Rapport om översyn av IKT-riskhanteringsramverket

S:t Erik Försäkrings AB
(Artikel 6.5 i förordning (EU) 2022/2554 (DORA) och format/innehåll enligt RTS 2024/1774 artikel 27)
Granskningsperiod: 2026-01-01 – 2026-02-28
Datum för upprättande: 2026-03-09
Ansvarig funktion: Riskfunktionen
Fastställd av styrelsen: 2026-03-27

Kommentar [MA1]: Låt vara i Advisense mall

Innehåll

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

1. Inledning

1.1. Om S:t Erik och syfte med rapporten

Denna rapport avser S:t Erik Försäkrings AB (”Bolaget”), org.nr 516401-7948, och utgör den årliga översynen av Bolagets IKT-riskhanteringsramverk i enlighet med DORA artikel 6.5 samt RTS 2024/1774 artikel 27.

S:t Erik Försäkrings AB ägs till 100 procent av Stockholms Stadshus AB, som i sin tur är helägt av Stockholms stad. Bolaget bedriver direktförsäkringsverksamhet för Stockholms stads förvaltningar och närstående bolag inom områdena egendom, ansvar och olycksfall. Övriga försäkringar som kommunkoncernen har behov av upphandlas av Bolaget från externa försäkringsgivare.

Rapporten syftar till att:

- bedöma effektiviteten i Bolagets IKT-riskhanteringsramverk,
- identifiera svagheter, brister och utvecklingsområden, samt
- ge styrelsen en samlad bedömning av Bolagets digitala operativa motståndskraft.

1.2. Definitioner

Kommentar [MA2]: Lägg till definitionen av IKT.

- **IKT (Informations- och kommunikationsteknik)**
  Teknik, system och tjänster som används för att behandla, lagra, överföra eller skydda information, inklusive nätverk, hårdvara, mjukvara och molnbaserade lösningar.
- **IKT-risk**
  Risken för negativ påverkan på verksamheten till följd av brister, störningar eller angrepp mot nätverks- och informationssystem.
- **Digital operativ motståndskraft**
  Bolagets förmåga att förebygga, upptäcka, hantera och återhämta sig från IKT-relaterade incidenter så att kritiska eller viktiga funktioner kan upprätthållas.
- **Förmåga**
  Den samlade kapaciteten inom ett område av IKT-riskhantering (styrning, identifiera, skydda/upptäcka, åtgärda/återställa), bedömd utifrån processer, kontroller och uppföljning.
- **Kritisk eller viktig funktion**
  En verksamhetsfunktion vars avbrott kan få betydande negativ påverkan på Bolagets verksamhet, regelefterlevnad eller förtroende.
- **BIA (Business impact anlaysis)**
  En strukturerad analys för att identifiera kritiska eller viktiga funktioner samt bedöma konsekvenser och acceptabla avbrottstider (t.ex. RTO/RPO) vid störningar i verksamheten.
- **IKT-tillgång**
  En teknisk eller informationsrelaterad resurs som stödjer verksamheten, exempelvis system, **databaser eller molntjänster.**

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

- **IKT-system**
  Ett sammanhängande system av hårdvara, mjukvara och nätverk som behandlar eller lagrar information och stödjer verksamhetsfunktioner.
- **IKT-tjänst**
  En tjänst som helt eller delvis bygger på IKT-system och som tillhandahålls internt eller av extern leverantör för att stödja verksamheten (t.ex. molntjänster, drift, applikationstjänster).

1.3. Kontext – art, omfattning och komplexitet samt beroenden

S:t Erik Försäkring är en mindre organisation med begränsad egen IT-drift. Bolagets IT-miljö är, med undantag för försäkringssystemet Insman**,** integrerad i Stockholms stads gemensamma IT-struktur.

Detta innebär att:

- upphandling, drift, teknisk säkerhet och övergripande kontroller i stor utsträckning hanteras av Stockholms stad,
- Bolagets roll primärt är kravställande, uppföljande och riskbedömande,
- Bolagets möjlighet till självständig verifiering av tekniska kontroller är beroende av stadens kontrollfunktion.

