Region Jönköping

Rapport: Granskning av IT-säkerhet

Mars 2018

Oscar Rydén
Max Wann-Hansson

Building a better working world

Sammanfattande bedömning och rekommendationer

EY har på uppdrag av regionrevisionen genomfört en granskning syftande till att ge revisorerna underlag för att bedöma om IT-säkerheten inom kritiska områden i vårdinformationssystemet Cosmic, samt dess integration till rapportverktyget Diver hanteras på ett ändamålsenligt sätt.

Granskningen har fokuserats kring nedan fem revisionsfrågor:

- Finns kontroller avseende behörighetshantering i Cosmic som säkerställer att personal endast har åtkomst till funktioner lämpliga för dennes behov?
- Finns kontroller avseende programförändringar i Cosmic som säkerställer att inga förändringar som inte är ändamålsenliga för systemet implementeras?
- Finns kontroller och uppföljningsrutiner hos regionen som säkerställer att driften av Cosmic hanteras på ett säkert och ändamålsenligt sätt?
- Är informationssäkerhetsarbetet inom regionen ändamålsenligt i syfte att säkerställa patientsäkerhet i Cosmic?
- Säkerställer integrationen mellan Cosmic och Diver dataintegritet, dvs. sker hantering och överföring av data från Cosmic till Diver på ett sätt sådant att det är aktuell och korrekt data som presenteras i Diver?

Sammantaget bedömer vi att IT- och informationssäkerhetsarbetet inom kritiska områden i vårdinformationssystemet Cosmic, samt dess integration till rapportverktyget Diver i allt väsentligt är fungerande. Samtidigt har i granskningen iakttagelser inom granskade områden noterats. Dessa iakttagelser presenteras i kapitel 4 i rapporten tillsammans med tillhörande rekommendationer avsedda att stödja regionen i dess fortsatta arbete med IT- och informationssäkerhet.

Identifierade iakttagelser har klassificerats enligt tre risknivåer avseende hur omfattande dess eventuella inverkan på IT-säkerheten anses vara. De iakttagelser som anses medföra högre risk är att:

- Serveradministratörer har behörighet till samtliga servrar inom regionen
- Ingen kontroll av priviligierade användares loggar i Cosmic genomförs

IT-miljön i regionen möjliggör idag ingen begränsning av serverbehörigheter utifrån vilka servrar som är relevanta för en serveradministratörs arbetsuppgifter. Serveradministratörer har således tillgång till samtliga övriga servrar i regionen och inte enbart till de man har behov för. Regionen har ett pågående arbete med segmentera serveradministratörers behörigheter sådant att behörighet ska begränsas till relevanta servrar. EY ser detta som ett viktigt led i att stärka IT-säkerheten och rekommenderar regionen att säkerställa att segmenteringen realiseras inom snar framtid.

IT-personal i regionen innehar höga behörigheter i Cosmic i syfte att kunna utföra sina arbetsuppgifter. Dessa behörigheter är breda och gör att användaren har möjlighet att läsa eller ändra information i stora delar av systemet. Uppföljning av loggar för hur dessa behörigheter används genomförs vid misstanke om regelbrott, men ingen kontinuerlig uppföljning sker. EY bedömer att uppföljningen av dessa behörigheter kan stärkas, och rekommenderar regionen se över hur en manuell- eller automatisk kontroll av dessa användares aktiviteter kan implementeras.

1. Inledning

1.1 Bakgrund

Hantering av känslig data så som patientinformation ställer högra krav på IT-säkerhet inom Hälso- och sjukvården. Samtidigt blir man i takt med en accelererande digital utveckling i allt högre utsträckning beroende av informationssystem för att kunna bedriva verksamheten på ett effektivt sätt. Denna utveckling innebär med andra ord nya möjligheter men introducerar även nya risker. För effektiv leverans av Hälso- och sjukvård krävs ofta ett stort antal system, applikationer och komponenter som behöver vara integrerade med varandra. Dessa behöver även i många fall kunna användas externt av utomstående aktörer. Denna digitalisering medför även ytterligare utmaningar under 2018 i ljuset av EU:s nya dataskyddsförordning (GDPR) som träder i kraft 25 maj 2018, vilken får konsekvenser för hur verksamheter hanterar personuppgifter och information.

Utan ett väl fungerande och strukturerat IT- och informationssäkerhetsarbete finns risk för både avsiktliga och oavsiktliga störningar samt en risk att känslig information som rör enskilda personer kan läcka till obehöriga. Detta kan i sin tur leda till att Region Jönköpings trovärdighet och anseende skadas, vilket kan resultera i såväl monetära som icke-monetära förluster.

Ett centralt informationssystem för Region Jönköping är vårdadministrationssystemet Cosmic som används mycket brett i hela regionen, både inom primärvården och specialistvården. Ett ytterligare centralt system för verksamhetens fungerande och dess ledning är publiceringsverktyget Diver som används för uppföljning och analys av verksamhetsdata, ekonomi och personalinformation. Information och data i Cosmic ligger till grund för en stor del av den information som publiceras i Diver (statistik, tillgänglighet, besök, produktion, remisser, etc).

Mot bakgrund av förestående utmaningar inom IT- och informationssäkerhet och att revisorerna i sin riskanalys har identifierat Cosmic och Diver som kritiska för regionens verksamhet, har en granskning genomförts av hur systemens säkerhet och kvalitet säkerställs, inkluderande kontroller och rutiner kring Cosmic, hur kvaliteten i integrationen mellan Cosmic och Diver säkerställs, samt regionens arbete med IT- och informationssäkerhet för att upprätthålla patientsäkerhet.

1.2 Syfte

Granskningen syftar till att ge revisorerna underlag för att bedöma om IT-säkerheten inom kritiska områden i Cosmic, samt dess integration till Diver adresseras på ett ändamålsenligt sätt.

För att uppnå granskningens syfte besvaras följande delfrågor:

- Finns kontroller avseende behörighetshantering i Cosmic som säkerställer att personal endast har åtkomst till funktioner lämpliga för dennes behov?
- Finns kontroller avseende programförändringar i Cosmic som säkerställer att inga förändringar som inte är ändamålsenliga för systemet implementeras?
- Finns kontroller och uppföljningsrutiner hos regionen som säkerställer att driften av Cosmic hanteras på ett säkert och ändamålsenligt sätt?

- Är informationssäkerhetsarbetet inom regionen ändamålsenligt i syfte att säkerställa patientsäkerhet i Cosmic?
- Säkerställer integrationen mellan Cosmic och Diver dataintegritet, dvs. sker hantering och överföring av data från Cosmic till Diver på ett sätt sådant att det är aktuell och korrekt data som presenteras i Diver?

1.3 Genomförande

Granskningen baseras på dokumentgranskning samt intervjuer (se källförteckning). I förekommande har även stickprovsgranskning genomförts av relevanta kontroller inom ramen för granskningens revisionsfrågor. Samtliga intervjuande har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

1.4 Revisionskriterier

Med revisionskriterier avses bedömningsgrunder som används i förstudien för analyser, slutsatser och bedömningar. Revisionskriterierna kan hämtas ifrån lagar och förarbeten eller interna regelverk, policyer och fullmäktigebeslut. Kriterier kan också ha sin grund i jämförbar praxis eller erkänd teoribildning.

I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Regionens budget och verksamhetsplan 2017 och flerårsplan 2018-2019
- Myndigheten för samhällsskydd och beredskaps (MSB) ledningssystem för informationssäkerhet (LIS)

2. Styrning och förvaltning av IT inom regionen

2.1 Fullmäktiges målsättningar och uppdrag i budget 2017

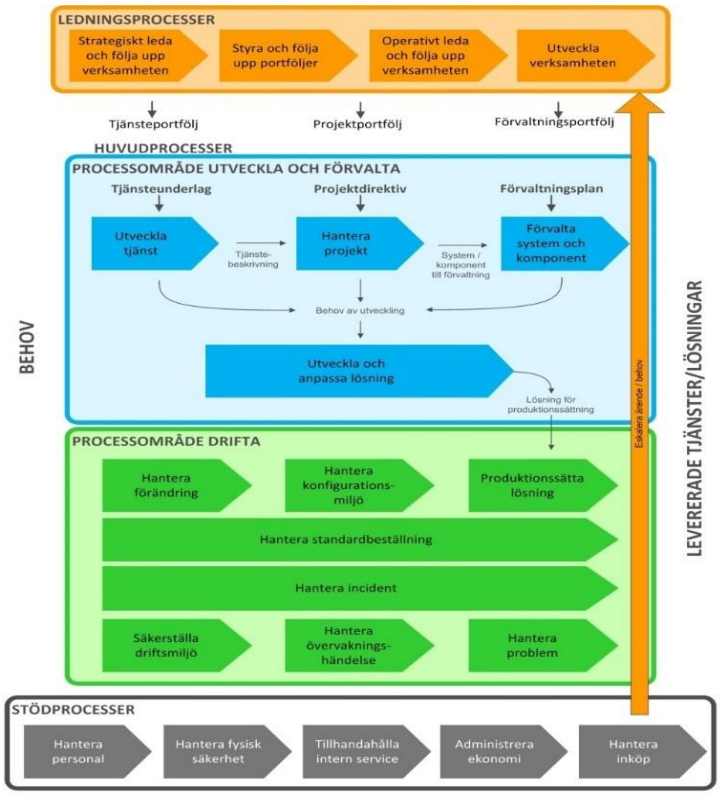
I enlighet med Regionens budget och verksamhetsplan 2017 och flerårsplan 2018-2019 ska den operativa verksamheten verka för kontinuerlig utveckling och förbättring av vårdens arbetssätt och genom nationell och regional samverkan kring standardiserat arbetssätt arbeta för en effektiviserad vård, ökad kvalitet och patientsäkerhet. Utgångspunkten är att rätt information ska finnas på plats i rätt tid vilket kräver kontinuerlig utveckling av vårdens IT-stöd, där vårdinformationssystemet Cosmic är en viktig del.

Regionens budget och verksamhetsplan 2017 beskriver även ett IT-stöd som möjliggör samverkan mellan vårdcentraler, kliniker och hemsjukvård som ett viktigt led i att möjliggöra en trygg och effektiv vårdsamordning som minskar återinläggningar och undvikbar sjukvård. Patienter som inte längre har behov av resurser i den slutna vården ska så snart som möjligt kunna lämna denna på ett tryggt sätt.

