Revisionskontorets sammanfattning av granskningsrapport

Nr 17/2015
Jan 2016

Granskning av IT-kontroller

Uppdrag och syfte
Deloitte AB har på revisorernas uppdrag och som ett led i redovisningsrevisionen genomfört en granskning av IT-miljön inom Region Skåne. Syftet med uppdraget 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.

Bakgrund
Enligt den revisionsplan som antagits för 2015 års redovisningsrevision ska Deloitte utföra en särskild granskning av IT-miljön inom Region Skåne. De system som identifieras som mest kritiska för den finansiella rapporteringen och som valts ut är Region Skånes huvudsakliga ekonomisystem Raindance samt den personal-relaterade applikationen Personec P (del av HR Fönster). Granskningen av IT-kontroller har omfattat följande områden:

- **Åtkomstkontroll** – Rutiner och systeminställningar för hur det säkerställs att ingen obehörig person kommer åt känslig information.
- **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.

Resultat av granskningen
Den sammanfattande bedömningen 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 granskningen noterades 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. Ett ställningstagande för att acceptera den potentiella risken kopplat till dessa gruppkonton har genomförts på lämplig ledningsnivå. Dock bör risknivån för dessa gruppkonton kontinuerligt utvärderas samt behovet avseende att implementera kompenserande rutiner för uppföljning av användningen av dessa konton.

Enligt intervjuade i granskningen fordras det 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.

Rapporten finns tillgänglig på www.skane.se/revisionen