LANDSTINGET KRONOBERG
Revisorerna
Till landstingsstyrelsen

Revisionsskrivelse
2014-11-10

EY har på vårt uppdrag genomfört en studie med syfte att få en uppfattning om hur behörigheter hanteras samt om uppföljning görs på användandet av patientinformationen i Cosmic. Detta uppdrag har även innefattat att titta på kraftiga behörigheter i Landstinget Kronobergs redovisningssystem Aplus. Därutöver har EY genomfört en granskning av IT- och informationssäkerhet, vad gäller policys, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå.

Behörighetsgranskning Cosmic och Aplus

Att behörigheter i system är korrekt satta är väsentligt, då de styr vad en användare kan göra och se. Om för kraftiga behörigheter delas ut finns risk för att den interna kontrollen försvagas. Borttag av behörigheter på användare som inte längre skall ha tillgång till information och system reducerar t ex risken att en gammal behöriget används av någon annan.

I vissa fall är det svårt att ha kontroller i systemet som förbjuder visst handlande, men där spårbarhet och granskning av vad användaren gjort blir kontrollen. Cosmic är ett öppet system där användarna t ex kan titta på de flestas patientinformation, men där det då också är möjligt att titta i logglistor vem som tittat på vilken patients information.

I resultatet av granskningen kan det konstateras att kontrollen att granska om en användare tittat enbart på ”sina” patienter inte fungerat tillfredsställande under året.

För inloggning i Cosmic krävs ett Smartcard och lösenord, där kortet ska låsas eller förstöras när en användare slutar anställningen. Vi har noterat att denna hantering bör förbättras, där sju av 25 stickprov inte hade låsts efter 15 dagar.

Följande förbättringsområden har identifierats:

- En tydligare och mer sammanhållen process rörande behörigheter till siths-kort och behörigheter till Cosmic. Införa en slutlig kontroll som säkerställer att kontrollmomenten uppfyllts.
- Alla enheter bör använda Anställningspaketet (ett antal kontroller och dokument som används vid t ex nyanställning) för att få en enhetlig kontrollstruktur.
- Uppföljning av att loggkontroller utförs bör utökas.
- Införa tydligare instruktioner om hur de lokala loggkontrollerna ska utföras.
- Finns många användare med kraftiga behörigheter till ekonomisystemet Aplus.

Revisorerna har inte för avsikt att i nuvarande läge gå vidare med en fördjupad granskning, men det är en rekommendation att i ett framtida projekt göra en utvärdering av de kraftiga konton som finns i Aplus och om dessa är rimligt satta.

Landstingets revisorer översänder bifogad rapport för kännedom till landstingsstyrelsen.

Granskning av landstingets övergripande IT och Informationssäkerhet

Som grund har granskningen gjorts utifrån Myndigheten för samhällsskydd och beredskaps ramverk för informationssäkerhet, BITS, och dess säkerhetsnivåer. BITS står för Basnivå för informationssäkerhet och har sitt ursprung i den internationella informationssäkerhetsstandarden ISO/IEC 27000. En jämförelse har även gjorts med resultatet från liknande granskningar i andra offentliga organisationer.

Av samtliga 82 granskningspunkter är fördelningen av bedömningarna följande:

Aktuellt område i BITS är hanterat och kontroll bedöms rimligen implementerad:	66%
Kontrollen identifierad och bedöms enbart delvis implementerad:	26%
Kontroll har ej identifierats/Har inte kunna identifierats som implementerad:	6%
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	2%

Som siffrorna ovan visar finns det en struktur för informationsarbetet inom organisationen som fungerar tillfredsställande, även om det finns områden som bör förbättras. En generell uppfattning är också att det finns en god vilja att förbättra det interna kontrollarbetet, vilket är positivt.

Följande förbättringsområden har identifierats:

- Det är naturligt att inte 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.
- Det finns omfattande policys och riktlinjer inom organisationen, men den generella uppfattning är att dessa inte riktigt når ut till användarna i den omfattning som behövs i en verksamhet som Landstinget bedriver.
- 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.

Revisorerna har inte för avsikt att i nuvarande läge gå vidare med en fördjupad granskning. Landstingets revisorer översänder bifogad rapport för kännedom till landstingsstyrelsen.

För landstingets revisorer

Sven-Åke Gustavsson
Ordf.

Jan Sahlin
Vice ordf.