Landstinget i Värmland

Granskning av generella IT-kontroller

Revisionsrapport

November 2012

Inledning

Granskningen av de generella IT-kontrollerna kring ekonomisystemet Raindance har påvisat ett antal observationer. Baserat på vår erfarenhet kring liknande uppdrag bedömer vi dock att Landstinget i Värmland har en god hantering samt förvaltning av sitt ekonomisystem. Enligt uppgift håller landstinget på att införa systemförvaltningsmodellen PM3. Ett arbete har påbörjats med konsolidering av de 600 verksamhetssystem som finns inom landstinget samt att utse objektsägare. Samtidigt har styrgrupper utsetts och förvaltnings-organisationer identifierats. Vi noterade att ekonomistaben redan innehar förvaltarrollen, vilket är en god förutsättning för införandet av PM3.

Kartläggningen av processen för programförändringar visade att ekonomistaben har en ändamålsenlig hantering. Behov kring utveckling/förändring fångas upp av verksamheten och leverantören. Erforderliga procedurer kring test och godkännande finns på plats.

Vad gäller processen för att hantera åtkomst till program och data finns det utrymme för förbättringar. Rutiner finns i dag på plats, dock behöver ekonomistaben formalisera samt dokumentera delar av hanteringen. IT-driften hanteras till stora delar av leverantören Logica och Landstings-IT. Backup-hanteringen bedöms som ändamålsenlig med undantag från larmhanteringen. Vad gäller de schemalagda jobben som går till och från Raindance, bedömer vi att ingen enhetlig hantering finns idag. I samband med att integrationsmotorn TEIS byts ut till JBOSS bör landstinget även se över rutinerna för sina schemalagda eller realtidsjobb.

Vidare bör ekonomistaben fortsätta med kartläggningen och dokumentationen av verksamhetsprocesserna samt även inkludera processerna kring programförändringar (Change management) och åtkomst (Access management). Detta bör ske i samarbete med Landstings-IT, vilka i dagsläget ser över möjligheterna att inkludera andra IT-processer så som release, problem, incident management, etc.

En observation som vi har gjort under vår granskning är att det inte finns formella SLA (Service Level Agreement) och OLA (Operational Level Agreement) upprättade mellan verksamhet, IT och ekonomi. Denna observation avser landstingets generella styrning och syftar till att tydliggöra ansvarfördelningen för respektive verksamhetsutövning. Som ett konkret exempel kopplat till denna granskning noterade vi att ansvaret för att lösa ett problem i samband schemalagda jobb, inte finns formellt definierat – d v s vad ska levereras, när övergår ansvaret och vem ska lösa problemet?

Nedan finner ni vår rapport som sammanfattar våra observationer, slutsatser och rekommendationer. Under avsnitt 6 presenteras även förslag på en fördjupad granskning kring applikationskontroller och registeranalyser.

Om ni har några frågor rörande denna rapport eller om det är något ytterligare vi kan hjälpa er med, tveka inte att kontakta oss. Slutligen vill vi passa på att tacka er för ett gott samarbete.

Ort & datum	Ort & datum
Amir Tehrani Projektledare	**Jon Arwidson** Uppdragsledare/kvalitetsansvarig

Innehållsförteckning

1. Bakgrund och Syfte

PwC har genomfört en granskning av generella IT-kontroller kring ekonomisystemet Raindance. Bakgrunden till denna granskning är att Landstinget i Värmlands revisorer i sin årliga riskbedömning och planering av revisionsåret bedömt att landstingets ekonomisystem bör granskas under 2012. Granskningen har avgränsats till IT-kontroller samt IT-risker som är kopplade till ekonomisystemet.

Denna granskning övergripande syfte är att granska ändamålsenligheten i de generella IT-kontrollerna med fokus på:

- Programförändring
- Systemutveckling
- Åtkomstkontroll
- IT-drift

Rapportstruktur

Vi har graderat de observationer som presenteras i denna rapport efter bedömd väsentlighet. Graderingen illustreras med hjälp av trafiksignaler. Även om graderingen ofrånkomligen är subjektiv och innehåller inslag av bedömningar och ställningstaganden kan definitionerna nedan vara vägledande.

Rött ljus åsätts en brist med så stor påverkan på system, processer eller intern kontroll att den kan medföra att Landstinget i Värmland exponeras för betydande förluster eller väsentliga fel i den finansiella rapporteringen.

Gult ljus åsätts en brist med påverkan på system, processer eller intern kontroll som kan medföra att Landstinget i Värmland exponeras för förluster eller betydande fel i den finansiella rapporteringen.

Grönt ljus åsätts mindre brister eller fel där risken för otillbörlig användning och/eller felaktigheter i bokföringen är lägre, men där det ändå bedöms finnas utrymme för förbättringar.

