkor. Instruktionen är däremot varken fullständig eller korrekt. Granskningen visar att regionen har konstaterat att en överföring av personuppgifter kommer att ske till Sri Lanka (en tredjelandsöverföring), vilket det saknas stöd för i instruktionen. Således är det en överföring som strider mot det ingångna avtalet.

Avseende huruvida ändamålsenliga tester av systemet har genomförts bedömer vi att de krav som finns i allmänna råd och vägledningar är uppfyllda. Däremot är det tydligt att test- och granskningsresultaten inte är tillfredsställande och inte heller åtgärdade innan systemet driftsattes. Avseende ändamålsenlig planering för uppföljning av leverantör och avtal har regionen, genom villkor i avtalen, skapat formella förutsättningar för att kunna följa upp leverantören och leveransen. Mot bakgrund av att uppföljningar genomförts redan innan driftsättning bedömer vi det som rimligt att det vid tiden för granskningen inte finns tidssatta planer för uppföljning.

Avslutningsvis bedömer vi att Region Norrbotten, genom relativt omfattande utbildningsinsatser, har skapat goda förutsättningar för att användarna ska ha kunskap

om säker hantering av information. Det är också fördelaktigt att informationssäkerhet har integrerats i utbildningen. Granskningen visar att regler, rutiner och vägledningar har arbetats fram och godkänts av en för detta avsedd gruppering, och därefter kommunicerats inom verksamheten. Det är tydligt att det funnits en systematik för arbetssättet.

Rekommendationer
Regionstyrelsen rekommenderas att:

- Säkerställa att riskanalyser avseende informationssäkerhet, konsekvensbedömningar avseende dataskydd samt lämplighetsbedömningar avseende sekretess, påbörjas i ett tillräckligt tidigt skede i framtida upphandlingar och införanden av IT-system och -tjänster,
- Säkerställa att de höga risker som inte kunnat reduceras innan driftsättning, snarast följs upp och åtgärdas,
- Säkerställa att de handlingsplaner (inklusive ytterligare tester och fortsatta externa granskningar av leverantören) som överlämnas från projektet till förvaltningen av vårdinformationssystemet genomförs,
- Säkerställa att slutgiltiga beslut avseende beslut om driftsättning, fastställande av riskanalyser, lämplighetsbedömning och liknande motiveras skriftligt.

Sammanfattande bedömningar utifrån revisionsfrågor

För fullständiga bedömningar, se respektive revisionsfråga i rapporten.

Revisionsfråga	Bedömning	
1. Har ändamålsenliga riskanalyser, konsekvens-bedömning och lämplighets-bedömning genomförts?	**Delvis** Utifrån genomförd granskning bedömer vi att genomförda riskanalyser, konsekvens-bedömningar och lämplighets-bedömningar följer branschstandard. Vi noterar att det i alla tre bedömningar och analyser saknas en dokumenterad och utvecklad motivering kring beslutet om fortsatt införande. Vi bedömer det som en brist att konsekvens- och lämplighetsbedömning fastställdes efter driftsättning. Granskningen bedömer det som problematiskt att det strukturerade riskarbetet påbörjats för sent. Den sammantagna bedömningen är att analyser och bedömningar följer lagkrav och branschstandard samt att de utförts och uppdaterats i takt med ändrade förutsättningar.	
2. Har ändamålsenliga risk- och behovsanalyser avseende behörighets-tilldelning genomförts?	**Delvis** Vi ser att regionen har en utarbetad process för behörighetstilldelning i Cosmic och det bekräftas att all verksamhet inom Region Norrbotten har inkommit med en behovs- och riskanalys innan någon behörighet i Cosmic tilldelats. Däremot är det tydligt att frågan om den reella åtkomsten till patientuppgifter är ett orosmoment som inte fått en tillfredsställande lösning innan driftsättningen.	
3. Finns ändamålsenligt tjänste- och person-uppgiftsbiträdesavtal med leverantören av systemet?	**Delvis** Tjänsteavtalet bedöms i allt väsentligt följa branschstandard och innehålla relevanta villkor. PUB-avtalet, exklusive instruktionen, bedöms i allt väsentligt följa branschstandard och innehålla relevanta villkor. Instruktionen är däremot varken fullständig eller korrekt. Granskningen visar att	

	regionen har konstaterat att en överföring av personuppgifter kommer att ske till Sri Lanka (en tredjelandsöverföring), vilket det saknas stöd för i instruktionen, och således är det en överföring som strider mot det ingångna avtalet. Vi bedömer att regionen och SUSSA samverkan har haft mycket gott om tid på sig att både uppdatera instruktionen och komma överens med leverantören om en uppdaterad version.	
4. Har ändamålsenliga tester av systemet genomförts?	**Delvis** Vi bedömer att de krav som finns i allmänna råd och vägledningar är uppfyllda. Det är positivt att testning och granskning har varit jämförelsevis omfattande, samt att regionen har varit aktivt pådrivande gentemot leverantören avseende åtgärdande av identifierade brister. Däremot är det tydligt att test- och granskningsresultaten inte är tillfredsställande och inte heller åtgärdade innan systemet driftsattes. För att balansera denna brist, hade det varit önskvärt med en mer konkret plan för uppföljning och ytterligare testning, vid tiden för driftsättning.	
5. Finns ändamålsenlig planering för uppföljning av leverantör och avtal?	**Ja** Avseende ändamålsenlig planering för uppföljning av leverantör och avtal har regionen, genom villkor i avtalen, skapat formella förut-sättningar för att kunna följa upp leverantören och leveransen. Mot bakgrund av att uppföljningar genomförts redan innan driftsättning bedömer vi det som rimligt att det vid tiden för granskningen inte finns tidssatta planer för uppföljning.	

