Region Skåne

Granskning av IT-kontroller

Per Stomberg
Niklas Westerlund

Deloitte AB
Januari 2016

Innehållsförteckning

1. Sammanfattning

Enligt den revisionsplan som antagits för 2015 års redovisningsrevision ska Deloitte utföra en särskild granskning av IT-miljön inom Region Skåne.

Syftet har varit att utvärdera de kontroller och rutiner som omger de delar av IT-miljön som är centrala för Region Skånes kritiska processer kopplade till finansiell rapportering. De system som identifieras som mest kritiska för den finansiella rapporteringen och som valts ut för denna granskning är Region Skånes huvudsakliga ekonomisystem Raindance samt den personalrelaterade applikationen Personec P (del av HR Fönster).

Denna rapport innehåller en sammanställning av iakttagelser och förbättringsförslag avseende interna kontroller och rutiner inom Region Skåne kopplade till det granskade området.

Vår övergripande bedömning är att Region Skåne har tillfredsställande IT kontroller som stödjer den finansiella rapporteringen, dock har områden identifierats där Region Skåne ytterligare bedöms kunna förbättra sina rutiner och interna kontroller, vilka stödjer en tillförlitlig hantering av finansiell information. Följande huvudsakliga iakttagelser har noterats:

Enligt gällande rutiner när en medarbetare avslutar sin anställning alternativt byter arbetsuppgifter inom Region Skåne, ligger ansvaret hos medarbetarens chef att säkerställa att behörigheten i system uppdateras enligt de nya omständigheterna. Under vår granskning noterade vi att medarbetares behörighet i de aktuella systemen Raindance och Personec P inte konsekvent har avslutats vid anställningens avslut. Brister i rutinerna för att uppdatera användares behörigheter kontinuerligt kan innebära att personer bibehåller obehörig åtkomst till kritiska IT-system och information. Detta kan leda till otillbörlig spridning, manipulering eller otillgänglighet av finansiell information.

Gruppkonton med kraftfull behörighet används av leverantören i ekonomisystemet Raindance. Enligt praxis ska gruppkonton, i största möjliga mån, undvikas eftersom spårbarheten kring denna typ av konton är begränsad. Den potentiella risken, kopplat till dessa gruppkonton, har accepterats på lämplig ledningsnivå. Dock bör risknivån för dessa gruppkonton kontinuerligt utvärderas samt behovet avseende att implementera kompenserande rutiner för uppföljning av användningen av dess konton.

Det fordras endast ett godkännande i systemet Personec P för upplägg och ändring av löner. Därmed saknas en tvingande fyra-ögons-princip för attestering av upplägg och förändringar av löner. Avsaknad av tvingade systemkontroller medför ett ökat behov av manuella rutiner som säkerställer att samtliga förändringar sker enligt förväntande intentioner.

2. Inledning

2.1 Bakgrund och syfte

Enligt den revisionsplan som antagits för 2015 års redovisningsrevision ska Deloitte utföra en särskild granskning av IT-miljön inom Region Skåne.

Region Skåne är beroende av systemens funktionalitet p.g.a. höga transaktionsvolymer och kritiska gränssnitt mellan försystem och ekonomisystem. Därmed ställs krav på välutformade IT-kontroller. De system som identifieras som mest kritiskt för den finansiella rapporteringen och som valts ut för denna granskning är Region Skånes huvudsakliga ekonomisystem Raindance samt den personalrelaterade applikationen Personec P. Personec P är en del av de system som refereras till som HR Fönster av Region Skåne.

Granskningen av IT-kontroller har omfattat följande områden:

- **Åtkomstkontroll** – Rutiner och systeminställningar för hur det säkerställs att ingen obehörig person kommer åt känslig information. Vidare att kontroller finns för att information endast är tillgänglig för den som behöver den för att kunna utföra sina arbetsuppgifter samt att spårbarhet finns till unika användare.

- **Drift av IT system** – Att befintliga driftsrutiner stödjer en fullständig och korrekt bearbetning av finansiell data. Det här omfattar exempelvis säkerhetskopiering av information och övervakning av schemalagda jobb.

- **Systemunderhåll –** Att förändringar av applikationer utförs på ett sätt som syftar till att säkerställa att informationen i systemen är fullständig, korrekt och tillgänglig.