Bolaget omfattas av stadsgemensamma upphandlingar av IT, ekonomi och vissa andra tjänster. Hantering av IT-avtal och kontroller sker genom fullmakt till Stockholms stad.

Bedömningen av ramverkets effektivitet har genomförts proportionerligt utifrån verksamhetens art, omfattning och komplexitet.

1.4. Kritiska eller viktiga funktioner

Mot bakgrund av verksamhetens art och proportionalitet har följande funktioner identifierats som kritiska eller viktiga:

- Försäkringsadministration (försäkring, återförsäkring, RM)
- Skadehantering
- Finansiell och regulatorisk rapportering (ekonomi, FI m.m.)

1.5. Beroenden av IKT-tjänster och system

Bolagets verksamhet är i hög grad beroende av ett begränsat antal centrala IKT-system och tjänster som direkt stödjer identifierade kritiska eller viktiga funktioner. Dessa utgörs främst av:

- INSMAN (försäkringssystem),
- IA (incidentrapporteringssystem),

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

- Agresso (ekonomisystem),
- Standardiserade kontors- och kommunikationsverktyg,
- Stadens gemensamma infrastruktur och IT-tjänster.

Dessa system är integrerade i Bolagets löpande verksamhet och utgör en förutsättning för att kunna upprätthålla såväl operativa processer som regulatoriska åtaganden. En väsentlig del av den tekniska driften och säkerhetskontrollerna är centraliserade inom Stockholms stad, vilket innebär att Bolagets digitala operativa motståndskraft är nära kopplad till stadens samlade IT-förmåga. En total förlust eller allvarlig degradering av dessa tjänster skulle kunna leda till:

- Förseningar i skadehantering och försäkringsadministration
- Brister i finansiell och regulatorisk rapportering
- Ökad operativ och reputationsmässig risk
- Behov av manuella reservrutiner

Sammantaget innebär detta att Bolagets IKT-beroenden är koncentrerade till ett fåtal centrala system samt till Stockholms stads gemensamma IT-miljö. Detta medför en strukturell koncentrationsrisk, då störningar i stadens infrastruktur kan få direkt påverkan på Bolagets verksamhet.

Samtidigt innebär beroendet av Stockholms stad att Bolaget omfattas av en större och mer resursstark IT-organisation med etablerade skydds-, övervaknings- och beredskapsfunktioner. Detta ger tillgång till stordriftsfördelar, specialiserad kompetens och centraliserade säkerhetsåtgärder, vilket sammantaget bidrar till en högre teknisk skyddsnivå än vad Bolaget proportionerligt skulle kunna upprätthålla i egen regi.

2. Sammanfattning

2.1. Övergripande IKT-riskprofil

Bolagets övergripande IKT-riskprofil ska förstås i ljuset av verksamhetens storlek, begränsade egen IT-drift samt det starka beroendet av Stockholms stads gemensamma IT-miljö och externa leverantörer. Riskbilden präglas i första hand av beroende- och koncentrationsdimensioner snarare än av komplex intern teknisk miljö.

Bolagets huvudsakliga IKT-risker utgörs av:

- **Cybersäkerhetsrisk**, särskilt kopplad till otillbörlig åtkomst, dataintrång och nätfiske. Risken är nära förknippad med identitets- och behörighetshantering samt beroendet av gemensamma plattformar och molnbaserade tjänster. Även om Bolaget hanterar begränsade mängder känsliga personuppgifter kan ett intrång få betydande påverkan på förtroende, regelefterlevnad och verksamhetens kontinuitet.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

- **Avbrotts- och tillgänglighetsrisk**, kopplad till stadens gemensamma IT-miljö och utlagda system såsom försäkringssystemet och ekonomisystemet. Eftersom Bolaget har begränsad egen driftmiljö är kontinuiteten i hög grad beroende av extern infrastruktur och centraliserade tjänster. Störningar i dessa kan påverka skadehantering, försäkringsadministration och rapportering.