6. Finns ändamålsenlig utbildningsplan för vårdinformations-systemets användare?	**Ja** Region Norrbotten har genomfört en omfattande utbildning för det nya vårdinformationssystemet, vilket vi bedömer har skapat goda förut-sättningar för att användarna ska ha kunskap om säker hantering av information. Det är särskilt positivt att utbildning och övning har kunnat ske i en simulerad systemmiljö eftersom det ger en betydligt bättre möjlighet till förberedelse jämfört med endast teoretiska övningar. Det är också fördelaktigt att informationssäkerhet har integrerats i utbildningen.	
7. Finns ändamålsenliga regler, rutiner och vägledning som reglerar och stödjer användningen av det nya systemet?	**Ja** Granskningen visar att regler, rutiner och vägledningar har arbetats fram och godkänts av en för detta avsedd gruppering och därefter kommunicerats inom verksamheten. Det är tydligt att det funnits en systematik för arbetssättet och det är positivt att det avsatts en utökad supportfunktion. Vi bedömer att det skapats ändamålsenliga förutsättningar för användningen av det nya vårdinformationssystemet. Vi bedömer inte avsaknaden av en samlad utvärdering som avgörande i detta skede.	

27 januari 2025,

Kristian Damlin	Charlotte Arnell
Uppdragsledare	*Projektledare*

Bilaga - Förteckning över granskad dokumentation

Riskanalyser, konsekvensbedömning och lämplighetsbedömning

- Uppdragsbeskrivning riskanalys för införande av Cosmic, februari 2024
- Fastställande av nivå för informationsklassning Cosmic, juni 2024
- Delprojektrapport inför BP4 augusti 2024, delprojektrapport inför BP6 inför beslut 11 november 2024 och delprojektrapport inför BP6 inför beslut 18 november 2024
- Införande av Framtidens vårdinformationsstöd, FVIS, delegationsbeslut, mars 2020
- Konsekvensbedömning avseende dataskydd enligt art. 35 GDPR för vård- och omsorgsverksamhet, första version i mars 2024 samt version till beslutsfattare i november 2024
- Lämplighetsbedömning vid utkontraktering av IT-drift - Mallformulär för genomförande av lämplighetsbedömning i enlighet med 10 kap. 2 a § offentlighets- och sekretesslagen (2009:400), första version inför BP4 samt version till beslutsfattare i november 2024
- Införandet av nytt journalsystem (övergripande riskanalys ut perspektiven informationssäkerhet och patientsäkerhet), maj 2024
- Övergripande riskanalys driftsättning av Cosmic, augusti 2024, och uppföljande rapport, november 2024

Risk- och behovsanalyser avseende behörighetstilldelning

- Rutin behörighet till Cosmic (odaterad)
- Behovs och riskanalys behörigheter i Cosmic, september 2024

Tjänste- och personuppgiftsbiträdesavtal

- Inriktningsbeslut Framtidens vårdinformationsstöd FVIS, ärende till regionstyrelsen i april 2020
- Införande av Framtidens vårdinformationsstöd FVIS, delegationsbeslut mars 2020
- Framtidens vårdinformationsstöd, Avtal köp, undertecknad juni 2020
- Personuppgiftsbiträdesavtal (PUBA), DU-avtal – bilaga DU7, 2020
- Framtidens vårdinformationsstöd DU-avtal – bilaga DU7-1, Personuppgiftsbiträdesavtal - Instruktion, 2020
- Personuppgiftsbiträdesavtalets instruktioner, uppdaterade 2024-12-06.

Tester av systemet

- Cambios Statement of Applicability, version 1.0
- Cambios certifiering ISO/IEC 27001:2022 samt Statement of Applicability, version 2.0, november 2024

- Testrapport för Region Norrbotten leveransobjekt informationssäkerhet inom Framtidens VårdInformationsStöd (FVIS), januari 2024
- Strategi Flödestester v01, odaterad
- Strategi och plan för omtester – Verksamhetens tester v01, odaterad
- Strategi Verksamhetens tester v01, odaterad
- Testrapport Integrationstester BP5_V1.1, oktober 2024
- Testrapport Tekniska tester BP5_V1.2, oktober 2024
- Testrapport verksamhetens tester BP5_V1.1, oktober 2024
- Teststrategi – Integrationer och anslutningar produktionsmiljö v01, augusti 2024
- Teststrategi – Integrationer och anslutningar v01, odaterad
- Teststrategi flödestester i ACCv01, odaterad
- Teststrategi övergripande, odaterad

Planering för uppföljning

- Cambios certifiering ISO 27001:2013, januari 2024
- Cambios certifiering ISO 27001:2022, november 2024
- Certifiering MDR, september 2024
- CE-märkning enl MDR (MDR Declaration of Conformity)
- Utvecklingsplan kopplat till FVIS–plan, version 0.91, november 2024
- Cambio samarbete inom regulatorisk efterlevnad, maj 2024
- SUSSA vårdstöd Samverkanshandbok, juni 2022

Utbildningsplan för användare

- Rapport FVIS delprojekt utbildning, oktober 2024
- Regional utbildningsplan (odaterad)
- Cosmic Användarstöd, Utbildning av medarbetare, version 2.0
- Filmer: Jeanette och det Cosmiska - del 1-3 och Jeanette talar

Regler, rutiner och vägledning för det nya systemet

- Rapport Verksamhetens införande (oktober 2024)

Övrig dokumentation

- Presentationsmaterial inför beslut om driftsättning, FVIS inför BP6, november 2024
- Presentationsmaterial - Tidslinje, FVIS-projektet, odaterad