2.2 IT-centrum

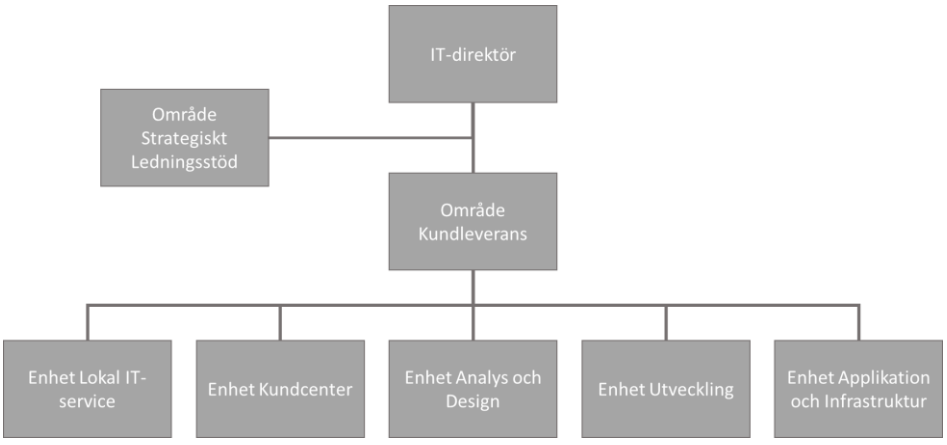
Leverans av IT inom Region Jönköping sker i huvudsak genom stödverksamheten IT-centrum, i samverkan med verksamheterna och systemförvaltningsorganisation för respektive system (Se vidare under avsnitt *2.4 – Systemförvaltningsmodell* nedan). IT-centrum har samlat ansvar för IT-stöd för hela regionens verksamhet inom både Folkhälsa och Sjukvård och Regional Utveckling. Detta är således ett mycket brett uppdrag med ett stort antal system och tjänster. Viss IT, framför allt inom Regional Utveckling, hanteras lokalt men den långsiktiga målsättningen är att all drift och förvaltning av IT inom regionen ska ligga hos IT-centrum.

IT-centrum arbetar processinriktat enligt en styrmodell kallad Vägvisaren, se nedan illustration i figur 1. Organisationens ingående områden och enheter är utformade för att kunna tillhandahålla tjänster och lösningar enligt denna modell.



Figur 1 - Styrmodell IT-centrum

IT-centrum har idag cirka 175 medarbetare. Organisationen leds av IT-direktören och är indelad i två områden. Figur 2 visar hur organisationen är uppdelad i två områden. Det ena området är ”Strategiskt ledningsstöd” som arbetar med strategisk ledning och styrning av IT-centrums verksamhet och det andra huvudområdet är ”Kundleverans” som ansvarar för leveransen av IT.



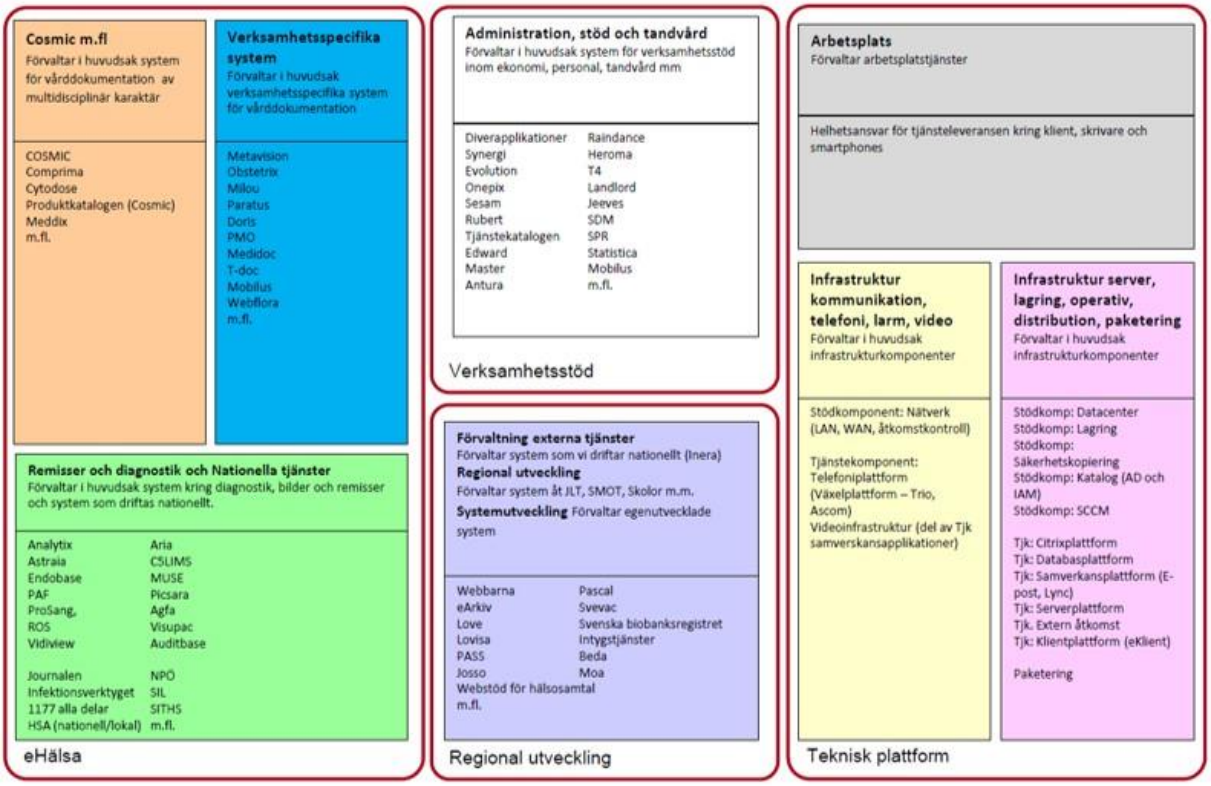
Figur 2 - Organisationskarta IT-centrum

- Enhet Lokal IT-service – Har kontakt med kunder på plats för att kunna utföra support, felsökning, och installationer som kräver fysisk närvaro.
- Enhet Kundcenter – Har kontakt med kunder via Kundcenter och ansvarar för support, fånga upp och hantera incidenter, samt viss övervakning av IT-miljön.

- Enhet Analys och Design – Leder, analyserar, och kvalitetssäkrar verksamhetens IT-lösningar.
- Enhet Utveckling – Ansvarar för nyutveckling och vidareutveckling av system och IT-tjänster.
- Enhet Applikation och infrastruktur – Hanterar den tekniska infrastrukturen inom IT-miljön.

Majoriteten av IT-centrums personal är placerade i IT-centrums lokaler i Huskvarna. Utöver detta finns ett 30-tal medarbetare inom Enhet Lokal IT-service som är placerade på de tre akutsjukhusen i Jönköping, Eksjö, och Värnamo.

För den praktiska förvaltningen av systemen, tjänster, och komponenter är IT-centrum organiserade i åtta förvaltningsgrupper, se figur 3 nedan. Varje förvaltningsgrupp ansvarar för förvaltning av en samling system inom en viss kategori. Inom var och en finns medarbetare från verksamhetens olika enheter beskrivna i syfte att samla kompetens nödvändig för förvaltningen och motverka att verksamhetens enheter arbetar i silos. De förvaltningsgrupper som är mest intressanta inom ramen för denna granskning är förvaltningsgruppen ”Cosmic m.fl”, förvaltningsgruppen ”Administration, stöd och tandvård” som förvaltar Diver, samt förvaltningsgruppen ”Infrastruktur server, lagring, operativ, distribution, paketering” som förvaltar servrar och databaser för både Diver och Cosmic.



Figur 3 - Förvaltningsgrupper IT-centrum

2.3 Vårdinformationssystemet Cosmic

Vårdinformationssystemet Cambio Cosmic (fortsatt Cosmic) har varit i bruk inom Region Jönköping sedan 2008 och används idag av cirka 10000 användare. Systemet är byggt

på en central plattform med en rad olika tillhörande moduler för att kunna stödja all typ av hälso- och sjukvård. Region Jönköping har sedan införandet haft som strategi att Cosmic ska användas gemensamt i hela regionen för att skapa förutsättningar för god och säker vård. Det ska vara ett vårdinformationssystem som stödjer hela patientprocessen och skapar förutsättningar för att ge rätt vård till rätt patient vid rätt tillfälle, med rätt information som underlag. Med en tydlig struktur, standard och systematik i systemet ska förutsättningar ges för likvärdig patientadministration samt underlättad teknisk administration. Verksamheten använder idag de flesta tillgängliga moduler i Cosmic, både inom primärvården och specialistvården.

Cosmic är utvecklat och levereras av Cambio Healthcare Systems (fortsatt Cambio). I Sverige använder sig sju landsting och regioner förutom Jönköping av systemet: Region Jämtland Härjedalen, Region Östergötland, Region Kronoberg, Landstinget i Värmland, Landstinget i Västmanland, Landstinget i Kalmar Län, och Uppsala Läns Landsting. Samtliga dessa använder likt Jönköping systemet inom både primärvården och specialistvården. Dessa åtta vårdgivare, tillsammans med en privat aktör i Capio AB, har gått samman i ”Kundgrupp Cosmic”. Kundgruppen träffas regelbundet i syfte att samverka kring förvaltning och utveckling av systemet, och skapa en enhetlig kravställning gentemot Cambio inför kommande versionsuppgraderingar.

Trots den samverkan som sker i kundgrupperna ser versionerna för de olika landstingen väldigt olika ut. Cosmic präglas av en hög grad av konfigurerbarhet för att kunna anpassa systemet efter verksamhetens behov, och det är även integrerat med andra mindre system. Versionsuppgraderingar av systemet är därför mycket tidskrävande och involverar både systemspecialister inom IT-centrum, konsulter från Cambio, samt systemförvaltare och modulansvariga inom Folkhälsa och sjukvård som analyserar och beslutar om lämplig konfigurering samt ansvarar för utbildning och informationsinsatser mot verksamheten.

Den senaste versionsuppgraderingen infördes i oktober 2017 då man gick upp i Cosmic 8.1. Inom Sydöstra sjukvårdsregionen (Region Jönköping, Region Östergötland, och Landstinget i Kalmar Län) finns en fördjupad samverkan kring standardiserat användande utifrån ett IT-perspektiv. Denna samverkan syftar till att utreda i vilken mån landstingens verksamhetsprocesser kan harmoniseras och på så sätt skapa en mer enhetlig kravställning gentemot Cambio samt skapa skalfördelar vid införande av versionsuppgraderingar.

Som nämnt ovan är Cosmic uppbyggd med en central plattform med tillhörande moduler och komponenter som kan kopplas på beroende på verksamhetens behov. En viktig komponent inom ramen för denna granskning är Cosmic Intelligence (CI) som är ett informationslager varifrån användare kan hantera, beskriva, och presentera information från samtliga moduler i Cosmic. CI innehåller samma information som Cosmic men är utvecklad för att tillhandahålla översiktlig information och användas för analys, rapportering, och uppföljning. Från CI överförs sedan data som presenteras i presentationsverktyget Diver.