- **Leverantörs- och beroenderisk**, särskilt kopplad till Stockholms stad och externa aktörer. Denna riskdimension avser inte enbart tekniskt beroende, utan även begränsad insyn och verifierbarhet i uppföljningen av kontroller. Bolagets möjlighet att självständigt bedöma effektiviteten i vissa tekniska skydds- och detektionsåtgärder är i delar beroende av rapportering från stadens kontrollfunktion och externa leverantörer.

Den samlade riskprofilen bedöms som låg till medel. Bolaget har en relativt begränsad och standardiserad IT-miljö, vilket reducerar komplexiteten. Samtidigt föreligger en strukturell koncentrationsrisk och en verifierbarhetsutmaning till följd av det starka beroendet av stadens IT-funktion och externa leverantörer.

Riskprofilen bedöms därmed vara hanterbar, men beroende av att styrning, uppföljning och testning sker systematiskt och proportionerligt i relation till identifierade kritiska eller viktiga funktioner.

2.2. Hotbild

Hotbilden omfattar såväl fysiska som digitala och informationsrelaterade hot. Känsligheten för störningar i samhällsviktiga funktioner ökar i takt med den tekniska utvecklingen och det ökade beroendet av digital infrastruktur. Samtidigt har informations- och kommunikationsmönstren blivit snabbare och mer svåröverskådliga, vilket skapar förutsättningar för desinformationskampanjer och andra former av informationspåverkan i syfte att undergräva tillit till offentliga aktörer och demokratiska institutioner. Ur ett IKT- och DORA-perspektiv innebär detta att cyberangrepp, sabotage eller störningar riktade mot stadens gemensamma IT-miljö kan få indirekt påverkan på Bolagets verksamhet.

För S:t Erik Försäkring innebär detta att hotbilden inte kan analyseras isolerat utifrån bolagets egen storlek och exponering, utan måste förstås i kontexten av Stockholms stads samlade hotbild. Bolagets digitala operativa motståndskraft är därmed indirekt kopplad till stadens förmåga att skydda, upptäcka och hantera antagonistiska hot mot samhällsviktig infrastruktur.

Sammantaget bedöms hotbilden vara förhöjd i ett övergripande samhällsperspektiv, även om Bolagets direkta exponering är begränsad. Detta understryker vikten av tydlig styrning, systematisk uppföljning av leverantörsberoenden samt dokumenterad testning av kontinuitets- och incidenthanteringsförmåga.

2.3. Samlad bedömning av digital operativ motståndskraft

Mot bakgrund av den identifierade IKT-riskprofilen och den övergripande hotbilden har Bolagets digitala operativa motståndskraft bedömts genom en förmågebaserad analys (se avsnitt 6).

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

Översynen visar att Bolaget har etablerat grundläggande strukturer och processer för hantering av IKT-risker, inklusive styrande dokument, årlig riskbedömning, verksamhetskonsekvensanalys (BIA) samt dokumenterade incident- och kontinuitetsrutiner. För det verksamhetskritiska försäkringssystemet Insman föreligger god insyn och styrbarhet genom eget avtal och uppföljning.

Samtidigt präglas den samlade bedömningen av ett strukturellt beroende av Stockholms stads gemensamma IT-miljö och externa leverantörer. Detta medför att Bolagets kvarstående IKT-risker i huvudsak är kopplade till:

- begränsad självständig verifierbarhet av centralt driftade system,
- avsaknad av formaliserad oberoende uppföljning av IKT-riskhanteringsramverket,
- behov av mer systematisk och dokumenterad testning av kritiska förmågor.

Den samlade mognadsbedömningen per förmåga (se avsnitt 6.5) ligger på nivån **Etablerad**, vilket innebär att förmågorna är implementerade och i huvudsak fungerar operativt, men att identifierade förbättringsområden behöver hanteras för att stärka verifierbarhet och systematik.

Bolagets digitala operativa motståndskraft bedöms därmed vara proportionerlig och tillräcklig i nuläget, men utvecklingsbar. De föreslagna åtgärderna syftar främst till att höja mognadsnivån genom stärkt styrning, dokumentation, uppföljning och testning snarare än att införa helt nya kontrollområden.