2. Granskningens omfattning och revisionskriterier

Vi har genomfört vårt uppdrag genom att belysa följande generella IT-kontroller för applikationen Raindance. Domänen *Systemutveckling* som finns med som en generell IT-kontroll har exkluderats från denna granskning då Raindance är ett standardsystem där utveckling sker av leverantören Logica. De utvecklingar som sker i systemet och som påverkar landstinget har validerats som en del av domänen *Programförändring*.

Område	Kontroller
Programförändring (PF)	1. Programförändringar till kritiska applikationer initieras genom formell begäran 2. Programförändringar testas och testresultat godkänns före driftsättning 3. Programförändringar som implementeras i produktionsmiljön godkänns före driftsättning fullständigt och riktigt 4. Begränsad åtkomst till produktionsmiljön för utvecklare
Åtkomstkontroll (ÅK)	1. Formella rutiner vid upplägg av nya användare eller ändringar i befintliga behörigheter 2. Periodisk genomgång av användare och deras respektive behörigheter 3. Säkerhetspolicy och rutiner finns definierade och dokumenterade 4. Kontroll och övervakning av åtgärder utförda av privilegierade användare
IT-drift (ID)	1. Kontroll att kritiska batch-jobb genomförs korrekt och fullständigt 2. Formella backup-rutiner finns upprättade
Tredjepartsleverantör (ID)	3. Tredjepartleverantören säkerställer leverans enligt avtal 4. Interna kontroller kring drift och förvaltning finns på plats

3. Tillvägagångssätt

Granskningen har genomförts under oktober 2012 främst genom intervjuer med representanter inom ekonomistaben på landstinget, Landstings-IT och tredjepartleverantören Logica. Vi har även som en del av granskningen erhållit stickprov/underlag som styrker kontrollernas utformning.

4. Sammanfattande observationer

Granskningen har resulterat i ett antal områden där vi anser att landstinget bör förbättra eller förstärka de interna IT-kontrollerna. Vi bedömer att ett antal kontrollmoment finns på plats och är ändamålsenliga. Våra observationer från granskningen sammanfattas i nedanstående tabell. Varje observation är graderad efter trafikljusmodellen beskriven på sidan 4. Referensnumret i denna tabell hänvisar till numrering i kapitlet ”Detaljerade observationer” på sidan 7.

#	Område	Observation	Riskgradering
ÅK2	Åtkomstkontroll	Landstinget saknar en formell kontroll kring periodisk genomgång av användarrättigheter och behörighet till Raindance.	
ID1	IT-drift	Ingen enhetlig rutin och larmhantering kring schemalagda batch-jobb.	
ID2	Tredjepartsleverantör	Ingen formell avrapportering kring avtalad leverans från leverantören Logica.	

5. Detaljerade observationer

I detta avsnitt sammanställs detaljerad information rörande de observationer som noterats, risker som är relaterade till observationen samt rekommenderad åtgärd.

Referens	ÅK2
Riskgradering	Medium
Område	Åtkomstkontroll
Observation	Det görs ingen formell regelbunden granskning av behörigheter för att verifiera att användare i Raindance har behörigheter som motsvarar arbetsuppgifter. Denna granskning syftar till att säkerställa att användare som tidigare erhållit behörighet till system och applikationer fortfarande har behov av tilldelad behörighet, och inte t.ex. har bytt funktion eller avdelning, eller har slutat vid landstinget.
Risk	Utan en regelbunden granskning av aktuella behörighetsnivåer ökar risken att användare har behörigheter som inte är aktuella för nuvarande arbetsuppgifter, eller att personen slutat vid landstinget. Därmed ökar risken för otillbörlig åtkomst och användning av Raindance.
Rekommendation	Vi rekommenderar att en formell rutin utformas för att regelbundet granska behörigheter 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.
Verksamhetsansvarigas kommentar	

Referens	ID1
Riskgradering	Medium
Område	IT-drift
Observation	I dagsläget finns schemalagda jobb definierade i verktyget TEIS och all larmhantering sker via e-post. Vi noterade dock att larmhanteringen inte är enhetligt definierad. Enligt uppgift finns det jobb som saknar larmhantering. Om exempelvis en fil saknas i samband med att jobbet ska genomföras, larmas inte de ansvariga.
Risk	Utan en formell rutin av schemalagda finansiellt signifikanta jobb ökar risken att finansiell data hanteras felaktigt i systemen. Utan en formell rutin med definierat ansvar för övervakning och problemlösning av sådana jobb ökar risken för att problem inte följs upp samt hanteras korrekt. Detta ökar risken för att riktigheten av finansiell data påverkas.
Rekommendation	Vi rekommenderar att Landstings-IT utarbetar en formell rutin för hur jobb och scheman ska definieras samt ändras. Vi rekommenderar även ett klarläggande av 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/SLA.
Verksamhetsansvarigas kommentar	

