Revisionskontoret

Sammanfattning av granskningsrapport

Granskning av IT-säkerhet

Uppdrag och syfte

KPMG har på revisorernas uppdrag följt upp synpunkter och rekommendationer från granskningen från 2019 av ”IT-säkerhet med inriktning på system som har betydelse för intern kontroll inom redovisningen”.

Syftet med granskningen är att följa upp Region Skånes åtgärder utifrån de rekommendationer som lämnades i den tidigare granskningen av IT-säkerhet från 2019. Då uppdraget är en uppföljning av den tidigare granskningen har den avgränsats till att granska system som hanterar stora transaktionsvolymer i avsikt att säkerställa en korrekt redovisning. IT-miljön har därmed begränsats till att inkludera systemen Raindance och Personec P, i enlighet med den tidigare granskningen.

Bakgrund

Utgångspunkt för den under 2019 genomförda granskningen var för området relevanta styrande dokument, vilket inte enbart begränsades till aspekter utifrån IT-säkerhet (enligt granskningens rubricering), utan även aspekter på regionens arbete med informationssäkerhet. Regionens arbete utifrån Dataskyddsförordningen (2018:218) berördes också. Eftersom begreppet informationssäkerhet i allt större utsträckning numera används som ett samlingsbegrepp där såväl dataskydd som IT-säkerhet ingår, sker denna uppföljning även med denna utgångspunkt.

Granskningen omfattar regionstyrelsen.

Resultat av granskningen

i samband med Dataskyddsförordningens ikraftträdande (maj 2018) utfördes kartläggning/registerföring av känsliga informationsslag lokalt vid Region Skånes olika förvaltningar. Kartläggningen, liksom efterföljande arbete med klassificering, riskanalys, beslut om skyddsåtgärder samt lokalt införda skyddsåtgärder, är dokumenterade utan gemensam struktur vid de olika förvaltningarna. Arbetet har därför inte kunnat sammanställas eller följas upp centralt. Av denna anledning finns osäkerhet med avseende på det genomförda arbetets omfattning och kvalitet. Exempel på noterat kvarvarande arbete är att endast 1/3 av Region Skånes befintliga system hittills klassificerats.

Beslut har nu fattats om att införa ett gemensamt systemstöd (iFacts) och därmed enhetlig struktur, för att dokumentera genomfört arbete. Införandet av systemet planeras ske under 2023.

Uppföljning och rapportering rekommenderas ske utifrån beslutade ”Key Perfomance Indicators” (KPI:er) som representerar hela arbetsprocessen för informationssäkerhet. Dessutom bör uppföljningen ske mot respektive operativ enhet inom regionen för att undanröja eventuella otydligheter med avseende på ansvarsfördelningen för arbetet.

Bland annat lämnas följande rekommendationer efter genomförd granskning:

att inställningarna för autentisering via lösenord av användare i Raindance förstärks betydligt.

att tillämpad periodicitet av inaktivitet i Raindance (24 månader), för att inaktivera användarkonto bör kortas väsentligt.

att regionen utvecklar gemensamma krav på autentisering via lösenord utifrån resultatet av respektive systems klassificeringsnivå.

att rutin som gör det möjligt att säkerställa alla användares aktualitet i Raindance bör införas.

att rutin införs för att möjliggöra kontroll av aktiviteter som utförs av användare med höga behörigheter i Raindance.

att inte använda gruppkonton eftersom det förhindrar möjligheten att konstatera att endast behörig åtkomst till känsliga informationsslag förekommit.