Genom att genomföra åtgärdsplanen bedöms Bolaget kunna öka graden av verifierbar och dokumenterad digital operativ motståndskraft, minska beroenderelaterad osäkerhet samt tydligare kunna styrka efterlevnad av DORA vid en eventuell tillsyn.

3. Bakgrund och skäl till översynen

3.1. Skäl till översyn

Översynen har genomförts som en årlig översyn i enlighet med artikel 6.5 i DORA samt de krav på innehåll och struktur som anges i RTS 2024/1774 artikel 27. Enligt DORA åligger det ledningsorganet att regelbundet granska och utvärdera effektiviteten i den finansiella entitetens ramverk för hantering av IKT-risker.

Syftet med översynen är att:

- bedöma om Bolagets IKT-riskhanteringsramverk är ändamålsenligt, proportionerligt och anpassat till verksamhetens art, omfattning och komplexitet,
- identifiera svagheter, brister och gap i ramverkets utformning eller tillämpning,
- utvärdera om fastställda kontroller och processer fungerar i praktiken,
- säkerställa att Bolaget upprätthåller tillräcklig digital operativ motståndskraft i förhållande till identifierad IKT-riskprofil och aktuell hotbild.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

Översynen utgör en del av Bolagets systematiska arbete med intern styrning och kontroll och ska ge styrelsen ett samlat underlag för att bedöma om ytterligare åtgärder, prioriteringar eller resursförstärkningar är nödvändiga.

3.2. IKT-relaterade incidenter under perioden

Under perioden har inga väsentliga IKT-incidenter som allvarligt påverkat kritiska eller viktiga funktioner dokumenterats.

4. Ansvar och metod

4.1. Funktion ansvarig för översynen

Översynen har genomförts av riskfunktionen i samverkan med första linjen. Oberoende har säkerställts genom att den samlade bedömningen har sammanställts utan operativt linjeansvar för de bedömningar som gjorts.

4.2. Metod och struktur

4.2.1. Metod

Metoden bygger på:

- workshop med första linjen (matrisgenomgång),
- intervjuer med nyckelpersoner,
- granskning av styrande dokument, riskregister, IKT-tillgångsregister och BIA analys samt evidens där sådan funnits.

Bedömningen har genomförts proportionerligt och riskbaserat utifrån Bolagets IKT-riskprofil och beroenden.

4.2.2. Struktur

Översynen av Bolagets IKT-riskhanteringsramverk, samt den därav följande bedömningen av Bolagets digitala operativa motståndskraft, har strukturerats i enlighet med etablerad praxis och med utgångspunkt i NIST-ramverkets huvudområden för hantering av IKT-risk. Den förmågebaserade strukturen möjliggör en samlad och systematisk bedömning av såväl styrning och riskidentifiering som förebyggande, detekterande och återställande åtgärder.

Genom att använda NIST:s huvudområden som analysram säkerställs en tydlig koppling mellan identifierad IKT-riskprofil, befintliga kontroller och Bolagets faktiska förmåga att upprätthålla digital operativ motståndskraft i enlighet med DORA:s krav.

Bedömningen baseras på en genomgång av följande förmågor:

- **Styrning:** Förmågan att fastställa ramar, krav och en ändamålsenlig styrmodell för hantering av IKT-risker.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

- **Identifiera**: Förmågan att förstå verksamhetens värden, kritiska eller viktiga funktioner samt beroenden och risker kopplade till dessa.
- **Skydda och upptäcka**: Förmågan att begränsa sannolikheten för och effekten av IKT-relaterade hot genom förebyggande och detekterande tekniska och organisatoriska åtgärder.
- **Åtgärda och återställa:** Förmågan att hantera IKT-incidenter på ett kontrollerat sätt samt att återställa verksamheten efter en störning.

5. Större förändringar och förbättringar sedan föregående översyn (inkl. påverkan)

Eftersom detta är S:t Eriks första rapport avser "föregående översyn" den senaste interna uppföljningen och utvecklingen av ramverket under perioden.

