Deloitte.

Region Skåne

Granskning av IT-kontroller

Deloitte AB
Januari 2019

Innehållsförteckning

1. Sammanfattning

I enlighet med den revisionsplan som antagits för 2018 års redovisningsrevision har Deloitte utfört 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).

Rapporten innehåller en sammanställning av iakttagelser och förbättringsförslag avseende interna kontroller och rutiner inom Region Skåne kopplade till det granskade området. Under årets granskning har förbättringsområden som identifierades i 2015 års granskning följts upp.

Utifrån intervjuer och inhämtat material är vår övergripande bedömning att Region Skåne har fungerande processer och kontroller avseende Raindance och Personec P. Vi har dock noterat förbättringsområden avseende verksamhetens IT-kontroller kopplat till Raindance och Personec P. Områden för förbättring, i syfte att stödja en tillförlitlig hantering av finansiell information, specificeras i sektion 3 och sammanfattas nedan uppdelade per riskområde. De förbättrings-områden som identifierades i 2015 års granskning har inte kunnat konstateras åtgärdade vid årets granskning.

Övergripande kontrollmiljö

- Vi rekommenderar Region Skåne att implementera formella och avtalade krav avseende leveransen från CGI (leverantören som underhåller Raindance) samt implementera formella rutiner för uppföljning av leveransen. Vi är informerade att ett projekt pågår hos Region Skåne att uppdatera samtliga kontrakt avseende utlagd verksamhet och att kravställningen är planerad till nästa uppdatering av avtalet.

Åtkomstkontroll

Fem rekommendationer har identifierats inom området för åtkomstkontroll och sammanfattas nedan.

- Vi rekommenderar att Region Skåne och CGI fortsätter på inslagen väg att ersätta gruppkonton med individuella och unika konton för Raindance. 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, om kontona ej tas bort, bör det utredas vilken typ av kompenserande rutiner som kan implementeras, såsom loggning av kritiska förändringar som sker genom användandet av dessa konton. Vi rekommenderar även Region Skåne att etablera en kravställning i syfte att kontrollera vilka personer hos leverantören som har tillgång till gruppkonton.
- 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

- 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. Vi rekommenderar Region Skåne att utvärdera möjligheten att införa en automatisk kontroll av borttag när en person avslutar sin anställning, alternativt att en central HR-process informerar behörighetsadministrationen för Raindance att en behörighet ska avslutas.
- Vi rekommenderar att följande lösenordsinställningar implementeras: längd på lösenord 8 tecken, komplexitetskrav, lösenordshistorik 6 samt 3-6 felaktiga inloggningsförsök innan användarens konto spärras och att lösenord förfaller inom 90 dagar.
- Vi rekommenderar Region Skåne att säkerställa efterlevnad av den årliga rutinen som avser godkännande av rolluppsättningen i Raindance. Om det inte kan undvikas att konflikter tilldelas för en användare bör lämpliga begränsande åtgärder kartläggas mot användaren och testas regelbundet.

Drift av IT-system

En rekommendation har identifierats inom området för drift av IT system.

- 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.

Systemunderhåll

En rekommendation har identifierats inom området för systemunderhåll.

- Vi rekommenderar Region Skåne att utvärdera möjligheterna att stärka den nuvarande rutinen för förändringshantering och öka spårbarhet kring vilka aktiviteter som vidtagits hos underleverantören för att säkerställa att förändringar implementeras korrekt.

2. Inledning

2.1 Bakgrund och syfte

Enligt den revisionsplan som antagits för 2018 års redovisningsrevision skulle en särskild granskning av IT-miljön inom Region Skåne utföras.

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

- Good practice för intern kontroll inom IT-området

2.3 Metod och genomförande

Granskningen har genomförts av Felix Baart genom platsbesök på Region Skånes kontor i Kristianstad samt genom Skypemöten. 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.

Faktagranskning av sakuppgifter har genomförts av de personer som varit föremål för intervjuer vid granskningen.

3. Granskningsområden

3.1 Raindance

Raindance underhålls av underleverantören CGI som sköter drift och systemunderhåll utifrån uppsatta processer. Även om systemets drift och underhåll är outsourcad bör kontroller som Region Skånes interna regelverk framställer även följas av CGI. Region Skåne bör även ha formella processer för att säkerställa att CGI efterlever Region Skånes kravställning. Definition av kontrollerna och relaterad uppföljning bör finnas avtalat mellan Region Skåne och CGI.

Iakttagelse: Formell kravställning i form av avtal har inte upprättats av Region Skåne för att säkerställa att CGI utför de kontroller som är nödvändiga enligt Region Skånes behov och förutsättningar för att ändamålsenligt hantera risken för fel i den finansiella rapporteringen. Därmed minskar möjlighet till formell uppföljning av Region Skånes kontroller som är utlagda hos tredje part.

