WESSLAU SÖDERQVIST

Promemoria

Ang. fortsatta arbetet med informationssäkerhet och implementering av DORA-förordningen

1 Inledning

S:t Erik Försäkrings AB, nedan Bolaget, har tillsammans med Bolagets funktion för regelefterlevnad, upprättat följande ”färdplan” för implementeringsarbetet av DORA-förordningen och det fortsatta arbetet med informationssäkerhet. I planen redogörs dels för föreslagna åtgärder som rekommenderas i Bolagets verksamhet, dels i vilken ordning åtgärderna ska företas. Bolaget utgör enligt artikel 3 p.64 ett medelstort företag i förordningens mening, vilket spelar roll vid proportionalitetsbedömningen i vissa delar av förordningen samt hur krav däri ska tillämpas.

DORA-förordningen börjar gälla den 17 januari 2025.

2 Rekommendationer och förslag till åtgärder

2.1 Leverantörsavtal

Samtliga leverantörsavtal som var föremål för granskning och justering inför införandet av Eiopa:s IKT-regler, bör ses över ånyo mot bakgrund av DORA. Översynen bör även innefatta eventuellt nytillkomna leverantörer av digitala tjänster. Om avtalen behöver justering är det bra om detta påbörjas så snart som möjligt.

Vår rekommendation är att detta prioriteras och bör påbörjas under det andra kvartalet 2024.

2.2 Policydokument

DORA-förordningen ställer bl.a. krav på intern styrning och kontroll, kontinuitetshantering, kommunikationshantering (internt/externt), riskhantering, incidenthantering och outsourcing för att nämna några större områden. Bolagets styrdokument och processer som styr dessa områden behöver översyn för att anpassas till DORA och det behöver även analyseras huruvida eventuellt nya styrdokument behöver upprättas.

Vår rekommendation är att detta prioriteras, primärt med en analys över vilka styrdokument som behöver ses över och eventuellt tas fram, därefter påbörja nödvändiga justeringar. Detta bör påbörjas under det andra kvartalet 2024.

2.3 Riskhantering och tredjepartsrisker

Likt i Eiopa:s IKT-regler är riskhantering och då primärt hanteringen av informationssäkerhetsrisker centralt. Ett stort arbete har sedan tidigare lagts ner i verksamheten för att genomlysa vilka risker som bör prioriteras, så det i det fortsatta arbetet behöver det stämmas av om något ytterligare tillkommer i och med DORA-förordningen. Tredjepartsriskerna är tämligen lika i verksamheten om man ser utifrån DORA, där utkontraktering bör prioriteras såsom nämnts ovan i 2.1. En process för kontraktsuppföljning inklusive återrapportering till Bolagets styrelse finns sedan tidigare etablerad. Därtill har en utvidgad process tagits fram för att användas vid all kontraktsuppföljning och i synnerhet gällande leverantörer av IKT-tjänster och IKT-system. Dessa bör ses över mot bakgrund av DORA och görs till viss del enligt rekommendationen i 2.2.

Vår rekommendation är att prioritera en gemensam avstämning mellan Bolaget, funktionen för regelefterlevnad och funktionen för riskhantering för att göra en gemensam bedömning avseende behovet av en utvidgad riskanalys/riskregister. Detta bör påbörjas tidigt under andra kvartalet 2024.

Styrdokument avseende riskhantering ses över i enlighet med förslag i p. 2.2.

2.4 Systemhantering, behörigheter och informationsklassning

Bolaget har nyligen reviderat avbrottsplan samt kris- och kontinuitetsplan. Dessa behöver likväl granskas för att stämma av efterlevnaden gentemot DORA. Utöver dessa styrdokument behöver även styrdokument och processer kopplade till IT-säkerhet granskas. Vi rekommenderar vidare att styrdokument från Staden som har bäring på IT-säkerhet, genomgås för att klargöra om dessa behöver på något sätt anpassas för att inte gå emot reglerna i DORA.

Vår rekommendation är att det fastställs en process, om sådan inte redan finns, för inköp av nya system och vilka risker som behöver hanteras och kontrolleras i anslutning till detta. Likaså en process för behörighetstilldelning. Därtill rekommenderar vi att ovan nämnda dokument genomgås för att säkerställa efterlevnaden av DORA-förordningen.

Arbetet ovan bör påbörjas i slutet av det andra kvartalet, alternativt i början av det tredje kvartalet.

2.5 Incidenthantering

Befintlig rutin för incidenthantering behöver ses över mot bakgrund av DORA-förordningen. Med största sannolikhet kommer det även behöver ske vissa justeringar i processen då DORA uppställer krav på en vidare förberedelse inför en eventuell incident. Bolaget måste bl.a. ha klart för sig hur en incident ska klassificeras, redan innan den inträffar. Således behöver Bolaget ta fram parametrar för att tydligare bedöma ”allvarlighetsgraden” i olika typer av IT-relaterade incidenter.

Vår rekommendation är att arbetet påbörjas under det tredje kvartalet 2024.

2.6 Revision, kontroll och testning

Bolaget måste etablera en rutin för att godkänna och regelbundet se över Bolagets IKT-internrevisionsplaner, IKT-revisioner och väsentliga ändringar av dessa. Vidare behöver rutinen för testning av system och dokumentation ses över mot bakgrund av DORA-förordningen.

Vidare behöver Bolaget se över befintlig rutin för internkontroll så att denna fångar upp de krav som ställs i DORA.

Vår rekommendation är att arbetet påbörjas under det tredje kvartalet 2024.

3 Strategi och analys

Vi rekommenderar att den strategi och analys avseende IKT-risker m.m. som beslutades år 2021, ska ses över mot bakgrund av DORA-förordningen. Arbete behöver göras tillsammans med styrelsen och kan företrädesvis utföras i anslutning till utbildning inom DORA-förordningen.

I anslutning till detta bör även framtagande av en kommunikationsstrategi diskuteras.

Vår rekommendation är att detta genomförs i under det tredje kvartalet 2024.

4 Utbildning

Såväl styrelsen som Bolagets anställda behöver ytterligare utbildning om DORA-förordningen. Passen kommer vara av praktisk karaktär för att underlätta arbetet med styrning och kontroll avseende informationssäkerhet samt inkludera mer strategiskt arbete för styrelsen.

Vår rekommendation är att utbildningspassen genomförs i under det tredje kvartalet 2024.

5 Kommande föreskrifter

Den sista leveransen av tekniska standarder ska komma i juni år 2024.

2024-05-13/Erik Fischer, Johan Gagner och Johan Grenefalk