2.4 Diver

Diver är ett verktyg för planering, kontroll, analys och uppföljning med syfte att tillhandahålla beslutsunderlag för styrning av verksamheten. Systemet är ett publiceringsverktyg för verksamhetsdata, ekonomidata, och personalinformation och är

därför centralt för Region Jönköpings fungerande på ledningsnivå. Inom ramen för denna granskning innefattas data i Diver som härrör från Cosmic. Diver är dock integrerat med tiotalet ytterligare system som föder data även inom områdena Tandvård, Läkemedel, Personal, och Ekonomi för att kunna ge verksamhetsövergripande information. Inom Region Jönköping finns ett så kallat ”Diverråd” som utöver systemförvaltningen innehåller representanter från samtliga system som föder data till systemet. Syftet med detta forum är att fånga upp respektive systems krav och önskemål kring systemet för att kunna besluta om och prioritera utveckling.

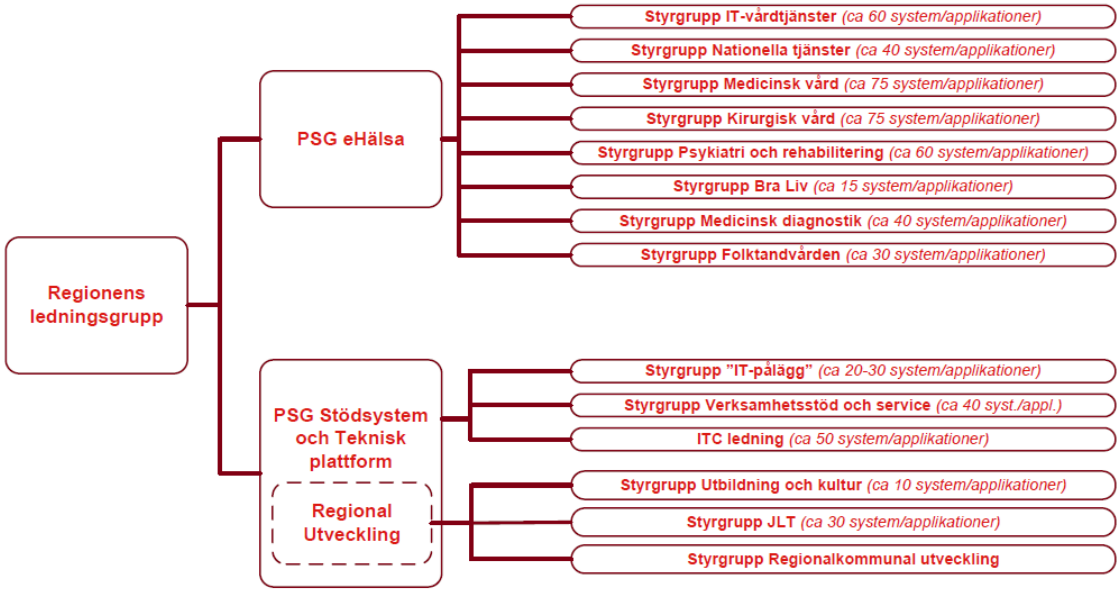
Systemleverantör av Diver är företaget Infotool. De är dock i ytterst liten utsträckning involverade i förvaltning och vidareutveckling av systemet. Detta ansvar ligger primärt hos förvaltningsgruppen för Administration, stöd och tandvård inom IT-centrum som utför fortlöpande vidareutveckling och nyutveckling av rapporter som kan publicera information som efterfrågas av verksamheten.

2.5 Systemförvaltningsmodell

Region Jönköpings ramverk för systemförvaltning har sin grund i förvaltnings- och portföljstyrningsmodellen pm3 som används av i stort samtliga landsting i Sverige. Modellen har dock i viss mån justerats av regionen med en ambition att fokusera på utveckling av processer och verksamhetsflöden i första hand, samt värdera hur IT-stöd och digitala lösningar kan användas optimalt kopplat till verksamhetsprocessernas behov.

Den övergripande strukturen för regionens systemförvaltningsmodell illustreras i figur 4 nedan. I de två så kallade programstyrgrupperna sitter berörda representanter från regionens ledningsgrupp med ansvar för övergripande samordning och prioritering för de underliggande styrgrupperna, strategisk utblick och styrning, samt att frågor som berör hela regionen lyfts till regionens ledningsgrupp.

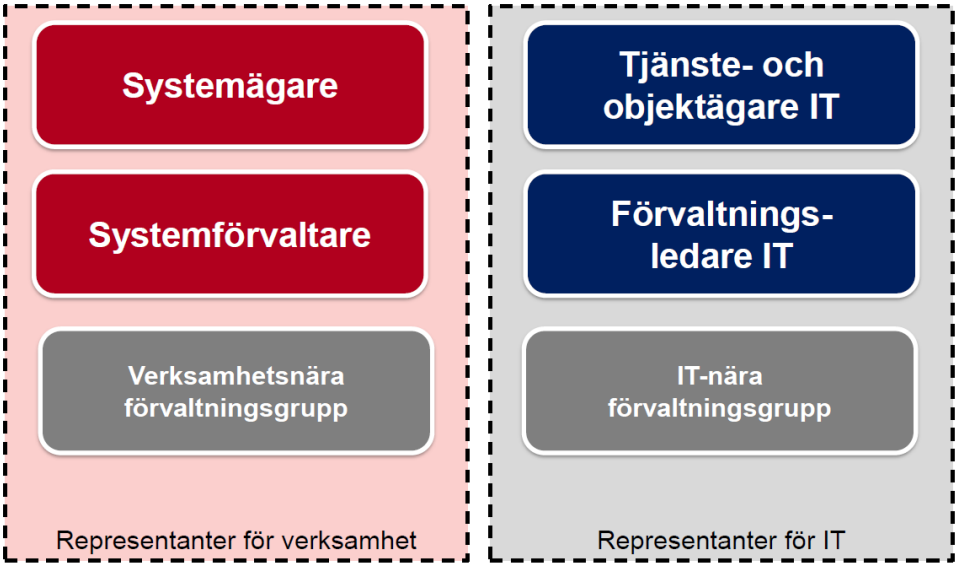
Under de två programstyrgrupperna finns så kallade styrgrupper indelat per verksamhetsområde med ansvar för relaterade system och applikationer.



Figur 4 – Systemförvaltningsmodell

Styrgrupperna får sitt uppdrag från och rapporterar till respektive programstyrgrupp. Styrgruppen har budgetansvar för de system som ligger inom styrgruppens område och har mandat att prioritera och agera inom ramen för tilldelad budget. På årsbasis ska styrgruppen utforma förvaltningsplaner som rapporteras till programstyrgruppen och beskriver de initiativ man anser nödvändiga inför kommande verksamhetsår. Styrgruppen har också ett ansvar att säkerställa att nyttor och effekter av beslutade utvecklingsinitiativ kan realiseras i verksamheten. Beroende på omfattningen av styrgruppens ansvar sker deras sammanträden med olika frekvens. Styrgruppen IT-vårdtjänster som ansvarar för, bland annat, förvaltningen av Cosmic har veckovisa sammanträden då de har ett brett ansvar och många frågor att gå igenom.

Styrgruppens sammansättning för verksamheten beslutas av ansvarig direktör. Därutöver utser regionledningskontoret och IT-centrum representation på ledningsnivå från sina respektive verksamheter. För de viktigaste systemen utses specifika roller och ansvar enligt figur 5 nedan.



Figur 5 - Roller och ansvar i förvaltningsgrupp

- Systemägare – Har det yttersta ansvaret för systemet och fattar övergripande beslut för systemet under dess livscykel. Som huvudregel är ansvarig direktör systemägare för samtliga system som direktörens styrgrupp ansvarar för, men systemägarskapet kan även delegeras till medarbetare som är underställda direktören.
- Systemförvaltare – Tillsätts av systemägare. Systemförvaltaren är operativt ansvarig för systemet (tillsammans med förvaltningsledare IT) utifrån beslut från systemägaren, samt utifrån fastställd systemförvaltningsplan. Systemförvaltaren ansvarar för att verksamhetens behov och önskemål tillgodoses genom att, till exempel, planera och genomdriva förändringar, samordna utvecklingsinsatser för systemet, samt ansvara för information och utbildning till användare i verksamheten.
- Tjänste- och objektägare IT – Har övergripande ansvar för IT-delen och arbetar strategiskt med utveckling, förvaltning, och leverans av IT för att säkerställa att den möter verksamhetens behov på ett effektivt sätt. Tillsammans med systemägare arbetar tjänste- och objektägare IT för att skapa en enhetlig strategi på lång sikt avseende utveckling och förvaltning av systemet.

- Förvaltningsledare IT - Är ansvarig på taktisk och operativ nivå för utveckling, förvaltning, och leverans av IT utefter fastställd budget och strategisk riktning kommunicerad från tjänste- och objektägare IT. Förvaltningsledare IT ansvarar för att rätt kapacitet och kompetens finns i förvaltningsgruppen för att kunna säkerställa korrekt leverans.

3. Beskrivning av granskade områden

3.1 Behörighetshantering i Cosmic

Beträffande IT- och informationssäkerhet är det av yttersta vikt att behörigheter i informationssystem är lämpligt definierade, det vill säga att rätt personer har rätt tillgång vid rätt tidpunkt, med rätt anledning. Antalet Cosmic-användare i regionen är mycket högt vilket gör behörighetshanteringen komplex och ökar risken för att kritisk information går förlorad eller sprids till obehöriga. En hög grad av den information som behandlas i Cosmic omfattas av patientdatalagen varvid det föreligger höga krav på att känslig information så behandlas med integritet och tillförlitlighet.

Granskningen har fokuserats kring kontroller och rutiner relaterat till:

- Autentisering och säkerhetsinställningar
- Tillägg av ny behörighet
- Förändring av befintlig behörighet
- Borttag av behörighet
- Periodisk genomgång av befintliga behörigheter
- Hantering av priviligierade behörigheter

Autentisering och säkerhetsinställningar

Enligt framtagna riktlinjer gällande lösenord i regionens informationssäkerhetspolicy ska lösenordsinställningar i verksamhetens informationssystem (på ett minimum):

- Bestå av minst 8 tecken
- Innefatta komplexitet med en kombination av siffror, bokstäver och specialtecken
- Bytas var 90:e dag
- Systemadministratörer ska ha utökat lösenordskrav på minst 10 tecken.

I granskningen har faktiska lösenordsinställningar i Cosmic efterfrågats, och det har kunnat säkerställas att de inställningar som är definierade överensstämmer med regionens informationssäkerhetspolicy.

Tillägg och förändring av behörigheter

Vid beställning av ny behörighet i Cosmic ligger HSA-katalogen till grund för användarregistrets uppgifter. HSA är en elektronisk nationell katalog som innehåller kvalitetsgranskade uppgifter om personer och verksamheter inom svensk vård och omsorg. Vid nyanställning registreras man per automatik i HSA-katalogen genom att man läggs upp som anställd i Heroma, regionens HR- och lönesystem. Endast personer som finns upplagda i HSA-katalogen kan bli registrerade som användare i Cosmic eftersom det användar-ID som generas i HSA ligger till grund för det användar-ID som används för att tilldela användaren behörighet i Cosmic. För att övriga personer (icke-anställda, till exempel konsulter eller studenter) ska kunna läggas upp i Cosmic behöver en lokal HSA-administratör i verksamheten manuellt skapa en post i HSA-katalogen som sedan kan användas för att generera ett användar-ID i Cosmic.