2.2 Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser, slutsatser och bedömningar avseende processer och rutiner som har granskats. Följande revisionskriterier har använts i denna granskning:

- Lagen om Kommunal Redovisning
- Best practices för intern kontroll inom IT-området

2.3 Metod och genomförande

Granskningen har genomförts genom platsbesök på Region Skånes kontor i Kristianstad samt i Malmö. Granskningen har genomförts främst genom intervjuer med personer som administrerar, övervakar och underhåller systemen. Vidare har relevant dokumentation inhämtas som verifierar de diskussioner som genomförts.

3. Granskningsområden

3.1 Raindance

3.1.1 Åtkomstkontroll

För att få tillgång till ekonomisystemet Raindance krävs det en separat inloggning på applikationsnivå. Det finns en formell rutin för tilldelning av behörigheter till Raindance.

En behörighetsblankett fylls i där det definieras vilken roll användaren ska erhålla samt om användaren ska erhålla sak- och beslutsrättigheter för att kunna godkänna fakturor i systemet. Användarens närmaste chef godkänner förfrågan genom att signera blanketten. Behörighetsblanketten vidarebefordras till Raindance behörighetsgruppering, som ansvarar för att verkställa behörighetsförfrågan i systemet. Genom denna rutin uppnås en arbetsfördelning mellan godkännande och verkställande av behörighetsförändringar. Vi bedömer att denna rutin fungerar tillfredsställande.

Det har genomförts en genomlysning avseende åtskild ansvars- och arbetsuppgiftsfördelning avseende rolluppsättningen (Segregation of duties) inom Raindance, som påvisar att det inte finns behörighetskonflikter inom definierade roller. Eftersom användare endast kan bli tilldelad en roll i Raindance uppnås en tillfredställande ansvars- och arbetsuppgiftsfördelning. I kommande uppdatering av Raindance möjliggörs alternativ för en användare att erhålla fler än en behörighetsroll i Raindance. Vi rekommenderar Region Skåne att ta detta i beaktande för att även fortsättningsvis bibehålla en tillfredställande ansvars- och arbetsuppgiftsfördelning för användare.

Iakttagelse: När en medarbetare avslutar sin anställning alternativt byter arbetsuppgifter inom Region Skåne, ligger ansvaret hos medarbetarens chef att säkerställa att behörigheten i system uppdateras enligt de nya omständigheterna. Under vår granskning noterade vi att medarbetares behörighet i Raindance inte konsekvent har avslutats vid anställningens avslut.

Vi noterade dock att den centrala behörighetsgruppen kontinuerligt tillhandahåller behörighetslistor till respektive förvaltningsansvariga som granskar behörigheter för sina medarbetare och bedömer behörigheterna utifrån arbetsuppgifter. Signerade listor returneras till behörighetsfunktionen, som uppdaterar behörigheterna enlig

förvaltningsansvarigas återkoppling. I samband med dessa användarinventeringar är det möjligt att fånga upp användare som har avslutat sin anställning alternativt bytt arbetsuppgifter, för att säkerställa att behörigheterna avslutas alternativ uppdateras för att reflekterar nuvarande arbetsuppgifter.

Potentiell konsekvens: Brister i rutiner för att uppdatera användarbehörigheter kontinuerligt kan innebära att personer bibehåller otillbörlig åtkomst till kritiska IT-system och information. Detta kan ge leda till otillbörlig spridning, manipulering eller otillgänglighet av finansiell information.

Vi rekommenderar att Region Skåne stärker den nuvarande rutinen för att säkerställa att användares behörighet uppdateras eller avslutas inom rimlig tid, på begäran av dennes chef.

Iakttagelse: Supporten av Raindance tillhandahålls av leverantören CGI. Leverantören har tilldelas kraftfull behörighet i systemet Raindance för att kunna genomföra sina arbetsuppgifter. Vi noterade under vår granskning att leverantören har fortlöpande tillgång till Raindance genom två gruppkonton. Med gruppkonton avses tillgång som inte direkt kan kopplas till en unik användare.

Potentiell konsekvens: Användandet av gruppkonton, särskilt med kraftfulla behörigheter, begränsar möjligheten för att upprätthålla spårbarhet gällande förändringar då en unik identifierare saknas. Utan spårbarhet kan oegentligheter såsom medveten eller omedveten förändring av kritisk information bli svår att utreda då utförd ändring inte kan kopplas till en specifik individ.