Följande större förändringar och förbättringar har identifierats under granskningsperioden samt i jämförelse med tidigare interna arbetssätt och underlag på IKT-området. Eftersom detta är Bolagets första rapport enligt DORA/RTS artikel 27 avser "föregående översyn" i detta avsnitt den föregående interna uppföljningen/översynen av IKT-området och den utveckling som skett under perioden.

1. Förbättringsarbete avseende integrationer mellan Insman och Agresso

Påverkan: minskar risk för felaktig data i intern rapportering och risk för brister i datakvalitet/integrationer.

Påverkan på internkontroll: stärker kvalitet i underlag och kontroller kopplade till rapportering.

2. Pågående arbete med kontrollprocesser för utlagd IT-verksamhet

Påverkan: stärker styrning och uppföljning gentemot leverantörer samt stärker förmågan att upptäcka och hantera risker kopplade till brister/incidenter i utlagda tjänster.

3. Behörighetskontroller och revisioner (t.ex. behörighetsrevision införd enligt riskregistret)

Påverkan: stärker skyddsförmåga och intern kontroll av åtkomst.

Sammantaget påverkar förändringarna den digitala operativa motståndskraften främst genom ökad kontroll av dataflöden och förbättrad uppföljning av leverantörsberoenden.

6. Resultat av översyn per förmåga

Nedan redovisas översynens viktigaste iakttagelser per förmåga, baserat på genomförda workshops, intervjuer och granskning av tillgängligt underlag. För varje förmåga beskrivs nuläge, identifierade svagheter och brister samt i vilken utsträckning Bolaget har möjlighet att verifiera att fastställda krav fungerar som avsett i praktiken. Identifierade förbättringsbehov ligger till grund för de åtgärder som sammanställs i bilagan.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

De observationer som framkommer i analysen av respektive förmåga redovisas översiktligt i detta avsnitt. För en mer detaljerad redogörelse av identifierade iakttagelser och tillhörande bedömningar hänvisas till avsnitt 7.

6.1. Styrning

S:t Erik Försäkring har etablerat ett grundläggande ramverk för styrning av IKT-risker. En IKT-riktlinje är fastställd och utgör den övergripande strukturen för ansvarsfördelning, efterlevnad av tillämplig reglering samt hänvisningar till övriga styrande dokument inom IKT-området. Avtalsgenomgångar genomförs årligen och styrelsen erhåller regelbunden rapportering om IKT-relaterade frågor.

Översynen visar samtidigt att styrningsmodellen kan utvecklas, särskilt vad gäller tydliggörande av rollfördelning mellan första och andra försvarslinjen samt etablering av en formaliserad oberoende kontrollfunktion. Riskaptit och risktoleranser är i huvudsak kvalitativt formulerade och skulle kunna kompletteras med mer mätbara indikatorer.

6.2. Identifiera

Bolaget genomför årligen verksamhetskonsekvensanalyser (BIA) och IKT-riskbedömningar för att identifiera kritiska processer, tillgångar och risker. Register över IKT-tillgångar och leverantörer finns dokumenterade.

Översynen visar dock att dokumentationen i vissa delar är fragmenterad och att kopplingen mellan affärsprocesser, system och leverantörer kan göras mer överskådlig. En tydligare beroendekartläggning skulle stärka Bolagets förmåga att förstå beroendet till olika system och konsekvenserna av avbrott, samt snabbt bedöma påverkan och prioritera åtgärder vid incident.

6.3. Skydda och Upptäcka

Bolaget har infört grundläggande skyddsåtgärder, såsom årlig säkerhetsutbildning och rutiner för behörighetshantering. Mer avancerade tekniska säkerhetsåtgärder implementeras i huvudsak av leverantörer och inom Stockholms stads gemensamma IT-miljö.

Bolagets möjligheter att självständigt verifiera att skyddsåtgärder och detektionsförmåga fungerar som avsett är dock begränsade, särskilt avseende centralt driftade system. Uppföljning och testning sker i stor utsträckning inom stadens kontrollfunktion, vilket medför att verifierbarheten varierar beroende på system.

6.4. Åtgärda och återställa

Incident- och kontinuitetsplaner är dokumenterade och kända i organisationen. Bolaget har även avtalsreglerade exit-strategier gentemot leverantörer.