Potentiell konsekvens: Vid avsaknad av formellt kravställande ökar risken för att Region Skånes IT-relaterade risker inte hanteras ändamålsenligt och minskar Region Skånes insyn och kontroll av den utlagda verksamheten.

Rekommendation: Vi rekommenderar Region Skåne att implementera formella och avtalade krav avseende leveransen till CGI samt implementera formella rutiner för uppföljning av leveransen. Vi är informerade att ett projekt pågår hos Region Skåne att uppdatera samtliga kontrakt avseende utlagd verksamhet och att kravställningen är planerad till nästa uppdatering av avtalet.

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 är ändamålsenligt utformad.

Iakttagelse: Supporten av Raindance tillhandahålls av leverantören CGI. Leverantören har tilldelats 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. Vi är informerade om att Region Skåne och CGI avser att ta bort gruppkontona.

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.

Rekommendation: Vi rekommenderar att Region Skåne och CGI fortsätter på inslagen väg att ersätta gruppkonton med individuella och unika konton för Raindance.

Iakttagelse: När en medarbetare avslutar sin anställning alternativt byter arbetsuppgifter inom Region Skåne, ansvarar medarbetarens chef för att behörigheten i system uppdateras enligt de nya omständigheterna. Region Skåne förlitar sig även på den årliga behörighetsgenomgången för borttagsprocessen. Däremot saknas automatisering av borttag av behörigheter i Raindance. Iakttagelsen noterades i 2015 års granskning och vi är informerade att processuppdateringar ej genomförts.

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 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 reflektera nuvarande arbetsuppgifter.

Rekommendation: 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. Vi rekommenderar Region Skåne att utvärdera möjligheten att införa en automatisk kontroll av borttag när en person avslutar sin anställning, alternativt att en central HR-process informerar behörighetsadministrationen för Raindance att en behörighet ska avslutas.

Iakttagelse: Lösenordsparametrar i systemet Raindance är inte ändamålsenligt utformade. Vi noterade avvikelser mot följande inställningar som vi anser bör användas: längd på lösenord 6 tecken, inga komplexitetskrav, lösenordshistorik 3, och antal felaktiga försök innan användarens konto spärras.

En användare måste 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. Windows Active Directory används av Region Skåne som inloggnings- och autentiseringsmekanism för åtkomst till sitt generella användarkonto och Region Skånes nätverk. Detta skalskydd minskar den potentiella risken som de nuvarande lösenordsinställningarna medför.

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

Rekommendation: 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.

Vi är informerade att Region Skåne är i slutfasen av en process att implementera Single-Sign-On där inloggningen till Raindance styrs av det centrala nätverkssystemet Active Directory. Lösningen för Single-Sign-On kommer att kräva multifaktorsautentisering med kort och kod, vilket skulle förstärka lösenordsinställningarna för Raindance.

Det ska enligt Region Skånes processer genomföras en genomgång avseende åtskild ansvars- och arbetsuppgiftsfördelning avseende rolluppsättningen (Segregation of duties) inom Raindance, som påvisar att det inte finns behörighetskonflikter inom definierade roller. Såsom att en användare med behörighet att ändra en leverantörs bankkontoinformation inte har behörighet att boka en utbetalning. Däremot har inte rolluppsättningen gåtts igenom eller godkänts av Ekonomidirektör under 2018. En användare kan bli tilldelad flera roller i Raindance, och vid tilldelning kontrolleras att användarens tilldelade roller inte orsakar en konflikt.

Iakttagelse: Rolluppsättningen i Raindance har inte gåtts igenom eller godkänts av Ekonomidirektören under 2018 enligt uppsatta riktlinjer.

Potentiell konsekvens: Otillräcklig kontroll avseende rollkonflikter höjer risken att användare har behörigheter och kan genomföra handlingar som överskrider kontroller uppsatta i systemmiljön.

Rekommendation: Vi rekommenderar Region Skåne att säkerställa efterlevnad av den årliga rutinen som avser godkännande av rolluppsättningen i Raindance. Om det inte kan undvikas att konflikter tilldelas för en användare bör lämpliga begränsande åtgärder kartläggas mot användaren och testas regelbundet.

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.

Rekommendation: 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.

3.1.3 Systemunderhåll

Systemet Raindance är ett inköpt och standardiserat system 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. 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.

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.

Rekommendation: 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 Visma. Medarbetare i Region Skåne rapporterar b.la. närvaro, frånvaro och resor i systemet Personec P, och samtliga medarbetare har ett konto med grundbehörigheter.

I Personec P finns det ett antal roller med kritiska behörigheter avseende den finansiella rapporteringen. Dessa roller är HR-funktion, Chef, Chefsstöd, Ekonomifunktion, Löneadministratör och Systemförvaltare. De nämnda rollerna har varit i fokus för granskningen.

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 roller med högre behörighet fylls en blankett i som närmaste chef godkänner och denna skickas till ansvarig person för HR Fönster vid respektive förvaltning för tilldelning av behörigheten. 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. Rutinens uppsättning bedöms som ändamålsenlig.