En ansvarig kontaktperson inom varje enhet utses för att ansvara för enhetens användarlista. Användarlistan ska dokumenteras enligt en framtagen standardiserad blankett kallad ID34. Denna ska innehålla samtliga anställda med Cosmic-behörighet

inom enheten och vad de har för användarroll. Kontaktpersonen, eventuellt tillsammans med ytterligare ansvariga inom enheten, utför även beställning av ny behörighet eller förändring av befintlig behörighet i Cosmic. Denna beställning görs i tjänstekatalogen på intranätet. Tjänstekatalogen är konfigurerad sådant att enbart behöriga personer har möjlighet att utföra en beställning. Med beställningen ska alltid aktuell rad i ID34 bifogas.

Tjänstekatalogen är integrerad med ärendehanteringssystemet SDM. Kundcenter på IT-centrum tar emot beställningen och kontrollerar att beställningen är korrekt utförd och att ID34 är bifogad, om inte returneras ärendet till beställaren. Kundcenter kontrollerar även användarnamn och övriga uppgifter mot HSA-katalogen och utför sedan upplägg eller förändring av behörigheten efter beställningen.

Behörigheter i Cosmic är rollbaserade, med extra behörigheter som kan läggas till för specifika personer efter behov. Användarrollerna styr vilka funktioner användaren kan utföra, och för vilka enheter. Avseende möjlighet att läsa information har samtliga användare i Cosmic i grunden full läsrätt, vilket innebär att man kan läsa information inom hela regionen och för alla dess patienter. Utgångspunkten är dock att man har tillgång till information inom sin enhet och för de patienter man ansvarar för. För att få tillgång till annan information krävs aktiva val från användaren. All åtkomst loggas i systemet varvid det finns möjlighet att i efterhand kontrollera vilken information användare har ändrat eller tittat på. För patienter med journalspärr kommer det också alltid upp en notis i systemet och för att komma vidare måste man bekräfta att man fått godkännande från patienten. Sådana ”överträdelser” av journalspärrar loggas och kan således följas upp i efterhand.

Borttag av behörigheter

Förfarandet för borttag av behörighet i Cosmic när en resurs avslutar sin anställning är i stort detsamma som för tillägg av ny behörighet. Denna process innefattar dock två olika typer av borttag. Dels tas resursens behörighet till Cosmic bort, det vill säga möjligheten att komma åt systemet, och dels inaktiveras användaren i Cosmic vilket innebär att det inte längre är möjligt att planera vårdåtgärder för resursen.

Det första steget är att göra en beställning för borttag av resursens behörighet. Denna beställning görs av enhetens kontaktperson med bifogat utdrag ur ID34, likt vid upplägg av nya behörigheter beskrivet ovan. Användarens behörighet till enheten som har beställt borttaget tas därefter bort av kundcenter på IT-centrum. Verksamheten ansvarar sedan för att genomföra kontrollpunkter enligt definierad checklista för borttag av resurs. Dessa innefattar kontroller för att säkerställa att samtliga besök, aktiviteter, åtgärder, osv. som finns planerade för resursen hanteras och planeras om. Detta är ett viktigt led i processen avseende patientsäkerheten. När dessa kontrollpunkter är genomförda lägger kontaktpersonen en ny beställning i tjänstekatalogen för inaktivering av resursen i Cosmic. I denna beställning bifogas en blankett där det intygas att samtliga åtgärder i checklistan har tagits. Användaren inaktiveras och finns inte längre som tillgänglig resurs för den enhet som har beställt borttag. Om det är den sista enheten som beställer borttag inaktiveras resursen helt i Cosmic och det går inte att planera in vårdåtgärder för resursen på någon enhet.

Regionen har en ekonomimodell som gör att varje enhet betalar för varje användare i Cosmic. Detta medför incitament för verksamheten att ta bort användare som inte är i behov av behörighet. Trots detta incitament är det inte ovanligt att verksamheterna är

långsamma på att beställa borttag av användare (se iakttagelse 1.1 i avsnitt 4). Det finns heller inga riktlinjer eller tidsreferenser för när borttag av användare ska göras.

Periodisk genomgång

En genomgång av behörigheter görs 3 gånger per år genom att IT-centrum skickar ut listor på aktiva HSA-användare till respektive verksamhet för granskning. Ansvarig person i verksamheten ska i denna gå igenom listan för att kontrollera att det inte finns kvar några anställda som har avslutat sin anställning i HSA-katalogen. Denna genomgång inkluderar dock inte en genomgång av behörigheter i Cosmic (se iakttagelse 1.2 i avsnitt 4). Det finns heller ingen koppling mellan HSA-katalogen och Cosmic som gör att användare avslutas per automatik om de tas bort i HSA-katalogen.

En rutin finns för att granska loggar i Cosmic regelbundet i syfte att säkerställa att användare inte utnyttjar möjligheten till full läsrätt i systemet för andra syften än de tjänsten kräver. Enligt rutinen ska verksamhetschefen granska loggar för två anställda varje månad och därefter fylla i ett dokument för spårbarhet i att granskningen har utförts. I dokumentet anges vilka loggar man har tittat på och om några avvikelser har identifierats. Verksamhetschefen signerar sedan dokumentet och skickar in det till IT-centrum per brev. Automatisk kontroll av loggarna i Cosmic finns inte (se iakttagelse 1.3 i avsnitt 4). Det finns för närvarande ett initiativ för att automatisera kontrollen av loggarna genom en lösning kallad Loggpoint. Tanken är att systemet ska identifiera utmärkande beteenden avseende vilka patienter och data användaren tittar på och på så vis upptäcka obehörig åtkomst till patientdata.

Priviligierade användare

Priviligierade användare definieras i denna granskning som användare med tillgång till infrastrukturkomponenter (server och databas) samt användare med utökad läs- och ändringsrätt i Cosmic.

Behörigheter till server och databas tilldelas främst systemtekniker vid IT-centrum med ett direkt behov av denna behörighet för att kunna utföra hans eller hennes arbetsuppgifter. Upplägg av dessa behörigheter ska beställas av användarens chef via tjänstekatalogen. Beställningen går sedan till förvaltningsgruppen för Infrastruktur server, lagring, operativ, distribution, paketering som beslutar om tilldelning av denna behörighet är lämplig.

Om man är serveradministratör är man det i dagsläget för samtliga servrar inom regionen och inte enbart de servrar som är relevanta för den anställdes arbetsuppgifter (se iakttagelse 1.4 i avsnitt 4). Det finns ett pågående arbete med att segmentera behörigheter så att man t.ex. som systemtekniker för Cosmic endast har tillgång till de applikationsservrar Cosmic driftas på. Samma sak gäller dock inte för behörigheter till databaser, för dessa har användare enbart tillgång till de databaser den anställdes arbetsuppgifter kräver.

Anställda från systemleverantören Cambio har behörighet till servrar och databas i syfte att kunna bistå med support och felsökning i Cosmic. Beställning av dessa behörigheter initieras av Cambio men följer i övrigt samma process som för interna behörigheter där godkännande sker av förvaltningsgruppen för Infrastruktur server, lagring, operativ, distribution, paketering. Även för Cambios behörigheter gäller att serveradministratörer har denna behörighet för samtliga servrar (se iakttagelse 1.4 i avsnitt 4).

Inom IT-centrum finns ett antal kategorier användare som innehar högre behörighet i Cosmic. Detta innefattar bland annat applikationsspecialister, kundservice, systemtekniker, systemutvecklare, och systemadministratörer, samt tre supportresurser från Cambio. Dessa är breda behörigheter som gör att användaren kommer åt i stort sett allt i applikationen. Dessa behörigheter beställs av förvaltningsledare IT utifrån den anställdes uppdrag och läggs upp av kundservice. Även ett fåtal användare i verksamheten har högre behörighet, men dessa är mer begränsade.

Då och då genomförs rensningar av höga behörigheter för servrar, databaser, och i applikationen. Det finns dock ingen etablerad process för att detta ska utföras regelbundet (se iakttagelse 1.5 i avsnitt 4). En kompenserande åtgärd är dock att användarens Active Directory-konto inaktiveras automatiskt då en anställd avslutas i HR-systemet Heroma, och för externa användare (konsulter) finns alltid ett definierat slutdatum som inaktiverar kontot vid avslutande av dennes uppdrag. Det sker heller ingen periodisk genomgång av behörigheter som innehas av support från Cambio (se iakttagelse 1.5 i avsnitt 4).

Granskning av loggar för priviligierade behörigheter i Cosmic genomförs vid misstanke om regelbrott. En liknande regelbunden stickprovskontroll som utförs för användare i verksamheten genomförs dock inte för priviligierade användare i applikationen (se iakttagelse 1.6 i avsnitt 4).

3.2 Utvecklings- och förändringsarbete i Cosmic

Förändringar och utveckling är en kritisk del i en verksamhetens hantering av informationssystem. För att applikationer och system ska kunna möta verksamhetens mål avseende funktionalitet, tillgänglighet, och integritet behöver kontinuerliga uppdateringar eller rättningar göras. I dessa fall är det viktigt att ha ett väl fungerande utvecklings- och förändringsarbete för att kritisk information inte ska gå förlorad och för att systemförändringar inte medför oönskad funktionalitet eller driftstopp.

Granskningen har fokuserats kring kontroller och rutiner relaterat till:

- Initiering och godkännande av programförändringar
- Testning och övervakning av programförändringar
- Implementation av programförändringar

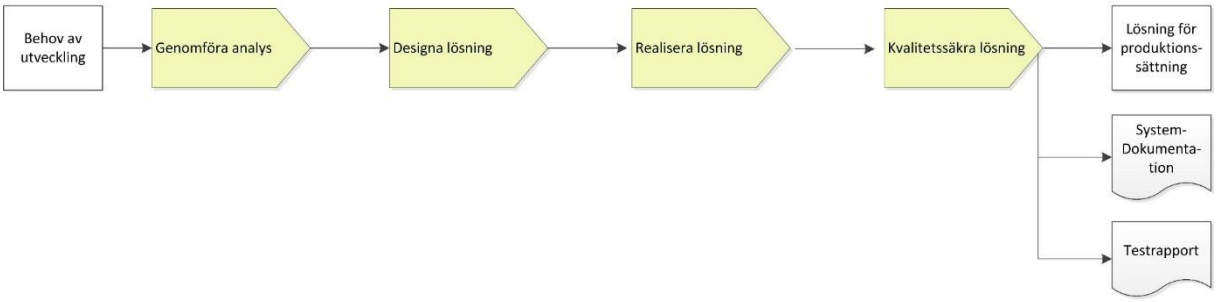
En viktig förutsättning för utvecklings- och förändringsarbete i Cosmic är kundgrupp Cosmic vilken Region Jönköping är del av tillsammans med 8 regioner och landsting samt en privat aktör i Capio AB. Tanken är att i detta forum skapa en enhetlig kravställning gentemot systemleverantören Cambio och arbeta för en standardiserad produkt som tillfredsställer behoven hos samtliga aktörer i kundgruppen. Kundgruppen tar gemensamt fram en utvecklingsplan som ligger till grund för Cambios produktplaner inför kommande releaser. Alla beslut som rör utveckling tas därför gemensamt i kundgruppen i dialog med Cambio.

