Missiv beslutsunderlag
Diarienr: 14LTK1283
Handläggare: Jan Cserpes, Kansliavdelningen
Datum: 2015-03-02

REGION KRONOBERG

Regionstyrelsen

Svar på revisionsrapport – Behörighetsgranskning Cosmic och Aplus, samt Granskning avseende IT- och informationssäkerhet

Förslag till beslut
Föreslås att regionstyrelsen beslutar

att ställa sig bakom svar till revisorerna.

att informera regionfullmäktige om rapport och svar.

Sammanfattning
EY har på revisorernas uppdrag genomfört en granskning av hanteringen av behörigheter samt uppföljningen av användandet av patientinformationen i Cosmic. Detta uppdrag har även innefattat kraftiga behörigheter i Region Kronobergs redovisningssystem Aplus. Därutöver har en granskning av IT- och informationssäkerhet för policys, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå genomförts.

Revisorerna konstaterar att strukturen för informationssäkerhetsarbetet inom organisationen fungerar tillfredsställande, även om områden finns som bör förbättras. Revisorerna uppfattar att det finns en god vilja att förbättra det interna kontrollarbetet i organisationen.

Revisorerna lyfter fram förbättringsområden i de båda rapporterna.

Behörighetsgranskning Cosmic och Aplus

Kommentar/förslag till revisorernas identifierade förbättringsområden

1. *En tydligare och mer sammanhållen process rörande behörigheter till SITHS-kort och behörigheter till Cosmic. Införa en slutlig kontroll som säkerställer att kontrollmomenten uppfyllts.*

REGION KRONOBERG

SITHS-koret är en tjänstelegitimation för både fysisk och elektronisk identifiering. Det ger i sig ingen behörighet till något system. Kortet är en säker identifiering av en person och det krävs en behörighet till själva systemet, exempelvis Cosmic. SITHS-kortet ger även en identifiering för användande av nationella eHälso-tjänster, som till exempel Pascal och Mina vårdkontakter.

Cosmic kräver ett SITHS-kort för identifiering. Utöver kortet behövs en behörighetstilldelning i Cosmic. Idag finns det en separat beställningen med ett eget webbformulär där behörig beställare fyller i ett antal parametrar. Dialoger pågår för att samordna Cosmics behörighetsbeställning och *anställningspaketet*. Det finns en del kvarstående frågor som t ex att behörighet i Cosmic ändras under en anställningsperiod och att det ”bakom” anställningspaketet finns en manuell hantering av alla parametrar.

Nationella eHälsotjänster kräver ett SITHS-kort för identifiering. Utöver kortet behövs en behörighetstilldelning i den nationella HSA-katalogen. Detta administrerar vårdenheterna själva direkt i Region Kronobergs verksamhetskatalog.

Avslut av SITHS-kortet, leder till att möjlighet att identifiera sig (inloggning) i Cosmic och i de nationella tjänsterna upphör. Förbättringsåtgärd kommer att vidtas för att säkerställa att behörigheten till Cosmic upphör. Det genom att ett automatgenererat ärende till VIS-support skapas, när en person avslutas via anställningspaketet. Region Kronoberg kommer att återgår till rutinen att ta bort behörigheter för användare som inte har varit aktiva på tre månader. Detta innebär en dubblerad säkerhet för att ta bort åtkomst till Cosmic. Är SITHS-kortet ogiltigt eller behörigheten i Cosmic avslutad får användaren inte någon åtkomst till Cosmic.

I samband med beställning av avslut av tjänst i anställningspaketet eller via ärende-hanteringssystemet (Easit) avslutas behörigheter i systemen. Kortet ska i samband med att avslut görs, skickas in till intern kundservice för makulering. Det är varje chefs ansvar att återta den anställdes e-tjänstekort vid avslut av tjänst. Det saknas idag en automatisk kontroll av att kort inkommer då anställningspaketet inte har någon påminnelsefunktion för de moment som ska genomföras. En rutin för manuell hantering ska upprättas och träda i kraft 2015-03-01. Det innebär en kontroll av samtliga avslutade ärenden för att säkerställa att kortet har inkommit för makulering. Ansvarig för upprättande av rutinen är avdelningschef för intern kundservice.

2. *Alla enheter bör använda Anställningspaketet (ett antal kontroller och dokument som används vid till exempel nyanställning) för att få en enhetlig kontrollstruktur.*

Samtliga anställda som har ett anställningsförhållande med Region Kronoberg hanteras via anställningspaketet, det gäller både vid nyanställning, byte av tjänst samt avslut av tjänst. Det är närmast ansvarig chef som tar initiativ till beställning av anställningspaketet. För övriga som har behov av ett e-tjänstekort hanteras beställningar via ärendehanteringssystemet Easit. Det kan gälla personer som är anställda vid kommuner, samt hyrpersonal.