Enligt praxis ska gruppkonton, i största möjliga mån, undvikas. Riskerna som är kopplade till användning av gruppkonton med kraftfulla behörigheter har kommunicerats till lämplig ledningsnivå, där man har tagit ställning till och accepterat den potentiella risken kopplat till detta. Vi rekommenderar Region Skåne att kontinuerlig utvärdera risknivå, kopplade till gruppkonton, om denna förändras. Denna utvärdering samt beviljade undantag bör formellt dokumenteras och godkännas. Vidare bör det utredas vilken typ av kompenserande rutiner som kan implementeras, såsom loggning av kritiska förändringar som sker genom användandet av dessa konton.

Iakttagelse: Avseende lösenordsparameterar i systemet Raindance noterades en brist i utformningen. Vi noterade följande avvikelser gentemot våra rekommendationer: längd på lösenord 6 tecken, inga komplexitetskrav, lösenordshistorik 3 samt antal felaktiga försök innan användarens konto spärras.

Potentiell konsekvens: Bristande krav på lösenords utformning, varaktighet och i förlängningen användning av svaga lösenord medför ökad risk för otillbörlig tillgång och/eller manipulation av finansiell och verksamhetskritisk data.

Baserat på ovanstående lösenordsparameterar rekommenderar vi följande inställningar: längd på lösenord 8 tecken, komplexitetskrav, lösenordshistorik 6 samt 3-6 felaktiga inloggningsförsök innan användarens konto spärras.

På grund av tekniska begränsningar är det för närvarande inte möjligt att aktivera komplexitetskrav på lösenord för inloggning i Raindance. Vidare måste användare vara

inloggade på Region Skånes IT-miljö för att kunna få tillgång till Raindance. För att logga in på Region Skånes IT-miljö fordras lösenord som styrs via Windows Active Directory. Detta skalskydd minskar den potentiella risken som de nuvarande lösenordsinställningarna medför.

Vi rekommenderar Region Skåne att utvärdera möjligheter för att förstärka de nuvarande lösenordskraven för Raindance. För närvarande utvärderar man möjligheten att implementera en Single-Sign-On-lösning där inloggningen till Raindance och därmed även lösenordsinställningarna skulle styras via Windows Active Directory. Denna lösning skulle förstärka lösenordsinställningar för Raindance.

3.1.2 Drift av IT system

Vi har granskat rutinen kring schemalagda jobb för Raindance. Vi har noterat att det finns en process för att definiera, förändra och övervaka schemalagda jobb för Raindance.

Iakttagelse: Vi noterade att det finns en teknisk övervakning för schemalagda jobb som notifierar avseende utfallet för de schemalagda jobben samt att det finns definierade användare som är ansvariga att följa upp och åtgärda eventuella fel för schemalagda jobb. Däremot noterade vi att det finns en begränsad spårbarhet kring vilka aktiviteter som har genomförts för att korrigera de felaktigheter i schemalagda jobb som uppmärksammats.

Potentiell konsekvens: Avsaknad eller brister i rutinen för övervakning och problemlösning av schemalagda jobb ökar risken för att problem inte följs upp samt hanteras korrekt inom rimlig tid och att schemalagda jobb därmed inte bearbetas enligt förväntan. Detta ökar risken för att riktigheten av finansiell data påverkas.

Vi rekommenderar Region Skåne att utvärdera möjligheterna att stärka den nuvarande rutinen för övervakning av schemalagda överföringar genom en förbättrad spårbarhet kring vilka aktiviteter som vidtagits för att korrigera uppkomna felaktigheter.

Iakttagelse: Under granskningen kunde vi inte verifiera att användare som har möjlighet att förändra schemalagda jobb är begränsade i tillräcklig omfattning. Den nuvarande strukturen i Raindance, medför vissa tekniska svårigheter att begränsa antalet användare som har tillgång till att göra förändringar i schemalagda jobb.

Potentiell konsekvens: Avsaknad eller brister i rutinen för att tilldelning av behörigheter som ger möjlighet att genomföra förändringar avseende schemalagda jobb ökar risken för felaktiga förändringar i produktionsmiljön som kan påverka riktigheten av finansiell data.

Vi rekommenderar Region Skåne att analysera den nuvarande rutinen för att ge användare behörigheter som medför möjlighet att genomföra förändringar avseende schemalagda jobb. Detta för att kunna utvärdera möjligheten att begränsa antalet användare med möjlighet att genomföra förändringar i schemalagda jobb.

3.1.3 Systemunderhåll

Systemet Raindance är ett standardsystem som tillhandahålls och utvecklas av leverantören CGI. Vi noterade att det finns en process inom Region Skåne för att erhålla information avseende krav och önskemål på ny funktionalitet inom Raindance. Region Skåne har en användarförening för Raindance. Det är användarföreningen som prioriterar och beställer ny funktionalitet för Raindance av leverantören. Vi uppmärksammade att det regelbundet följs upp vilka beställningar som gjorts samt vilka beställningar som levererats.