Region Jönköping har definierat fyra olika typer av förändringar som till större del baseras på förändringens storlek:

- Versionsuppgraderingar
- Feature packs
- Serivce packs

- Hot fixes

Oavsett vilken typ av förändring det är, följer alla nya uppdateringar samma övergripande förändringsprocess. Det som skiljer dem åt i processen är insatsen och hur genomgående varje del genomförs. Förändringsprocessen är indelad i två delar, en del för att utveckla och anpassa lösningen som visas nedan i figur 6 och en del för implementation.



Figur 6 - Process "Utveckla och anpassa lösning"

Godkännande av förändringar

För större uppgraderingar som berör hela Cosmics kundgrupp, beslutas all utveckling gemensamt av alla objektägare och CIOs i kundgruppen. Efter godkännande från kundgrupp är det Cambio som ansvarar för utvecklingen. I avtalet med Cambio framgår det vilka kvalitetssäkringsaktiviteter som Cambio måste genomföra vid ny utveckling.

När ett behov av utveckling som är specifikt för Region Jönköping har identifierats genomförs först ett antal analyser så som riskanalys och verksamhetsanalys. Utifrån analyser av verksamhetens behov skapas ett underlag som ligger till grund för de aktiviteter som ska anpassa produkten till verksamhetens behov och krav.

Testning av förändringar

För de uppgraderingar som är gemensamma för hela Cosmics kundgrupp skapas en referensgrupp som består av personer från alla eller utvalda kunder. En acceptanskontrollör (en av kunderna) utses gemensamt av kundgruppen och ansvarar för mottagande och acceptanstestning av utvecklingen. Det finns inget standardiserat testningsprotokoll som är gemensamt för hela kundgruppen. Däremot återkopplas all testning som acceptanskontrollören genomfört till kundgruppen och alla kunder kan framföra sina testningsbehov.

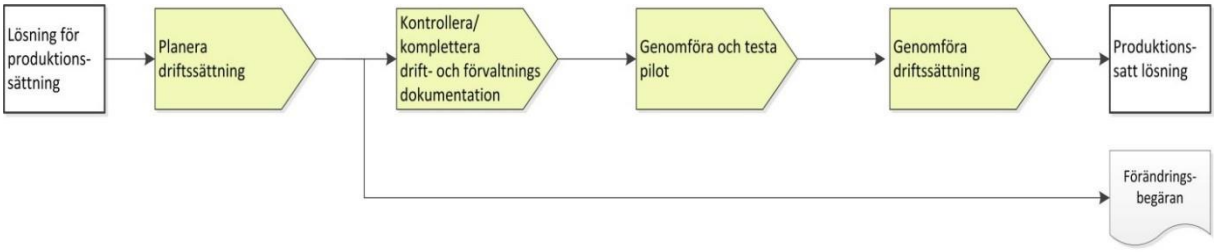
För Region Jönköpings egna specifika utvecklingsprojekt testas först en installation i en testmiljö för att säkerställa att den går att installera och att produkten är korrekt. En övergripande funktionskontroll genomförs också i testmiljön innan man går vidare. Nästa steg är att installera produkten i två produktionstestmiljöer, QA Test och QA Integration. I QA Integration säkerställer man att kopplingen mellan Cosmic och övriga system fungerar och i QA Test säkerställer man att Cosmic fungerar i enlighet med funktionella krav. Resurser för verksamheten är delaktiga i testningen för att säkerställa att produkten möter verksamhetens behov och krav. Efter testningen skapas en testrapport som innehåller utfall av testerna, testresultat, erfarenheter och defekter med handlingsplan.

All testning dokumenteras och lagras i ett program som heter ReQtest medan felhantering för identifierade avvikelser hanteras av Cambio och rapporteras i deras ärendehanteringssystem Jira.

Implementation av förändringar

Vid implementation av uppgraderingar som är gemensamma för hela kundgruppen är det acceptanskontrollören som först produktionssätter dessa. Övriga aktörer i kundgruppen avvaktar till acceptanskunden har implementerat förändringen.

När Region Jönköping ska implementera en lösning eller en produkt följer det alltid den hantering och process för implementation som illustreras i figur 7 nedan. För att inte påverka verksamheten i för stor omfattning har regionen två definierade servicefönster per år, ett på våren och ett på hösten, när förändringar får implementeras.



Figur 7 - Process "Implementation av lösning"

Vid implementation utformar en leveransansvarig inom berört projekt eller förvaltningsgrupp en driftsättningsplan. Leveransansvarig skickar också en förändringsbegäran i ärendehanteringssystemet SDM till driftchef som alltid ska godkänna alla förändringar innan driftsättning. Innan förändringsbegäran är godkänd genomförs tester av återställningsmöjligheter och acceptanskriterier inför implementation. När dessa tester är klara och förändringsbegäran är godkänd implementeras förändringen enligt driftsättningsplanen.

Vid kritiska eller akuta förändringar går utveckling- och förändringshanteringsprocessen till på samma sätt som för övriga förändringar fast i en snabbare takt. Denna typ av förändringar kan även implementeras utanför de två definierade servicefönstren, vilket det i dessa fall är systemägare och styrgrupp som beslutar om.

Förändringsledning

En stor del av arbetet vid införande av förändringar är förändringsledning i syfte att realisera och införliva lösningen i verksamheten. I detta görs en översyn som involverar verksamhetsanalys, processkartläggning, framtagande av övergripande riktlinjer, samt underlag för konfigurering. Efter leverans av lösningen från IT-centrum samordnas utbildnings- och informationsinsatser till verksamheten av Folkhälsa och sjukvård som driver förändringen i samverkan med utsedda superanvändare i verksamheten. Det är superanvändarna som leder det dagliga implementerings- och förändringsarbetet i verksamheten för att förankra lösningen.

På ett minimum fyra gånger per år genomförs kontaktpersonsnätverksträffar inom regionens tre länsdelar. Där förmedlas och inhämtas information som ska säkerställa ett

korrekt användande av Cosmic. Även inom användargruppen för Cosmic anordnas regelbundna träffar för avstämning kring aktuella frågor kopplade till vårdens behov.

3.3 IT-drift för Cosmic

Rutiner och kontroller inom IT-drift är av stor vikt i syfte att säkerställa en IT-miljö som tillgodoser verksamhetens behov avseende säkerhet och tillgänglighet. För Cosmic föreligger höga krav på en tillförlitlig IT-drift för effektiv leverans av vårdtjänster och patientsäkerhet i vården.

Granskningen har fokuserats kring kontroller och rutiner relaterat till:

- Hantering av incidenter relaterade till Cosmic
- Säkerhetskopiering (Backuphantering) och återläsning av information i Cosmic
- Övervakning av schemalagda jobb till och från Cosmic
- Övervakning av driftmiljön

Hantering av incidenter relaterade till Cosmic

Ärendehanteringssystemet Service Desk Manager (SDM) används av regionen som verktyg för registrering och hantering av incidenter. Primärt ansvar för processen för hantering av incidenter ligger hos enhet Kundcenter inom IT-centrum. Incidenter kommer in via tre vägar:

- En användare ringer eller mailar till first line support hos Kundcenter som registrerar ärendet i SDM utifrån användarens uppgifter.
- En användare registrerar en incident i tjänstekatalogen på intranätet. First line support hos Kundcenter mottar incidenten och registrerar i SDM.
- Incident genereras inom processen för övervakning och registreras i SDM av ansvarig person för övervakningen.

Kundcenter är ansvariga för att värdera incidenten och förbereda åtgärd. Incidenten värderas genom att prioritet sätts utifrån dess omfattning samt påverkan. Om first line support själva kan hantera en inkommen incident gör de detta direkt, om inte tilldelas den second line-support eller respektive förvaltningsgrupp för att genomföra utredning och felsökning. Vid större incidenter med stor påverkan kopplas även incident manager in för att leda arbetet med incidenten. Ansvarig person för incidenten genomför lämpliga åtgärder för att hantera incidenten, vid behov kan även en förfrågan om förändring initieras. När incidenten är åtgärdad, det vill säga när användaren inte längre bedöms vara påverkad, skall ansvarig person markera den som ”Åtgärdad” i SDM. Användaren som rapporterade incidenten informeras då och har 7 dagar på sig att återkoppla om han eller hon fortfarande inte anser den vara åtgärdad. Om ingen återkoppling sker inom 7 dagar bedöms incidenten vara avslutad. Vid större incidenter som haft mycket stor påverkan på verksamheten initieras en så kallad ”Händelseanalys” för att utreda grundorsaker och nödvändiga åtgärder.

Säkerhetskopiering och återläsning av information i Cosmic

För schemaläggning och hantering av säkerhetskopiering använder sig Region Jönköping av IBM’s lösning för programvarudefinierad lagring *IBM Spectrum Storage.* Full säkerhetskopiering av information i Cosmic sker dagligen under natten. I dessa tas en komplett kopia på databasen som sedan sparas på disk. Under dagen tas även backuper på databasens transaktionsloggar varje kvart. Detta är loggar som sparar alla

händelser (det vill säga alla förändringar som sker) i databasen, vilket i praktiken innebär att maximalt 15 minuters information går förlorad vid händelse av ett avbrott i Cosmic.

Det tekniska ansvaret för säkerhetskopieringen, det vill säga att se till att den fungerar, ligger hos förvaltningsgruppen för Infrastruktur server, lagring, operativ, distribution, paketering inom IT-centrum. Den kontinuerliga övervakningen, det vill säga att kontrollera att säkerhetskopior tas enligt planen, ligger hos enhet Kundcenter. *IBM Spectrum Storage* är konfigurerat så att automatiska mail skickas till en gemensam mailbox om en backup inte har genomförts, eller inte har kunnat tas som planerat. Enligt ett rullande schema har 2nd line på Kundservice har kontinuerlig monitorering av denna mailbox. Om en backup inte har kunnat genomföras körs den om på nytt. Vid eventuella kvarvarande fel registreras en incident i SDM för hantering av förvaltningsgruppen för Infrastruktur server, lagring, operativ, distribution, paketering.

