LANDSTINGET I VÄRMLAND
Revisionskontoret
Johan Magnusson

Rev/16020

2016-11-14

Generella IT-kontroller – uppföljning av granskning genomförd 2012

Rapport 12-16

Generella IT-kontroller - uppföljning

Bakgrund

Landstingets revisorer ansvarar för att genomföra årlig granskning av landstingets samtliga verksamheter. Utifrån detta uppdrag och ansvar har landstingets revisorer utarbetat dokumentet ”Granskningsstrategi” i vilket de beskrivit de områden som revisorerna främst ska fokusera på under innevarande mandatperiod. Baserad på granskningsstrategin gör revisorerna en årlig riskbedömning och revisionsplan. I ”Revisionsplan 2016” har revisorerna aktualiserat en uppföljande granskning avseende generella IT-kontroller.

Landstingets revisorer genomförde år 2012 en granskning avseende ”Generella IT-kontroller” med fokus på landstingets ekonomisystem. I granskningen framkom bland annat att:

- landstinget saknade en formell kontroll kring periodisk genomgång av användarrättigheter och behörighet till Raindance,
- det inte fanns någon enhetlig rutin och larmhantering kring schemalagda batch-jobb (beräkningar och rapporter i t.ex. EA- respektive PA-systemen som körs automatiskt) och att
- det inte skedde någon formell avrapportering kring avtalad leverans från leverantören Logica samt att det inte sker någon avstämning mot avtal eller Service Level Agreement (SLA)[1].

Av landstingsstyrelsens svar på revisorernas rapport framgick att ekonomistaben skulle se över de aktuella rutinerna för hantering av behörigheter med syfte att förbättra och säkerställa regelbunden granskning av behörigheter och användare i Raindance.

Landstings-IT skulle se över de aktuella rutinerna och utarbeta riktlinjer för hur integrationer, som Landstings-IT har driftansvaret för, ska implementeras och dokumenteras (en ”integrationsstandard”) med syfte att förbättra och säkerställa hur automatisk och manuell övervakning, larmhantering samt felrapportering skall hanteras.

Ekonomistaben skulle utveckla agendan för driftsmöten med formella stående avrapporteringspunkter med syfte att tillgodose en bättre uppföljning av drifts- och supportavtal med leverantören.

[1] I IT-sammanhang reglerar ett SLA vanligtvis vilken tillgänglighet ett system ska ha, hur lång tid det högst får gå innan felavhjälpning ska påbörjas, hur snabbt felet ska vara åtgärdat och hur många gånger ett fel får förekomma under en given tidsperiod.

Syfte och revisionsfrågor

Den övergripande revisionsfrågan är om landstingsstyrelsen har vidtagit åtgärder med anledning av den kritik och de synpunkter som framkom i revisorernas granskning från 2012.

Granskningen ska ge svar på följande revisionsfrågor:

- Har landstingsstyrelsen säkerställt att rutinerna för hantering av behörigheter och användare i Raindance regelbundet granskas?

- Har landstingsstyrelsen tillsett att riktlinjer utarbetats för hur integrationer, som Landstings-IT har driftansvaret för, ska implementeras och dokumenteras?

- Har landstingsstyrelsen säkerställt att agendan för driftsmöten, med IT-leverantören, innehåller formella stående avrapporteringspunkter med syfte att tillgodose en bättre uppföljning av drifts- och supportavtal med leverantören?

- Om granskningen visar att det finns brister, vilka förbättringsåtgärder behöver vidtas?

Avgränsning

Granskningen har avgränsats till att omfatta en uppföljning av rapporten Generella IT-kontroller från 2012.

Revisionskriterier

Granskningen har utgått från tillämplig lagstiftning, relevanta fullmäktigebeslut och styrdokument.

Ansvarig nämnd

Landstingsstyrelsen ansvarar för att tillse att lagar och andra tillämpliga bestämmelser samt fullmäktiges beslut efterlevs. Landstingsstyrelsen ansvarar för den interna kontrollen.

Metod

Granskningen har genomförts i form av dokumentstudier och intervjuer.

Granskningens resultat:

1 Har landstingsstyrelsen säkerställt att rutinerna för hantering av behörigheter och användare i Raindance regelbundet granskas?

I revisionsrapporten från 2012 framfördes en rekommendation om att en formell rutin utformas för att regelbundet granska behörigheter. Detta för att säkerställa att användare i applikationerna och underliggande system har behörigheter som motsvarar arbetsuppgifter. Denna rutin bör utföras minst en gång per verksamhetsår samt dokumenteras.

Av landstingsstyrelsens svar på revisorernas rapport från 2012 framgick att ekonomistaben ska se över rutinerna för hantering av behörigheter. Syftet med översynen var att förbättra och säkerställa granskning av behörigheter och användare i Raindance.

Ekonomistaben har gjort en översyn av rutinerna för hantering av behörigheter och användare, bland annat har en total inventering av användare och behörigheter gjorts. I samband med inventeringen avslutades behörigheter för användare som slutat i landstinget eller fått andra arbetsuppgifter. Ekonomistaben har också infört tydliga grupperingar av de behörigheter som utfärdas, det finns till exempel en mall för vilken typ av behörighet en controller ska ha.