Applikationsutvecklingen för Raindance hanteras av leverantören CGI, som även testar och kontrollerar versionerna innan de skickas till Region Skåne. CGI:s testmetodik tillämpas och dokumenteras, vi har inte tagit del av denna dokumentation under granskningen.

Region Skåne genomför acceptantstester för förändringar som utvecklas av leverantören. Detta för att säkerställa att de nya förändringarna är anpassade i tillräcklig utsträckning för att uppfylla Region Skånes behov och krav. Vi har tagit del av resultat för ett urval av acceptanstester som genomförts under 2015.

Iakttagelse: En fortlöpande dialog sker mellan Region Skåne och de leverantörer som är involverade i applikationsutvecklingen och produktionssättning av nya förändringar. I dialogen säkerställer man att tillräckliga tester av förändringar har genomförts och att de nya förändringarna kan implementeras i produktionsmiljön. Vi noterade att spårbarheten kring denna dialog och dess utfall kan formaliseras ytterligare.

Potentiell konsekvens: Avsaknad av eller ofullständig testdokumentation kan utgöra tecken på vissa brister i testprocessen vilket kan resultera i att fel i nya funktioner inte upptäcks.

Vi rekommenderar Region Skåne att förstärka den nuvarande förändringshanteringen genom att kritiska beslutsmoment dokumenteras adekvat. Detta för att säkerställa att tester av nya förändringar har genomförts enligt förväntan samt öka spårbarheten kring vilka besluts som fattas inom förändringshanteringsprocessen.

3.2 Personec P

3.2.1 Åtkomstkontroll:

Systemet Personec P är ett standardsystem som tillhandahålls och utvecklas av leverantören Aditro (från 1/1 2016 Visma Enterprise). Det finns en formell rutin för tilldelning av behörigheter till Personec P. Medarbetare i Region Skåne rapporterar b.la. närvaro, frånvaro och resor i systemet Personec P.

I Personec P finns det ett antal roller med kritiska behörigheter med avseende för den finansiella rapporteringen. Dessa roller är HR-funktion, Chef, Chefsstöd, Ekonomifunktion, Löneadministratör och Systemförvaltare. Det är dessa roller som varit i fokus för denna granskning.

Medarbetare blir tilldelade en roll i systemet Personec P i samband med anställning eftersom det specificeras vilka behörigheter medarbetare behöver för att utföra sina arbetsuppgifter. För att erhålla rollen chef fylls en blankett i som närmaste chef godkänner och denna skickas till ansvarig person för HR Fönster vid respektive förvaltning för granskning. När granskning är utförd skickas blanketten till behörighetsgrupperingen som ansvarar för att verkställa behörigheter i systemet. Det är modulen Neptune som används för att lägga till nya behörigheter i Personec P. Vi noterade att tillgången till Neptune är begränsad till behörighetsgrupperingen. Genom denna rutin uppnås en arbetsfördelning mellan godkännande och verkställande av behörighetsförändringar. Denna rutin förefaller fungera tillfredställande.

Iakttagelse: När en medarbetare avslutar sin anställning alternativt byter arbetsuppgifter inom Region Skåne, ligger ansvaret hos medarbetarens chef att säkerställa att behörigheten i system uppdateras enligt de nya omständigheterna. Under vår granskning noterade vi att medarbetares behörighet i Personec P inte konsekvent har avslutats vid anställningens avslut.

Vi noterade dock att den centrala behörighetsgruppen kontinuerligt tillhandahåller behörighetslistor till respektive förvaltningsansvariga som granskar behörigheter för sina medarbetare och bedömer behörigheterna utifrån arbetsuppgifter. Signerade listor returneras till behörighetsfunktionen, som uppdaterar behörigheterna enligt förvaltningsansvarigas återkoppling. I samband med dessa användarinventeringar är det möjligt att fånga upp medarbetare som har avslutat sin anställning alternativt bytt arbetsuppgifter, för att säkerställa att behörigheterna avslutas alternativt uppdateras för att reflekterar nuvarande arbetsuppgifter.

Potentiell konsekvens: Brister i rutinerna för att uppdatera behörigheter kontinuerligt kan innebära att personer bibehåller obehörig åtkomst till kritiska IT-system och information. Detta kan ge leda till otillbörlig spridning, manipulering eller otillgänglighet av finansiell information.