3. *Uppföljning av att loggkontroller utförts bör utökas.*
4. *Införa tydligare instruktioner om hur de lokala loggkontrollerna ska utföras.*

Svar till punkterna 3 och 4.

Verksamhetschefen är ansvarig för att loggkontroller genomförs på sin vårdenhet. Detta har förtydligats i riktlinjen ”Behörighet och åtkomst till Cosmic” som gäller från 2014-11-10, denna omfattar även loggkontrollen.

I Region Kronobergs internkontrollsplan finns en central uppföljningspunkt för kontroll av loggar. Den centrala kontrollen är genomförd årligen med en uppföljning.

Processen för uppföljning förbättras genom att utöka antalet uppföljningar på de verksamheter som inte har en tillfredsställande dokumentation av loggkontrollen. Detta sker månadsvis tills de har en tillfredsställande dokumentation. Rutinen för loggkontroll har uppdaterats med denna förbättrade uppföljning.

Användare och verksamhetschefer har en hög förståelse för att loggkontroller ska genomföras. Dock finns det en stor önskan om ett bättre IT-stöd där ett avvikande beteende kan identifieras och följas upp. En förstudie om hur detta ska lösas för samtliga loggar av patientinformation (loggar från olika system) i Region Kronoberg ska genomföras. Syfte är finna en lösning där verksamhetscheferna (eller den de har delegerat uppdraget till) får ett bra IT-stöd, med beslutsstöd för loggkontroller. Region Kronoberg kommer, enligt de nationella riktlinjerna, även publicera loggen till invånarna själva när denna nationella tjänst finns tillgänglig i ”journal via nätet”.

5. *Finns många användare med kraftiga behörigheter till ekonomisystemet Aplus.*

Inför 2015 har samtliga behörigheter till ekonomisystemet Aplus gåtts igenom och gjorts om. De nya behörigheterna börjar användas 1 januari 2015 och de gamla stängs löpnade under de första månaderna 2015. I den nya behörighets-strukturen kommer endast sex personer ha kvar kraftiga behörigheter. Av dessa sex personer är det tre konsulter hos Aditro som fortsätter ha kraftiga behörigheter. Det för att Aditro ska kunna utöva den supportfunktion Region Kronoberg har behov för. Resterande kraftiga behörigheter innehas av två personer på IT systemstöd ekonomi och av en person på redovisningsstöd.

Granskning avseende IT- och informationssäkerhet

Kommentar/förslag till revisorernas identifierade förbättringsområden

1. *Det är naturligt att inta alla system och avdelningar har samma höga säkerhetsnivå som t ex Patientsystemet, men där det bör finnas en tydlighet vilka regler som gäller för vad.*

Region Kronoberg ska införa en modell informationsklassning.

REGION KRONOBERG

Modellen för klassificering ska baseras på säkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Nivåbestämningen ska utgå från bedömd skada vid obehörig åtkomst, bristande riktighet, bristande tillgänglighet och bristande spårbarhet. Klassificeringen av informationstillgångar ska ligga till grund för vilka skyddsåtgärder som ska utformas och vilka rutiner som ska gälla, dvs. hur informationen får hanteras, lagras, distribueras och avvecklas. Strävan är att åstadkomma en konsistent bedömning av en och samma informations värde oavsett var eller av vilken verksamhet informationen hanteras.

2. *Det finns omfattande policys och riktlinjer inom organisationen, men den generella uppfattning är att dessa inte riktigt när ut till användarna i den omfattning som behövs i den verksamhet som Lanstinget bedriver.*

Inom landstinget finns det en Policy, den är övergripande för hela verksamheten. I och med regionbildningen (1/1 2015) kommer denna policy ses över för att mer harmoniera med Region Kronobergs uppdrag. Avseende riktlinjerna inom organisationen ska även dessa ses över med hänsyn till Region Kronobergs uppdrag. Både policy och riktlinjer ska därefter kommuniceras till användarna i den omfattning som behövs för att bedriva den verksamhet som Region Kronoberg gör.

3. *Det bör även finnas tydligare instruktioner och struktur i hur det övergripande kontrollarbetet ska utföras, för att säkerställa att de kontroller Landstinget vill ha på plats, verkligen utförs som tänkt och i den omfattning som tänkt.*

Årligen ska det upprättas en granskningsplan för de interna kontrollerna, i syfte att följa upp att det interna kontrollsystemet fungerar tillfredsställande. Resultatet av den antagna planens uppföljning ska rapporteras i den omfattning som anges i planen.

Regiondirektören ska senast i samband med årsredovisningen ge en samlad återrapportering av resultatet från granskningen av den interna kontrollen till regionstyrelsen.

Martin Myrskog
Regiondirektör

Jan Cserpes
ITdirektör

Bilagor: Missiv IT-granskningar
Behörighetsgranskning Cosmic och Aplus
Granskning avseende IT- och informationssäkerhet