En rutin för årlig kontroll av utfärdade behörigheter har införts. Användare som inte varit inloggade de senaste 9 månaderna inaktiveras.

En formell rutin för behörighetskontroll kommer att inarbetas i den internkontrollplan som ekonomistaben utarbetar under hösten 2016.

2 Har landstingsstyrelsen tillsett att riktlinjer utarbetats för hur integrationer, som Landstings-IT har driftansvaret för, ska implementeras och dokumenteras?

I revisorernas rapport från 2012 rekommenderades landstingsstyrelsen att tillse att Landstings-IT utarbetar en formell rutin för hur jobb och scheman ska definieras samt ändras. Rekommendationen omfattade även att klarlägga ansvaret för övervakning av jobb och hantering av eventuella fel samt att detta ska följa en formaliserad rutin. Dessa rutiner kan med fördel definieras under implementeringen av det nya integrationsverktyget JBOSS och ingå i formella OLA(Operational level agreement)/SLA.

Landstingsstyrelsen svarade revisorerna, att Landstings-IT ska se över dagens rutiner och utarbeta riktlinjer för hur integrationer som Landstings-IT har driftansvaret för ska implementeras och dokumenteras (en ”integrationsstandard”) med syfte att förbättra och säkerställa hur automatisk och manuell övervakning, larmhantering samt felrapportering skall hanteras.

Landstings-IT har åtgärdat de brister som framfördes i revisorernas rapport från 2012. Det finns rutiner för hur integrationer, som Landstings-IT har ansvar för, ska implementeras och dokumenteras. ICC (Integration

Competence Center) är en funktion inom Landstings-IT som ansvarar för övervakning, larmhantering och felrapportering.

I revisorernas rapport framfördes vikten av att ha formella rutiner inom detta område. Landstings-IT har checklistor som ska följas i samband med integrationer och ”har sedan 2012 infört en ny integrationsplattform Biztalk.” När en integration ska tas i drift görs det specifikationer, utveckling och uppkoppling till Landstings-ITs övervakningssystem.

Ansvaret för att definitivt fastställa huruvida informationen gått från ett system till ett annat ligger dock på den verksamhet som använder systemet

3 Har landstingsstyrelsen säkerställt att agendan för driftsmöten, med IT-leverantören, innehåller formella stående avrapporteringspunkter med syfte att tillgodose en bättre uppföljning av drifts- och supportavtal med leverantören?

I revisionsrapporten från 2012 framfördes en rekommendation om att landstinget under sina driftsmöten med Logica, borde begära formella avrapporteringspunkter. Punkterna skulle exempelvis kunna innehålla:

1) Tillgänglighet av servrar och system,
2) Öppna, stängda och fortgående ärenden samt tid för åtgärd,
3) Faktisk prestanda och upplevd prestanda,
4) Genomgång av avsteg från avtal eller SLA:s.

Landstingsstyrelsen angav i sitt svar på revisorernas rapport att ekonomistaben ska utveckla agendan för nuvarande driftsmöten med formella stående avrapporteringspunkter med syfte att tillgodose en bättre uppföljning av drifts- och supportavtal med leverantören.

Ekonomistaben har formaliserat innehållet i de driftsmöten som man har med leverantören CGI (tidigare Logica) var sjätte vecka. Vid driftsmötena deltar också (sedan 2014) en representant från Landstings-IT. Vid mötena rapporteras, som fasta punkter, såväl proaktiva som reaktiva åtgärder. Rapporteringen omfattar systemets tillgänglighet, svarstider, planerade uppgraderingar och funktionalitet/driftstörningar. Vid driftsmötena förs tydliga protokoll där det bland annat framgår *vad* som har hänt, *vem* som har ansvar och vem som ska göra vad samt *när* det ska göras.

Det finns en rutin, om ej formellt fastställd, för mötesstrukturen på olika nivåer inom ”Förvaltningsobjekt Ekonomi” (Raindance). Av rutinen framgår vilka personer/funktioner som deltar vid respektive möten och vilka frågor som ska hanteras. Rutinen anger också vilken information som ska återkopplas till nästa nivå.

Fyra gånger per år träffas styrgruppen för ”Förvaltningsobjekt Ekonomi” där objektägaren (landstingets ekonomichef) och förvaltningsledaren (IT-chefen) deltar.

Sammanfattande slutsats och bedömning

Denna uppföljande granskning har visat att ekonomistaben åtgärdat de brister som iakttogs vid granskningen 2012. De införda rutinerna är dock inte formellt fastställda, men detta kan åtgärdas genom att inarbeta rutinerna i den internkontrollplan som ekonomistaben kommer att ta fram under hösten 2016.

Landstings-IT har åtgärdat de brister som framkom i den granskning som revisorerna lät genomföra år 2012.

Vår bedömning är således att åtgärder vidtagits med anledning av den kritik och de synpunkter som framkom i revisorernas granskning från 2012.

Johan Magnusson
Certifierad kommunal yrkesrevisor