Vi rekommenderar att Region Skåne stärker den nuvarande rutinen för att säkerställa att användares behörighet uppdateras eller avslutas inom rimlig tid, på begäran av dennes chef.

Iakttagelse: Upplägg och förändringar av medarbetares löner sker i systemet Personec P. Upplägg och förändringar av löner kan genomföras av medarbetare med rollen HR-funktion eller med rollen Löneadministratör efter påskrivet underlag av berörd chef. Vi noterade att det endast fordras ett godkännande i systemet för upplägg och förändring av löner. Därmed saknas en tvingande fyra-ögons princip för attestering av upplägg och förändringar av löner. Dock loggas upplägg och förändringar i systemet samt följs kostnader upp regelbundet av chef och ekonom.

Eftersom det inte finns tvingade kontroller i systemet Personec P som fordrar att två personer är involverade i upplägg och förändring av löner, rekommenderar vi att Region Skåne säkerställer att det finns tillräckliga manuella rutiner som säkerställer att samtliga förändringar sker enligt förväntande intentioner.

4. Slutsats

Vår övergripande bedömning efter genomförd granskning är att Region Skåne har tillfredsställande IT-kontroller som stödjer den finansiella rapporteringen.

Vi har identifierat ett antal områden där förbättringar är påkallade med varierande angelägenhetsgrad.

- För de system som har omfattas av granskningen, Raindance och Personec P har i samtliga fall användares behörigheter inte avslutats inom rimlig efter avslutad anställning. Därmed bör den nuvarande rutinen förstärkas för att säkerställa att användares behörighet avslutas inom rimlig tid efter avslutad anställning.

- Gruppkonton med kraftfull behörighet används av leverantören i ekonomisystemet Raindance. Enligt praxis ska gruppkonton, i största möjliga mån, undvikas eftersom spårbarheten kring denna typ av konton är begränsad. Den potentiella risken, kopplat till dessa gruppkonton, har accepterats på lämplig ledningsnivå. Vi rekommenderar Region Skåne att kontinuerligt utvärdera risknivå, kopplad till dessa gruppkonton samt att utreda behovet avseende att implementera kompenserande rutiner.

- Avseende lösenordsparameterar i systemet Raindance noterades en brist i utformningen. I nuläget är det inte möjligt att definiera lösenordsparametrar så att de uppfyller best-practice krav. För närvarande utvärderas möjligheten att implementera en Single-sign on lösning var inloggningen till Raindance och därmed även lösenordsinställningarna styrs via Windows Active Directory. Denna lösning skulle förstärka lösenordsinställningar för Raindance.

- Det finns en begränsad spårbarhet kring vilka aktiviteter som vidtagits för att korrigera felaktigheter i schemalagda jobb för Raindance. Region Skåne bör utvärdera möjligheten att stärka den nuvarande rutinen för övervakning av schemalagda jobb genom en förbättrad spårbarhet kring vilka aktiviteter som vidtagits för att korrigera uppkomna felaktigheter.

- Vi kunde inte verifiera att antalet användare som har möjlighet att göra förändringar för schemalagda jobb för Raindance har begränsats i tillräcklig utsträckning. Region Skåne bör utvärdera möjligheten att begränsa antalet användare som har möjlighet att göra förändringar för schemalagda jobb.

- Det finns en definierad förändringshanteringsprocess för att implementera nya förändringar för Raindance. Det genomförs en fortlöpande dialog mellan Region Skåne och de leverantörer som är involverade i applikationsutvecklingen och produktionssättning av nya förändringar. I dialogen säkerställer man att tillräckliga tester av förändringar har genomförts och att de nya förändringarna kan implementeras i produktionsmiljön. Vi noterade att spårbarheten kring denna dialog och dess utfall kan formaliseras ytterligare. Detta för att säkerställa att tester av nya förändringar har genomförts enligt förväntan samt öka spårbarheten kring vilka beslut som fattas inom förändringshanteringsprocessen.

- Det fordras endast ett godkännande i systemet Personec P för upplägg och ändring av löner. Därmed finns det inte en tvingande fyra-ögons princip för attestering av upplägg och förändringar av löner. Upplägg och förändringar loggas i systemet och att kostnader följs upp regelbundet av chef och ekonom. Avsaknad av tvingade kontroller som fordrar att två personer är involverade i uppsättning av löner, ökar behovet av att det finns tillräckliga manuella rutiner som säkerställer att samtliga förändringar sker enligt förväntande intentioner.