NR 4 - juni 2017

Revisionskontoret

Sammanfattning av granskningsrapport

IT-säkerhet och informationssäkerhet

Uppdrag och syfte

På uppdrag av Region Skånes revisorer har PWC AB granskat IT-säkerhet och informationssäkerhet i Region Skåne. Det övergripande syftet med granskningen har varit att ge revisorerna underlag för att bedöma om Region Skånes informationssäkerhetsarbete, innefattande bland annat IT-säkerhetsåtgärder, bedrivs på ett systematiskt och effektivt sätt samt är ändamålsenligt på det sätt som förväntas och är önskvärt utifrån medborgare och patienters behov. Kontaktperson från revisorskollegiet har varit Michael Michaelsen och Fredrik Ljunggren har varit projektledare från revisionskontoret.

Resultat av granskningen

Resultatet av granskningen visar på den övergripande bedömningen att Region Skåne inte har ändamålsenliga rutiner och processer för att hantera IT-säkerhet och informationssäkerhet. Granskningen visar att det inte finns en fungerande styrmodell implementerad, inte heller tillräcklig omfattning av resurser, styrande dokument och rutiner till grund för att säkerställa ändamålsenlig hantering av informationstillgångar inom Region Skåne.

Organisation, roller och ansvar kopplat till IT- och informationssäkerhetsområdet är inte tydligt definierade. De roller som identifierats för område IT- och informationssäkerhet förefaller vara underdimensionerade beaktat Region Skånes storlek på verksamhet och den typ av informationstillgångar som hanteras i verksamheten. Granskningen visar att verksamhetsområdena för IT-säkerhet och informationssäkerhet inte har en egen budget per verksamhetsområde. Kostnaden för att investera i IT-säkerhetslösningar är distribuerad och inkluderad i den totala IT-budgeten för respektive verksamhetsområde. Vid identifierade behov av investeringar i området har IT-säkerhetsansvarig respektive informationssäkerhetschef historiskt behövt förhandla fram medel från budgetansvarig på verksamhetsnivå.

Det saknas en övergripande struktur som beskriver relationen mellan olika styrande dokument. Det saknas dokumenterade rutiner för väsentliga processer såsom till exempel inventering och kartläggning av information till grund för informationsklassificering samt för genomförande av riskanalyser.

Processen för incidenthantering saknar en tillräckligt specifik definition av IT-säkerhets- och informationssäkerhetsrelaterade incidenter, vilket leder till svårighet att följa upp incidenter och säkerställa att kontrollmiljön är relevant utifrån aktuella risker och brister.

Det saknas relevanta och tydligt definierade nyckeltal för styrning och uppföljning med syfte att säkerställa god IT- och informationssäkerhet samt kontinuerlig förbättring av kontrollmiljön, internt men även hos externa leverantörer. Vidare noteras att övervakningen av området för IT- och informationssäkerhet i dagsläget är i grunden mer reaktiv än proaktiv.

En del brister som noterats i samband med den utförda granskningen är kända av Region Skåne och flertalet initiativ har påbörjats för att hantera dessa. Det pågår även en process för att omorganisera området för IT.

Konsulten har framfört flera förbättringsförslag men revisorerna vill särskilt lyfta följande **förbättringsområden:**

1. Organisation, roller och ansvar ner på verksamhetsnivå med en budget anpassad för en effektiv och ändamålsenlig IT-säkerhet och informationssäkerhet.
2. Styrande dokument med riktlinjer och rutin för riskanalys och informationsklassificering samt kontroller och ansvar för regelbunden efterlevnad av respektive område.
3. Processen för incidenthantering.
4. Nyckeltal för IT-säkerhet och informationssäkerhet.

Rapporten finns tillgänglig på www.skane.se/revisionen

REGION SKÅNE