Återläsning från säkerhetskopior genomförs en gång i veckan på fredagseftermiddagar. Däremot genomförs inga regelbundna dokumenterade återläsningstester (se iakttagelse 2.1 i avsnitt 4). Den återläsning som görs sker till Cosmics så kallade elevmiljö, vilket är en utbildningsmiljö där nyanställda kan läras upp utan att påverka information och funktionalitet i produktionsmiljön. Elevmiljön är en direkt kopia av produktionsmiljön med skillnaden att patientdata är exkluderad. Den veckovisa återläsning som genomförs inkluderar därför inte patientdata, men i övrigt innebär det en full återläsning från senaste säkerhetskopia. Under helgen körs sedan en så kallad DBCC (Database Consistency Checker) vilket kontrollerar återläst data i syfte att säkerställa att denna inte är felaktig eller korrupt. Återläsning till produktionsmiljön görs inte på regelbunden basis. Senaste gången det gjordes var vid uppgraderingen till Cosmic 8.1 under 2017, vilket enligt uppgift gick smärtfritt och tog ett par timmar att genomföra.

Övervakning av schemalagda jobb i Cosmic

Enligt uppgift vid granskningen finns inga schemalagda jobb till eller från Cosmic som är kritiska avseende systemets funktionalitet eller integritet. Ett viktigt schemalagt jobb är dock den dataöverföring som sker mellan kärnsystemet Cosmic och informationslagret Cosmic Intelligence (CI). I CI kan organisationen hantera, beskriva, och presentera information från Cosmic, och det är även härifrån som rapporter i Diver hämtar data, varför riktigheten i överföringen mellan Cosmic och CI är viktig. Detta jobb körs varje natt och övervakas av förvaltningsgruppen för Cosmic samt förvaltningsgruppen för Diver genom att kontrollera automatiska rapporter som skickas till deras gemensamma mailbox.

Övervakning av driftmiljön

Omfattande övervakning sker i dagsläget av driftmiljön. På komponentnivå (så som servrar och databaser) sker övervakning med hjälp av Microsofts verktyg System Center Operations Manager (SCOM) i vilken händelser (events) genereras då fel eller problem inträffar. På applikationsnivå sker övervakning med hjälp av Cambio System Monitoring (CSM) vilket är ett integrerat övervakningssystem för Cosmic som kontinuerligt övervakar trender och prestanda i applikationen. I bägge fallen finns en grad av personberoende då övervakning sker av definierade grupper eller personer som behöver identifiera problem och registrera som incidenter i förekommande fall. Det finns en målsättning hos Region Jönköping att minska detta personberoende och förenkla processen för identifiering av problem i driftmiljön och man har därför ett pågående projekt med att helt automatisera övervakningen på komponentnivå i Microsoft System Center Operations Manager

(SCOM). I och med detta ska händelser (events) automatiskt generera incidenter i ärendehanteringssystemet SDM, vilket förenklar information till support hos Kundservice samt distribution till ansvarig servicetekniker. För komponenter relaterade till Cosmic förväntas denna lösning vara fungerande inom 1 till 2 år.

3.4 Integration mellan Cosmic och Diver

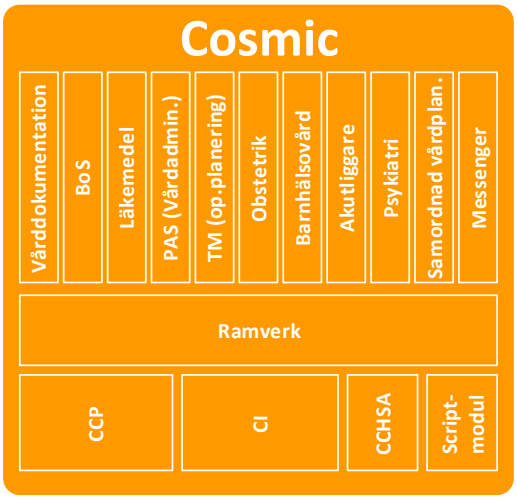
Diver är ett centralt verktyg för planering, uppföljning, och analys av regionens verksamhet med Cosmic som ett av de system som föder mest kritisk verksamhetsdata in i Diver. En viktig aspekt i detta är därigenom integrationen mellan Cosmic och Diver, det vill säga hur data överförs mellan systemen och hur denna säkerställer att det är korrekt och riktig information som presenteras i Diver.

Granskningen har fokuserats kring:

- Systemarkitektur för Cosmic
- Dataöverföring mellan Cosmic och Diver
- Säkerställande av dataintegritet, det vill säga hur det säkerställs att data som förs över från Cosmic är komplett

Systemarkitektur för Cosmic

Ansvaret för systemarkitekturen i Cosmic och dess ingående moduler ligger hos systemleverantören Cambio. De ansvarar för att säkerställa att systemets arkitektur är lämplig baserat på de krav som kommer från Cosmics kundgrupp och i samband med nya releaser upprätta en systembeskrivning som beskriver denna. Se nedan figur för en översiktlig systemarkitektur för Cosmic. Det är alltså Cambio och inte Region Jönköping som fattar beslut avseende denna även om man, tillsammans med representanter från övriga i kundgruppen, har möjlighet till diskussion och insikter kring de beslut som fattas av Cambio.



Figur 8 - Övergripande systemarkitektur Cosmic

Cosmic har dock ett stort antal integrationer till andra system som används inom vården. Majoriteten av dessa går genom Cosmic Connect Publish (CCP i figur 6 ovan), som är ett presentationsverktyg i Cosmic som möjliggör integration till externa system. Undantagen är integrationen till Diver som går via presentationsverktyget CI. De övriga verktygen i

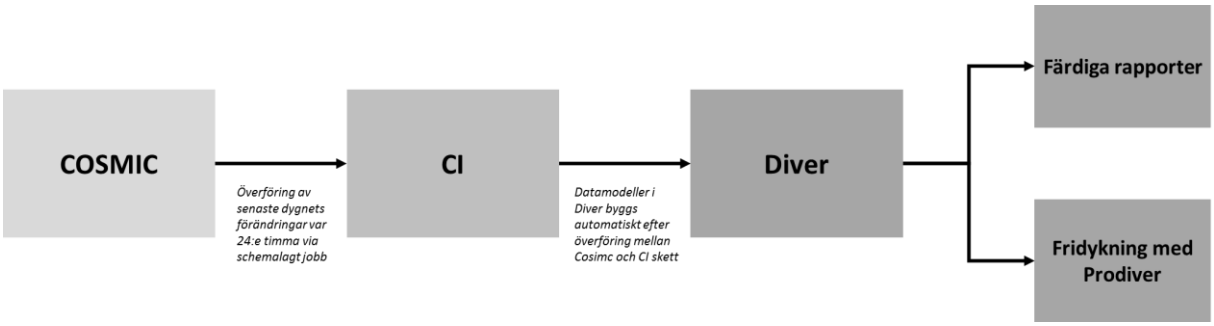
figuren ovan, Cosmic Connect HSA (CCHSA) som erbjuder standardiserad informationsöverföring mellan nationell HSA-katalog och Cosmic samt Scriptmodul används i dagsläget inte inom Region Jönköping.

Vid nyutveckling eller anpassning av befintliga lösningar ingår en analysfas som ett första steg i utvecklingsprocessen. I denna analysfas skall en arkitekturanalys genomföras, i vilken inverkan från lösningens arkitektur ska utvärderas. I denna fas har projektet eller förvaltningsgruppen som ansvarar för lösningen stöd av den så kallade arkitekturgruppen. I denna ingår chefsarkitekt, IT-strateg, IT-säkerhetsansvarig, samt alla som innehar titeln arkitekt. Denna grupp träffas varannan vecka och fungerar som rådgivande och beslutande organ i frågor som rör lösningsförslag.

Då det höga antalet integrationer inom regionens IT-miljö bidrar till en hög komplexitet har även bildats ett så kallat Integration competency center (ICC) för att säkerställa att dessa hanteras på ett enhetligt sätt. ICC innefattar ett team med integrationsspecialister som ska integrationer i applikationslandskapet hanteras strategiskt och strukturerat. Som utgångspunkt i arbetet finns ett framtaget ramverk med riktlinjer för integrationer, lösningsmönster, standarder, mallar, etc.

Dataöverföring och dataintegritet i integrationen mellan Cosmic och Diver

Som ett led i informationsflödet mellan Cosmic och Diver används Cosmic Intelligence (CI). Detta är en standardmodul i Cosmic och är ett informationslager varifrån man kan hantera, beskriva och presentera information från hela Cosmic. CI innehåller samma information som Cosmic fast tillrättalagd och optimerad för att användas för utdata som statistiska analyser, verksamhetsrapporter och uppföljningar.



Figur 9 - Dataflöde Cosmic till Diver

Dataflödet är illustrerat i figur 7 ovan. Varje dygn under natten laddas data från Cosmic till CI via ett schemalagt jobb. Detta innefattar komplett data från Cosmic, varvid CI kan ses som en kopia av produktionsdatabasen. I CI är dock denna information strukturerad med syfte att vara optimerad för att kunna presentera och analysera. Att detta jobb går som planerat och att komplett data överförs övervakas av förvaltningsgruppen för Cosmic och Diver. Automatiska rapporter som beskriver utfallet av överföringen skickas till en gemensam mailbox för respektive förvaltningsgrupp. Detta övervakas dagligen och i det fall fel inträffar i överföringen rapporteras ett ärende i Cambios ärendehanteringssystem för felhantering (se iakttagelse 3.1 i avsnitt 4).

När data har förts över till CI startat bygget av så kallade modeller i Diver, vilka samlar information inom definierade verksamhetsområden, vårdprocesser, med mera. I dagsläget finns cirka 150 sådana modeller i Diver. Data i dessa modeller är statisk under

ett dygn till dess att ny data från Cosmic förs över till CI under nästkommande natt. Viss del av innehållet i modellerna visas sedan i fördefinierade rapporter som användare kommer åt i en webbportal. Det är vanligtvis på detta sätt normalanvändare använder Diver. Kvalificerade användare kan alternativt själva analysera information i modellerna med hjälp av verktyget Prodiver.

Inom verksamheten sker kontinuerlig utveckling av nya modeller i Diver utifrån verksamhetens behov av vilken information man vill kunna följa upp och analysera. I samband med utveckling av nya modeller sker testning, dels av utvecklare men även av beställare från verksamheten som stämmer av att data som presenteras i Diver är vad som förväntas utifrån den underliggande informationen i Cosmic.

3.5 IT- och Informationssäkerhetsarbete

Vikten av god IT- och Informationssäkerhet är ett område som växer i takt med den digitala utvecklingen. Information som behandlas i verksamheters informationssystem är många gånger värdefull och behöver därför skyddas, något som för Cosmic är ytterst viktigt för att garantera patientsäkerhet. Ett genomarbetat IT- och informationssäkerhetsarbete ger verksamheten förtroende och lägger grunden för en effektiv informationshantering.

Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram ett metodstöd för systematiskt informationssäkerhetsarbete och implementation av ett ledningssystem för informationssäkerhet (LIS), vilket utgår från standarder enligt ISO27000 framtagna av internationella expertgrupper. MSBs metodstöd tillsammans med LIS har varit utgångspunkten för denna granskning. De delar som granskningen har fokuserats kring är:

- Policys och riktlinjer
- Utbildningsinsatser inom informationssäkerhet
- Klassning av information
- IT-säkerhet
- Riskanalys

Region Jönköping har i sitt informationssäkerhetsarbete haft LIS som utgångspunkt och regionens ledningssystem för informationssäkerhet är baserat på SS-ISO27000 - Ledningssystem för informationssäkerhet. En informationssäkerhetsgrupp har skapats internt för att leda regionens arbete med informationssäkerhet. Ambitionen är att gruppen ska verka på ledningssystemnivå och ansvara för att ta fram riktlinjer, regler och rutiner, samt att stödja och hjälpa i det dagliga arbetet ute i verksamheten.

Policys och riktlinjer

Regionen har en övergripande informationssäkerhetspolicy som gäller för hela verksamheten. Denna policy innehåller även underliggande riktlinjer för informationssäkerhet. Policyn i kombination med övriga riktlinjer är informationssäkerhetsgruppens ansvar, även om det yttersta ansvaret ligger på regionstyrelsen. Informationssäkerhetsgruppen består av fyra medlemmar. Regionens kanslidirektör ingår i gruppen och är utsedd informationssäkerhetsansvarig.

För att länka samma informationssäkerhetsgruppens arbete med verksamheten finns IT-kontaktpersoner i varje verksamhet. Dessa verkar som informationssäkerhetsgruppens förlängda arm.

Utbildning

Vid nyanställning finns det en checklista som varje anställd ska gå igenom. Denna innehåller även ett avsnitt om informationssäkerhet. Det är verksamhetschefens ansvar att denna checklista fylls i och efterföljs. Någon dokumenterad uppföljning eller kontinuerliga utbildningsinsatser inom informationssäkerhet finns dock inte för anställda inom regionen (se iakttagelse 4.1 i avsnitt 4).

Utöver genomgången vid nyanställningar genomförs, två gånger per år, träffar för alla IT-kontaktpersoner i verksamheterna där bland annat informationssäkerhet diskuteras. Det finns också en framtagen fördjupande informationssäkerhetsutbildning för IT-kontaktpersoner, vilken har sin grund i informationssäkerhetspolicyns riktlinjer.

Informationsklassning

Informationsklassning är en metod där den information som behandlas i informationssystem klassificeras enligt hur kritisk den är utifrån tillgänglighet, riktighet, och konfidentialitet. Denna klassning hjälper verksamheten att välja rätt åtgärder som skyddar informationen. En fullständig informationsklassning har inte genomförts av regionen (se iakttagelse 4.2 i avsnitt 4). Regionen har ett pågående arbete som hittills har mynnat ut i en informationsklassning av 16 system. Informationsklassning genomförs med hjälp av verktyget KLASSA från Sveriges Kommuner och Landsting, SKL. Diver och Cosmic har inte inkluderats bland de system som har informationsklassats.

Samtliga informationssystem finns identifierade och dokumenterade i en systemförteckning. Regionen har nyligen identifierat system som innehåller personuppgifter, bland annat genom ett arbete med informationshanteringsplaner. Detta har genomförts genom att ute i verksamhet titta på vilken information man har och var det finns personuppgifter, både digitalt och fysiskt.

IT-säkerhet

I regionens informationssäkerhetspolicy finns det riktlinjer framtagna för fysisk säkerhet. Enligt riktlinjerna ska verksamhetens kritiska IT-system och informationstillgångar skyddas i säkra utrymmen med skalskydd och lämpliga tillträdeskontroller. Region Jönköpings serverutrymmen är endast tillgängligt för driftchef och ett antal särskilt utvalda tekniker. Policyn innehåller även krav på att det ska finnas rutiner för hur utrustning ska avvecklas. Region Jönköping har ett samarbete med en extern part som hjälper till att hantera datorutrustning som behöver rensas eller tas ur bruk.

Penetrationstester genomförs kontinuerligt i syfte att identifiera eventuella sårbarheter. Inom IT-centrums säkerhetsorganisation används även ett tekniskt verktyg för att regelbundet identifiera sårbarheter i IT-miljön.

Riskanalys

En riskanalys genomförs för att identifiera och bedöma sådana risker som skulle kunna äventyra informationssäkerheten. Ingen övergripande riskanalys har gjorts för regionens verksamhet och inte heller specifikt för Cosmic eller Diver (se iakttagelse 4.3 i avnsitt 4). De riskanalyser som har genomförts av regionen har varit i samband med nya applikationer som införts. Riskanalyser är en bra grund i utformning av kontinuitetsplaner

samt ett stöd i beslut rörande förvaltning av IT-system. Ansvaret för att ha en kontinuitetsplan ligger på varje enskild systemägare. Informationssäkerhetsgruppen har tagit fram riktlinjer för hur en kontinuitetsplan bör utformas. Varje systemägare har sedan ansvaret för att ta fram en kontinuitetsplan för respektive system.

4. Iakttagelser och rekommendationer

Under granskningen har EY identifierat iakttagelser inom granskade områden. För varje iakttagelse har EY lämnat rekommendationer som syftar till att stödja regionen i dess framtida arbete med IT- och informationssäkerhet. De av EY identifierade iakttagelserna har klassificerats enligt tre risknivåer avseende hur omfattande dess eventuella inverkan anses vara:

HÖG	Observation av större karaktär som anses kunna ha hög påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer.
MEDEL	Observation som anses kunna ha påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av verksamhetens resurser.
LÅG	Observation som ej direkt påverkar verksamhetens mål, men kan medföra ineffektiv verksamhet, mindre brister i IT- och informationssäkerhet, efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.

1.1 Beställning för borttag av användare i Cosmic kan ske med visst dröjsmål

Iakttagelse MEDEL	Processen för borttag av användare i Cosmic fungerar inte alltid enligt den process som är definierad. Beställning från verksamheten för borttag av inaktiva användare kan ske med visst dröjsmål. Inom processen för borttag av behörigheter finns inga riktlinjer eller tidsreferenser definierade för när användare ska tas bort.
Rekommendation	Region Jönköping rekommenderas att implementera riktlinjer för borttag av användare som möjliggör att behörigheter tas bort snarast efter avslutad anställning. Regionen rekommenderas även utvärdera ifall processen för borttag av inaktiva användare kan automatiseras.

1.2 Ingen periodisk genomgång av användare i Cosmic genomförs

Iakttagelse MEDEL	Under EY's granskning framkom det att det inte görs någon periodisk genomgång av verksamhetens behörigheter i Cosmic för att säkerställa att dessa är lämpliga. En genomgång av HSA-katalogen görs 3 gånger per år för att identifiera avslutade resurser. Det finns dock ingen koppling mellan HSA-katalogen och Cosmic som gör att inaktiva användare i Cosmic upptäckts i den periodiska genomgången av användare i HSA.
Rekommendation	EY rekommenderar Region Jönköping att införa en process för periodisk genomgång av behörigheter i Cosmic. Processen bör innehålla följande: ► En granskning genomförd av ansvarig chef som täcker alla användare med behörighet till Cosmic, för att säkerställa att alla användare är lämpliga. ► Beskrivning för hur avvikelser ska rapporteras och hanteras. ► Den periodiska genomgången rekommenderas att genomföras minst årligen.

1.3 Kontroll av användarloggar i Cosmic omfattar ett begränsat urval

Iakttagelse MEDEL	Det genomförs en manuell stickprovskontroll av användares loggar i Cosmic. Kontrollen genomförs av varje verksamhets genom att månatligen kontrollera loggar för två anställda. Denna rutin omfattar således ett begränsat urval av loggar och det medför en risk att avvikelser i användares beteenden inte upptäcks.
Rekommendation	Region Jönköping har ett pågående initiativ att införa automatisk kontroll av loggar i Cosmic. EY rekommenderar regionen att fortsätta arbetet med att implementera en automatisk kontroll av loggar genom Loggpoint då det anses kunna stärka patientsäkerheten. Implementation rekommenderas ske på kort- eller medellång sikt.

1.4 Serveradministratörer har behörighet till samtliga servrar inom regionen

Iakttagelse HÖG	Blir man tilldelad rollen som serveradministratör får man tillgång till alla servrar hos region Jönköping. En serveradministratörs behörigheter är inte definierade utifrån vilka servrar som är relevanta för administratörens arbetsuppgifter. En serveradministratör för Cosmic har således tillgång till samtliga övriga servrar i regionen och vice versa. Detta gäller även för resurser från Cambio support med serveradministratörsbehörighet.

Rekommendation	Region Jönköping har ett pågående arbete med segmentera serveradministratörers behörigheter. EY rekommenderar regionen att fortsätta detta arbete så att tillgång till Cosmic-servrar endast innehas av personer med behov av detta för att kunna utföra sina arbetsuppgifter. Segmenteringen rekommenderas att genomföras på kort- eller medellång sikt.

1.5 Ingen periodisk genomgång av priviligierade användare genomförs

Iakttagelse MEDEL	Region Jönköping genomför sporadiska rensningar av höga behörigheter på servernivå, databaser och applikationen. Det finns dock ingen etablerad process för att en återkommande periodisk genomgång av höga behörigheter inklusive Cambio support ska genomföras.
Rekommendation	EY rekommenderar region Jönköping att införa en process för periodisk genomgång av priviligierade användare i Cosmic. Processen bör innehålla följande: ► En granskning genomförd av ansvarig chef som täcker alla användare med höga behörigheter till Cosmic, för att säkerställa att alla priviligierade användare är lämpliga. ► Beskrivning för hur avvikelser ska rapporteras och hanteras. ► Den periodiska genomgången rekommenderas att genomföras minst årligen.

1.6 Ingen kontroll av priviligierade användares loggar i Cosmic genomförs

Iakttagelse HÖG	Inom IT-centrum har en stor andel höga behörigheter i Cosmic för att kunna utföra sina arbetsuppgifter. Dessa behörigheter är breda och gör att användarens begränsningar är limiterade. Den manuella stickprovskontrollen av loggar som genomförs av verksamheten appliceras inte på de priviligierade användare som finns inom IT-centrum. Granskning av loggar för priviligierade användare kan ske men genomförs endast vid misstanke om regelbrott.
Rekommendation	Region Jönköping har ett pågående initiativ att införa automatisk kontroll av loggar i Cosmic. EY rekommenderar regionen att fortsätta arbetet med att implementera en automatisk kontroll av loggar genom Loggpoint och även applicera den för priviligierade användare. Implementation rekommenderas ske på kort- eller medellång sikt.

