Eva Tency Nilsson
Yrkesrevisor
Certifierad kommunal revisor
044-309 33 07
evatency.nilsson@skane.se

Fredrik Ljunggren
Yrkesrevisor
Certifierad kommunal revisor
040-675 30 57
fredrik.ljunggren@skane.se

Datum 2019-02-14
Dnr 1802181

Ekonomidirektör Lars-Åke Rudin
Processledare Peter Back

Granskning av IT-kontroller (rapport nr 12 - 2018)

Deloitte AB har på revisorernas uppdrag och som ett led i redovisnings-revisionen genomfört en 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).

I bifogad rapport redovisas resultatet av granskningen. Den sammanfattande bedömningen är att Region Skåne har fungerande processer och kontroller avseende Raindance och Personec P. Deloitte har dock noterat förbättrings-områden avseende verksamhetens IT-kontroller kopplat till både Raindance och Personec P. De förbättringsområden som identifierades i 2015 års granskning har inte heller kunnat konstateras åtgärdade vid årets granskning.

I granskningen presenteras flera förbättringsområden men nedan lyfts rekommendationerna inom övergripande kontrollmiljö och åtkomstkontroll:

- Att Region Skåne implementerar formella och avtalade krav avseende leverans från CGI (leverantören som underhåller Raindance) samt implementerar formella rutiner för uppföljning av leveransen. Det pågår ett projekt hos Region Skåne med att uppdatera samtliga kontrakt avseende utlagd verksamhet där denna kravställning är planerad till nästa uppdatering av avtalet.

- Att Region Skåne och CGI fortsätter på inslagen väg att ersätta gruppkonton med individuella och unika konton för Raindance. Risknivå kopplad till gruppkonton bör kontinuerligt utvärderas. 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. Deloitte rekommenderar även Region Skåne att etablera en kravställning i syfte att kontrollera vilka personer hos leverantören som har tillgång till gruppkonton.

- Att det finns tillräckliga manuella rutiner som säkerställer att samtliga förändringar sker enligt förväntande intentioner då det inte finns tvingade kontroller i systemet Personec P som fordrar att två personer är involverade i upplägg och förändring av löner.

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

- 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.

- Att säkerställa efterlevnad av den årliga rutinen som avser god-kännande av rolluppsättningen i Raindance.

Rapporten översändes för kännedom och beaktande.

George Smidlund
Revisionsdirektör