Översynen visar dock att testning och dokumenterad uppföljning inte genomförs fullt ut systematiskt. För att stärka den praktiska verifieringen av återställningsförmågan behöver testning formaliseras och dokumenteras mer konsekvent.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

6.5. Bedömning av digital operativ motståndskraft

6.5.1. Samlad analys

För att uppfylla DORA:s krav och säkerställa tillräcklig digital operativ motståndskraft behöver Bolaget samtliga ovanstående förmågor.

Det mest kritiska systemet för verksamheten är försäkringssystemet Insman, som direkt stödjer försäkringsadministration och skadehantering. Avseende detta system har Bolaget eget avtal och full insyn i leverantörens åtaganden, vilket ger en relativt god styrbarhet och kontroll.

Ekonomisystem, e-post och övrig datahantering driftas däremot inom Stockholms stads gemensamma IT-miljö. Detta innebär att Bolagets kontinuitet och informationssäkerhet i dessa delar är beroende av stadens tekniska och organisatoriska skyddsåtgärder. Den praktiska kontrollbilden är därmed differentierad:

- Direkt kontroll och insyn avseende Insman.
- Indirekt kontroll och begränsad verifierbarhet avseende centralt driftade system.

Sammantaget finns grundläggande strukturer på plats, men beroendet av stadens IT-leveranser medför att verifierbarheten varierar mellan system och förmågor.

6.5.2. Bedömning av mognad per förmåga

För att bedöma hur väl respektive förmåga fungerar används en tregradig mognadsskala:

- **Grundläggande** – strukturer och kontroller finns, men är inte fullt systematiskt implementerade eller verifierade.
- **Etablerad** – förmågan är i huvudsak implementerad och fungerar operativt, men utvecklingsområden kvarstår.
- **God** – förmågan är väl implementerad, systematiskt uppföljd och verifierad genom testning och dokumentation.

Mognadsbedömningen avser effektivitet i förmågan och är inte samma skala som allvarlighetsgrad (Låg/Medel/Hög) i avsnitt 7.

En bedömning på nivån *Etablerad* innebär att förmågan är tillräcklig i nuläget och att verksamheten fungerar, men att mognaden kan höjas genom ytterligare systematik, dokumentation eller testning.

Bedömningen för respektive förmåga är följande:

- **Styrning: Etablerad** – styrande dokument och rapportering finns, men oberoende kontrollfunktion saknas och riskaptiten är huvudsakligen kvalitativ.
- **Identifiera: Etablerad** – BIA och register finns, men beroendekartor och dokumentation kan förtydligas.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

- **Skydda och upptäcka: Etablerad** – tekniska kontroller är i huvudsak på plats via stadens IT-miljö, men verifierbarheten är begränsad i vissa delar.
- **Åtgärda och återställa: Etablerad** – planer finns, men testning och dokumenterad uppföljning behöver formaliseras.

6.5.3. Samlad mognadsbedömning

Den samlade mognadsnivån för Bolagets digitala operativa motståndskraft bedöms vara **Etablerad**.

Det innebär att ramverket fungerar och är proportionerligt i förhållande till verksamhetens art och komplexitet, men att identifierade förbättringsområden behöver hanteras för att stärka verifierbarhet och systematik.

7. Sammanfattning av iakttagelser

Baserat på genomförd översyn – inklusive workshop, dokumentgranskning och förmågebedömning – bedöms följande utvecklingsområden vara mest väsentliga för Bolagets fortsatta mognad inom digital operativ motståndskraft.

Bedömningen av allvarlighetsgrad (**Låg/Medel/Hög**) avser en samlad värdering av:

- påverkan på kritiska eller viktiga funktioner,
- sannolikhet samt
- graden av verifierbarhet (dvs. i vilken utsträckning förmågans funktion kan styrkas genom dokumentation, uppföljning och testning).

Observera att denna skala avser risk och påverkan, och skiljer sig från mognadsbedömningen i avsnitt 6.5.

Allvarlighetsgrad kan bli Hög även om sannolikheten inte bedöms hög, om påverkan på kritiska/viktiga funktioner är betydande eller om verifierbarheten är otillräcklig för kritiska beroenden.