2.1 Återläsningstester genomförs men dokumenteras inte

Iakttagelse LÅG	I granskningen noterades att återläsning av Cosmic-data sker veckovis när senaste diskbackup återläses till elevmiljön. Resultatet av återläsningen kontrolleras av systemtekniker. I samband med detta körs även en så kallad DBCC (Database Consistency Checker) för att kontrollera återläst data och säkerställa att denna inte är korrupt eller felaktig. Dessa återläsningstester dokumenteras dock inte, vilket de enligt regionens riktlinjer inom dess informationssäkerhetspolicy ska göra.
Rekommendation	EY bedömer risken relaterat till denna iakttagelse som mycket låg då det finns en etablerad rutin där återläsning genomförs ofta och regelbundet. Det kan dock föreligga en risk att återläsning, och tester som genomförs för att kontrollera att den skett korrekt, får en hög grad av personberoende om de inte dokumenteras enligt definierade riktlinjer. Region Jönköping rekommenderas att halvårsvis dokumentera återläsningen till elevmiljön samt de tester som genomförs för att kontrollera att den skett korrekt.

3.1 Regionen har låg insikt i hur kontrollen av dataöverföring mellan Cosmic och Diver är definierad

Iakttagelse LÅG	Varje dygn under natten överförs senaste dygnets förändringar i data från Cosmic till CI via ett schemalagt jobb. Automatisk monitorering är konfigurerad för att kontrollera att detta jobb går som planerat och att komplett data överförs. Detta genererar automatiska rapporter till förvaltningsgruppen för Cosmic och Diver och vid eventuella fel rapporterar de detta till Cambio för felhantering. I granskningen noterades att Region Jönköping inte har insikt i hur kontrollen att jobbet går enligt planen är definierad, dvs. vilka parametrar eller vilka attribut i överföringen som kontrolleras för att säkerställa att denna är korrekt.
Rekommendation	EY bedömer risken relaterat till iakttagelsen som låg då Cambio antas ha nödvändig insikt och kompetens för att säkerställa att dataöverföringen är komplett och korrekt. Då överföringen är viktig för att korrekt data ska presenteras i Diver, rekommenderas dock regionen att i samråd med Cambio säkerställa att man har tillräcklig insikt i hur kontrollen sker och att denna är lämplig givet regionens krav.

4.1 Kontinuerlig utbildning inom IT- och informationssäkerhet genomförs inte

Iakttagelse LÅG	Vid nyanställning får varje anställd ta del av material om informationssäkerhet. De IT-kontaktpersoner som finns i verksamheten har sedan möjlighet till att få en fördjupad informationssäkerhetsutbildning. För övriga anställda finns dock inga kontinuerliga utbildningsinsatser inom IT- och informationssäkerhet för att säkerställa god kompetens och efterlevnad av riktlinjer i verksamheten.
Rekommendation	Region Jönköping rekommenderas att se över möjligheten att införa en process för att säkerställa kontinuerlig utbildning inom IT- och informationssäkerhet för alla anställda. Utbildning rekommenderas att ske minst årligen och kan ske antingen fysiskt eller genom en digital lösning.

4.2 En fullständig informationsklassning av regionens verksamhet har inte genomförts

Iakttagelse LÅG	En fullständig informationsklassning omfattade samtlig information som behandlas i verksamheten har inte genomförts. Region Jönköping har dock genomfört informationsklassning för 16 enskilda system där Cosmic och Diver dock inte har inkluderats.
Rekommendation	Region Jönköping rekommenderas att utvärdera om en fullständig informationsklassning bör genomföras på medellång sikt för att bistå verksamheten i att välja rätt åtgärder och ställa rätt krav gentemot IT-centrum för att skydda informationen. Om inte behovet av en fullständig informationsklassning anses föreligga rekommenderas en informationsklassning av Cosmic genomföras då systemet behandlar kritisk information.

4.3 Regionen har inte genomfört en övergripande riskanalys

Iakttagelse LÅG	En övergripande riskanalys av Region Jönköpings verksamhet, eller riskanalyser för Cosmic eller Diver, har inte genomförts. De riskanalyser som har gjorts har varit i samband med implementationen av nya enstaka applikationer och inte för verksamheten i sin helhet. En riskanalys genomförs för att identifiera och bedöma risker kopplade till informationssäkerhet för att ligga till grund för beslut rörande systemförvaltning och/eller utformande av kontinuitetsplaner.

Rekommendation	EY rekommenderar Region Jönköping att utvärdera behovet av att genomföra en övergripande riskanalys av verksamheten, eller riskanalyser specifikt för Cosmic och Diver i syfte att stödja verksamheten i utformning av kontinuitetsplanen, samt beslut kring förvaltning av systemen. Om en övergripande riskanalys beslutas att genomföras bör den enligt MSBs metodstöd besvara följande tre frågor: ► Vad kan hända? ► Hur sannolikt är det? ► Vad blir konsekvenserna?

5. Svar på revisionsfrågor

Granskningen har syftat till att ge revisorerna underlag för att bedöma om IT-säkerheten inom kritiska områden i Cosmic, samt dess integration till Diver adresseras på ett ändamålsenligt sätt. Granskningen har utgått från fem revisionsfrågor, vilka besvaras nedan.

Finns kontroller avseende behörighetshantering i Cosmic som säkerställer att personal endast har åtkomst till funktioner lämpliga för dennes behov?

Kontroller och rutiner för att säkerställa att personal endast ska ha åtkomst till funktioner lämpliga för deras behov finns. Det finns en etablerad process för hur verksamheten ska beställa upplägg av nya behörigheter i Cosmic, samt borttag av behörigheter för anställda som har slutat. Det finns även etablerade rutiner för höga behörigheter där den anställdas chef samt förvaltningsgruppen skall utvärdera och godkänna behovet av dessa accesser.

EY har dock noterat iakttagelser inom området för behörighetshantering som anses viktiga för Region Jönköping att adressera för att stärka kontrollen kring användares behörigheter och aktiviteter i Cosmic. Primärt rekommenderas regionen att säkerställa att behörigheter i Cosmic (både normala och högre behörigheter) ses över på regelbunden basis, samt att logguppföljning av användares aktiviteter stärks och även innefattar höga behörigheter. För ytterligare information kring noterade iakttagelser och EY's rekommendationer, se avsnitt 4.

Finns kontroller avseende programförändringar i Cosmic som säkerställer att inga förändringar som inte är ändamålsenliga för systemet implementeras?

EY anser att kontroller och rutiner som praktiseras inom regionen avseende programförändringar är mycket lämpliga i syfte att säkerställa att endast lämpliga förändringar implementeras. Region Jönköping har ett fungerande samarbete i Kundgruppen Cosmic tillsammans med övriga aktörer vilket ger en tydlighet i kravställningen gentemot systemleverantören Cambio. Utöver kontroller kring testning och implementering av ny funktionalitet som sker inom ramen för kundgruppen anses även ändamålsenliga kontroller finnas inom regionens verksamhet vid införande av ny funktionalitet i Cosmic.

I granskningen har inga iakttagelser inom ramen för hantering av programförändringar noterats.

Finns kontroller och uppföljningsrutiner hos regionen som säkerställer att driften av Cosmic hanteras på ett säkert och ändamålsenligt sätt?

Rutiner kring IT-drift inom Region Jönköping bedöms vara lämpliga i syfte att säkerställa att denna hanteras på ett säkert, stabilt, och ändamålsenligt sätt. EY bedömer de och kontroller som finns på plats avseende hantering och övervakning av säkerhetskopiering, schemalagda jobb, incidenter, samt övriga komponenter i infrastrukturen vara goda och verka för att tillgodose verksamhetens behov avseende tillgänglighet, riktighet och sekretess.

Är informationssäkerhetsarbetet inom regionen ändamålsenligt i syfte att säkerställa patientsäkerhet i Cosmic?

EY's bedömning är att Region Jönköpings mognadsgrad avseende IT- och informationssäkerhetsarbetet är hög, och man har även pågående initiativ för att säkerställa att verksamheten anpassas till det kommande dataskyddsdirektivet GDPR som träder i kraft i maj 2018. Regionen har en väl utformad organisation rörande informationssäkerhetsarbetet vars ansvar är skilt från IT-centrum som ska verka för effektiv leverans av IT-tjänster. Policys och riktlinjer för informationssäkerhetsarbete finns etablerade och följer god praxis. EY rekommenderar dock att utbildningsinsatser för verksamheten stärks i syfte att säkerställa kunskap och efterlevnad inom området i hela verksamheten.

Informationssäkerhetsarbetet på ledningsnivå inom regionen anses ändamålsenlig i syfte att säkerställa patientsäkerhet. Dock har även iakttagelser inom processen för behörighetshantering som anses viktiga i syfte att säkerställa patientsäkerhet i Cosmic noterats. Se svar under första revisionsfrågan ovan för ytterligare förklaring kring dessa iakttagelser.

Säkerställer integrationen mellan Cosmic och Diver dataintegritet, dvs. sker hantering och överföring av data från Cosmic till Diver på ett sätt sådant att det är aktuell och korrekt data som presenteras i Diver?

EY bedömer att integrationen mellan Cosmic och Diver, och överföringen av data mellan de två systemen hanteras på ett strukturerat och säkert sätt. Övervakning sker dagligen i syfte att säkerställa att komplett och korrekt information förs över från Cosmic. Vid utvecklande av nya modeller i Diver, det vill säga möjliggörande att presentera ytterligare information från exempelvis Cosmic, sker avstämning och testning av både IT och beställande verksamhet för att kontrollera att förväntad data presenteras i Diver.

Vid granskningen noterades att kunskapen i hur övervakningen av att komplett data förs över från Cosmic är konfigurerad finns hos systemleverantören Cambio, varvid regionen rekommenderas säkerställa att denna insikt även finns internt.

6. Intervjuförteckning

Uppstartsmöte

- Kanslidirektör & Informationssäkerhetsansvarig
- IT-direktör
- Hälso- och Sjukvårdsstrateg & Systemägare Cosmic
- Ekonomidirektör & Systemägare Diver

Möte kring behörighetshantering I Cosmic

- Tjänste- och objektägare IT Cosmic
- Systemförvaltare Cosmic
- Utredare Folkhälsa & Sjukvård
- Systemutvecklare Diver

Möte kring informationssäkerhetarbetet i regionen

- Kanslidirektör & Informationssäkerhetsansvarig
- Informationssäkerhetsstrateg
- Informationssäkerhetsspecialist
- Informationssäkerhetsspecialist

Möte kring IT-drift av Cosmic

- Förvaltningsledare Infrastruktur kommunikation, telefoni, larm, video
- Systemtekniker Cosmic
- Incidentkoordinator Kundservice
- Tjänste- och objektägare IT Infrastruktur
- Tjänste- och objektägare IT Cosmic

Möte kring hantering av programförändringar för Cosmic

- Chefsarkitekt
- Tjänste- och objektägare IT Cosmic

Möte kring hantering av höga behörigheter

- Tjänste- och objektägare IT Infrastruktur
- Tjänste- och objektägare IT Cosmic

Möte kring integrationen mellan Cosmic och Diver

- Chefsarkitekt
- Utredare Folkhälsa & Sjukvård
- Systemutvecklare Diver