Yttrande över granskning av informations- och IT-säkerhet

Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som nämnden ansvarar för.

Svar:
Digitalisering IT och MT:s enhet för IT-säkerhet genomför informationsklassificeringar, riskanalyser och i förekommande fall konsekvensbedömningar enligt beslut från regiondirektör, samt instruktioner och processer. Merparten av de riskanalyser och konsekvensbedömningar som rör informationssäkerhet som görs inom Region Skåne genomförs under ledning av Digitalisering IT och MT.

Förvaltningen har anlitat konsulter som sedan början av år 2023 arbetar inom ett projekt med att leda informationsklassificeringar, riskanalyser och konsekvensbedömningar för de system inom Region Skåne som redan är i drift, men där arbetet med informationssäkerhet inte har gjorts tidigare. Som granskningen konstaterar (sida 11 i granskningsrapporten) har projektet startats efter ett uppdrag från tidigare regiondirektör, men beslut eller underlag för detta uppdrag har inte kunnat återfinnas.

Digitalisering IT och MT kan, liksom revisorerna (sida 18 i granskningsrapporten), konstatera att övriga förvaltningar inte alltid följer de styrande dokument som finns på området, bland annat *Instruktion för tillämpning av riktlinjer för informationssäkerhet.* Följden är att Digitalisering IT och MT tar ett större ansvar utöver förvaltningens ordinarie ansvar. I instruktionen står:

- 5.1.2 Förvaltningschef ska inom sin förvaltning utse informationssäkerhetssamordnare som har ett tydligt mandat och uppdrag att leda, samordna och följa upp förvaltningens informationssäkerhetsarbete.

- 5.1.3 Informationsägare som inte är förvaltningschef ska inom sin organisation utse informationssäkerhetssamordnare.

- 5.1.6 Förvaltningen ska avsätta tillräckligt med resurser för att arbetet ska kunna bedrivas effektivt.

- Bilaga 1 Informationssäkerhetssamordnaren ska leda, utveckla, samordna och följa upp informationssäkerhetsarbetet utifrån regionövergripande styrande dokument. Utöver det ska informationssäkerhetssamordnaren samarbeta med förvaltningens dataskyddssamordnare med att stödja verksamheten vid genomförandet av informationsklassificering och olika typer av riskbedömningar inkluderande konsekvensanalyser avseende dataskydd enligt dataskyddsförordningen.

Brister i ovanstående får till följd att Digitalisering IT och MT:s informationssäkerhetssamordnare och riskanalysledare måste täcka upp även för övriga förvaltningars behov vilket innebär:

- En alltför stor belastning på Digitalisering IT och MT.
- Ett långsammare förlopp vad gäller informationsklassificering och riskanalyser av IT-system.

Säkerställa att tekniska säkerhetsåtgärder vidtas utifrån identifierat skyddsvärde hos egna informationstillgångar, men även övriga styrelser och nämnders identifierade behov i informationsklassning och riskbedömning

Svar:
IT-säkerhetsansvarig på Digitalisering IT och MT tar, via två Security Operations Centers, del av de incidenter och problem som uppstår. Månatliga sårbarhetsskanningar genomförs och identifierade sårbarheter åtgärdas löpande. Incidenter kan komma in via Ritz eller via avvikelsesystemet AvIC. Precis som granskningen visar rapporteras dock inte alla incidenter. När de rapporteras sker det inte på ett enhetligt sätt. Dessutom får IT-säkerhetsansvarig och informationssäkerhetssamordnare inte alltid information och kännedom om inträffade incidenter.

Incidenthantering av informationstillgångar kan stärkas med stöd av teknisk systemövervakning, händelseloggar och automatiskt skapade incidentärenden baserat på fördefinierade tröskelvärden. Med automatisk eskalation och notifiering till ansvariga i drift- och supportorganisation kan tidig upptäckt av incident på informationstillgång reducera påverkan på informationstillgång och säkerställa data för underlag till förbättringsåtgärder.

Säkerställa att medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet

Svar:
Digitalisering IT och MT har under våren år 2023 tagit fram ett förslag till organisation för informationssäkerhet och dataskydd inom Digitalisering IT och MT. Under hösten har även förslag på utbildningsplan på flera olika nivåer utarbetats, vilket inkluderar den obligatoriska utbildning i informationssäkerhet som finns i Lärportalen. Målet är att en viss procent, exempelvis 80 %, av förvaltningens anställda ska ha genomfört utbildningen och 100 % av samtliga nyanställda inom den första anställningsmånaden. Mätning och uppföljning ska ske kontinuerligt av närmaste chef och informationssäkerhetssamordnaren.

Utöver detta kommer Digitalisering IT och MT:s strategiska informationssäkerhetssamordnare att utbilda processledare i samband med processforum, samt utsedda kontaktpersoner inom samtliga verksamhetsområden i förvaltningen. Utbildningsinsatserna kommer att behandla såväl övergripande informationssäkerhet som konkreta och praktiska delar som incidenthantering, informationsklassificering och riskhantering, styrning av åtkomst, kommunikationssäkerhet och lagringsmedia, avtalshantering med mera.

Säkerställa att rutiner för incidenthantering etableras i organisationen.

Svar:
Inom Digitalisering IT och MT finns etablerad process för IT- och MT-incidenthantering samt hantering av stora incidenter och IT-säkerhetshetsincidenter. Utbildningstillfällen för incidenthantering erbjuds regelbundet varje månad.

Under år 2024 pågår en processrevision inom Digitalisering IT och MT för övergång till processramverket ITIL4. I revisionen ingår bland annat:

- en översyn av incident- och problemprocessroller kopplat till organisatoriska roller och deras respektive ansvar i processen

- en kartläggning av beroenden till övriga processer i förvaltningen för att säkerställa en sammanhängande värdeskapandekedja.

Säkerställa att inträffade incidenter dokumenteras, analyseras och utgör underlag för att identifiera förbättringsbehov för att stärka IT-säkerheten

Svar:
Inom Digitalisering IT och MT finns en etablerad process för incidenthantering samt för hantering av stora incidenter och IT-säkerhetshetsincidenter. Processen registrerar och dokumenterar incidenter i systemstödet Ritz. Användare ska rapportera IT- och MT-incidenter genom att ringa servicedesk eller registrera sitt incidentärende via Ritz självserviceportal.

Vid upptäckt av potentiella problem som till exempel återkommande incidenter, registreras problemärende för orsaksutredning enligt processen problemhantering.

För att kunna analysera och identifiera förbättringsbehov utifrån IT- och MT-incidenter på system, tjänster och utrustning är det av stor vikt att incidenter rapporteras till Digitalisering IT och MT:s servicedesk, registreras och dokumenteras i systemstödet Ritz incidentformulär samt hanteras i ett kvalitetssäkrat supportflöde. Detta arbetar Digitalisering IT och MT kontinuerligt med och arbetet kommer att intensifieras under år 2024.