Iakttagelse: Support av Personec P tillhandahålls av Visma och Tieto. Båda leverantörerna har tilldelats kraftfull behörighet i systemet Personec P för att kunna genomföra sina arbetsuppgifter. Vi noterade under vår granskning att leverantörerna har fortlöpande tillgång till Personec P genom gruppkonton. Underleverantörerna använder gruppkontona i syfte att starta och kontrollera beslutade körningar. 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.

Rekommendation: Enligt praxis ska gruppkonton, i största möjliga mån, undvikas. 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, om kontona ej tas bort, bör det utredas vilken typ av kompenserande rutiner som kan implementeras, såsom loggning av kritiska förändringar som sker genom användandet av dessa konton. Vi rekommenderar även Region Skåne att etablera en kravställning i syfte att kontrollera vilka personer hos leverantören som har tillgång till gruppkonton.

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 och kostnader följs upp regelbundet av chef och ekonom.

Potentiell konsekvens: Bristen av tvingande dualitet i systemet ökar risken för att felaktiga löneförändringar och –utbetalningar genomförs.

Rekommendation: 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.

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. Borttag av behörigheter är även beroende utav behörighetsgenomgångar som ska göras av ansvariga chefer. Kontrollen är manuell och det finns risk för fel om inte närmaste chef anmäler att borttag ska ske för systemet. Kravställningen för genomgångar specificerar att samtliga behörigheter alltid ska vara korrekta, däremot inte med utsatta tidsintervall och det följs inte upp ifall en chef har genomfört genomgången.

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 leda till otillbörlig spridning, manipulering eller otillgänglighet av finansiell information.

Rekommendation: Vi rekommenderar Region Skåne att undersöka möjligheten att implementera en automatisk kontroll för borttag av behörigheter om anställda avslutar sin anställning. Vi rekommenderar även att implementera en uppföljningskontroll av behörighetsgenomgångarna för att säkerställa genomförandet.

Iakttagelse: Om en användare är tilldelad fler än 2 behörigheter till Personec P kopplas inte den behörigheten till Windows Active Directory och Personec Ps egna lösenordsinställningar styr inloggningen. Vi noterade avvikelser mot följande inställningar som vi anser bör användas : längd på lösenord 6 tecken, inga komplexitetskrav, lösenordshistorik 1 och lösenord förfaller inte.

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

Rekommendation: Baserat på ovanstående lösenordsparameterar rekommenderar vi följande inställningar: längd på lösenord 8 tecken, komplexitetskrav, lösenordshistorik 6, och att lösenord förfaller inom 90 dagar.

4. Slutsats

Vi har genomfört granskningen genom intervjuer med nyckelpersoner och inhämtat material som stödjer intervjuerna och kontrollutformningen. På en övergripande nivå har Region Skåne fungerande processer och kontroller på plats. Förbättringsområden som identifierades i 2015 års granskning har inte kunnat konstateras åtgärdade utifrån genomgångar och erhållet material. Förbättringsområden som framkommit vid granskningen sammanfattas nedan.

- Formell kravställning i form av avtal har inte upprättats av Region Skåne för att säkerställa att CGI utför de kontroller som är nödvändiga enligt Region Skånes behov och förutsättningar för att ändamålsenligt hantera risken för fel i den finansiella rapporteringen. Därmed minskar möjlighet till formell uppföljning av Region Skånes kontroller som är utlagda hos tredje part.

- Gruppkonton med kraftfull behörighet används av leverantören i ekonomisystemet Raindance och HR-systemet Personec P. Enligt praxis ska gruppkonton, i största möjliga mån, undvikas eftersom spårbarheten kring denna typ av konton är begränsad.

Vi rekommenderar Region Skåne att kontinuerligt utvärdera risknivå kopplad till dessa gruppkonton, utvärdera om de ska tas bort, och utreda behovet avseende att implementera kompenserande rutiner.

- 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 kostnader följs upp regelbundet av chef och ekonom. Avsaknad av tvingande 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.

- 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 2015 noterade vi att medarbetares behörighet i de aktuella systemen Raindance och Personec P inte konsekvent har avslutats vid anställningens avslut. Vi är informerade att inga ytterligare åtgärder är vidtagna sedan föregående granskning för att säkerställa att behörighetsborttag skett korrekt.

- 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 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.

- Avseende lösenordsparameterar i systemet Raindance noterades en brist i utformningen och de uppfyller inte best-practice-krav. I Personec P träder systemets egna lösenordsinställningar i kraft för användare som har fler än 2 behörigheter. Personec Ps inställningar uppfyller ej best practice-krav.

- Det ska enligt Region Skånes processer genomföras en genomgång avseende åtskild ansvars- och arbetsuppgiftsfördelning avseende rolluppsättningen (Segregation of duties) inom Raindance på årlig basis. Rolluppsättningen i Raindance har inte gåtts igenom eller godkänts av Ekonomidirektören under 2018.