Referens	ID2
Riskgradering	Låg
Område	Tredjepartsleverantör
Observation	Vi noterade under granskningen att inga formella leveransrapporter finns att tillgå. Det framkom dock att driftsmöten hålls mellan landstinget och Logica men att dessa är informella samt att ingen rapportering sker kring leverans eller att en avstämning mot avtal eller SLA:s genomförs.
Risk	Utan en formell uppföljning kring supportavtal finns en ökad risk att landstinget inte erhåller de tjänster som man betalar för, enligt upprättade avtal.
Rekommendation	Vi rekommenderar landstinget att under sina driftsmöten med Logica, begära formella avrapporteringspunkter. Punkterna kan exempelvis innehålla: • Tillgänglighet av servrar och system • Öppna, stängda och fortgående ärenden samt tid för åtgärd • Faktisk prestanda och upplevd prestanda • Genomgång av avsteg från avtal eller SLA:s
Verksamhetsansvarigas kommentar	

6. Förslag på fördjupad granskning

Som en del av detta uppdrag har vi nedan föreslagit en fördjupad granskning med fokus på applikationskontroller i Raindance och registeranalyser på angränsande områden. Detaljerade kontroller och revisionskriterier inom respektive område ska specificeras i samband med projektets uppstart. Notera även att nedanstående förslag kring applikationskontroller kan ligga till grund för en mer djupgående genomgång av manuella rutiner samt arbetssätt hos landstingets ekonomifunktion om en sådan granskning önskas.

Bokslut

Här kartlägger vi ekonomisystemet i syfte att identifiera och verifiera ändamålsenligheten i automatiska kontroller inom följande områden; kontoplan, registrering bokföringsorder, verifikationsnummer samt öppning och stängning av redovisningsperioder. Som en förlängning av applikationskontroller och rutiner kan även registeranalyser genomföras på huvudbokstransaktionerna. Analysen omfattar följande:

- Bedöm fullständighet i erhållet material, jämför UB föregående år mot UB innevarande år
- Poster som inte balanserar, debet <> kredit
- Resultatpåverkande transaktioner över ett visst belopp
- Identifiering av användare som gjort manuella bokningar i huvudboken, beloppsackumulering per användare samt eventuell extrahering av detaljer för valda användare
- Poster som dateras bakåt/framåt i tiden
- Konton med fåtal/onormala bokningar
- Ovanliga bokningar; kundfordringar med motbokning annat än Kassa/Bank (likvidkonto)

Kundreskontra

Här ska vi skapa oss en förståelse för hur eller om kundreskontran används i verksamheten för att sedan identifiera och verifiera automatiska kontroller inom följande: uppdatering av fasta data såsom kundregister och prislistor, fakturering, betalningsmatchning samt överföring från reskontra till huvudbok. Även under detta område kan registeranalyser utföras. Analysen av kundreskontran omfattar följande:

- Betalningsuppföljning
- Åldersanalys
- Avvikande kredittider
- Medborgare med fordran på bolaget
- Fordringar krediterade/justerade efter årsskiftet

Leverantörsreskontra

Initialt kommer vi att skapa oss en förståelse för hur eller om leverantörsreskontran används i verksamheten för att sedan identifiera och verifiera automatiska kontroller inom följande: uppdatering av fasta data såsom leverantörsregister och prislistor, tre-vägsmatchningar, betalning och överföring från reskontra till huvudbok, etc. Registeranalyser inom leverantörsreskontran omfattar:

- Validering av leverantörsregistret mot leverantörsreskontran
- Inköpsvolym/omsättning per leverantör och matchning mot ramavtal
- Förekomst av dubbla, eller mer, leverantörsnummer och leverantörsnamn i leverantörsregistret
- Identifiering av höga fakturabelopp
- Analys av verifikationsnummer
- Förekomst av krediteringar – per faktura och på detaljnivå
- Identifiering av leverantörer där landstinget har en nettofordran på leverantören
- Åldersanalys av obetalda fakturor, i 30-dagarsintervall från bokslutsdatum och bakåt
- Dubbla utbetalningar, förekomst av dubbla poster avseende fakturanummer

Segregation of Duties (SoD)

En kartläggning av kritiska roller och funktioner kommer att ligga till grund för granskningen av Segregation of Duties (SoD) i ekonomisystemet. Granskningen kommer främst att fokusera på funktioner såsom godkännande/attest och registrering/genomförande av:

- Bokföringsorder
- Kundfakturor
- Leverantörsfakturor/leverantörsbetalning