7.1. Tydlig ansvarsfördelning och oberoende uppföljning

Bolaget saknar i nuläget en tydligt formaliserad och dokumenterad oberoende kontrollfunktion avseende IKT-riskhantering. Även om ansvar i praktiken är fördelat och IKT-frågor behandlas löpande, är rollfördelningen mellan första och andra försvarslinjen inte fullt ut operationaliserad.

Detta innebär en risk för att uppföljning och kontroll huvudsakligen sker i linjen, vilket kan begränsa den systematiska verifieringen av att fastställda krav och kontroller fungerar över tid.

Allvarlighetsgraden bedöms som **Medel**, då grundläggande styrning finns på plats, men den oberoende uppföljningen behöver stärkas för att fullt ut uppfylla DORA:s krav.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

7.2. Beroendekartläggning och spårbarhet mellan funktion–system–leverantör

Dokumentation av kritiska funktioner, IKT-tillgångar och leverantörer finns, men kopplingen mellan dessa kan förtydligas och göras mer operativ.

En mer sammanhållen och lättillgänglig beroendekarta skulle stärka Bolagets förmåga att:

- snabbt bedöma påverkan vid incident,
- prioritera återställningsåtgärder,
- tydligare koppla IKT-risker till verksamhetsrisker.

Allvarlighetsgraden bedöms som **Medel**, då bristen främst påverkar effektivitet och tydlighet vid incidenthantering snarare än att innebära ett omedelbart kontrollgap.

7.3. Leverantörsuppföljning och verifierbarhet

Bolagets digitala operativa motståndskraft är i hög grad beroende av Stockholms stads gemensamma IT-miljö. Detta medför att flera skydds-, detektions- och återställningskontroller ligger utanför Bolagets direkta operativa kontroll.

Den kvarstående risken är därför främst kopplad till begränsad verifierbarhet, dvs. Bolagets möjlighet att självständigt säkerställa att kontroller fungerar som avsett genom tillgång till uppföljningsrapporter och evidens.

Allvarlighetsgraden bedöms som **Medel**, då kontrollmiljö i praktiken finns, men verifierbarheten och uppföljningsstrukturen behöver stärkas.

7.4. Testning av incident- och kontinuitetsförmåga

Incident- och kontinuitetsplaner finns dokumenterade, men testning och dokumenterad uppföljning sker inte fullt ut systematiskt.

Bolagets praktiska verifiering av digital operativ motståndskraft skulle stärkas genom regelbunden och dokumenterad testning av::

- incidenthanteringsprocessen,
- avbrottsplaner,
- återställningsförmåga för kritiska system,

Allvarlighetsgraden bedöms som **Medel**, då bristen avser systematik och verifierbarhet snarare än avsaknad av grundläggande planer.

8. Kontroll funktioners (Internrevisionens) iakttagelser och rekommendationer

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

Som en del av översynen har Bolaget beaktat internrevisionens granskning av IKT-tredjepartsrisker. Internrevisionen har lämnat fyra rekommendationer, varav en med riskklassificering Medel och tre med riskklassificering Låg, enligt nedan.

1. **Dokumenterat ansvar enligt DORA artikel 5.3 (Låg)**
Säkerställa tydligt dokumenterat ansvar för funktion/medlem i ledningen som övervakar arrangemang med tredjepartsleverantörer av IKT-tjänster, inklusive samverkan med kontrollfunktioner och rapporteringsvägar till styrelsen. Åtgärdsplan är framtagen med deadline Q4 2026.

2. **Riktlinjer för användning av IKT-tjänster som stödjer kritiska eller viktiga funktioner (Medium)**
Internrevisionen rekommenderar att Bolaget ser över de styrdokument som svarar mot Bolagets riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och säkerställer att dessa innehåller alla delar som RTS 2024/1773 föreskriver ska inkluderas i riktlinjerna. Åtgärdsplan är framtagen med deadline Q4 2026.

3. **Informationsregister – rutiner, roller och FI-rapportering (Låg)**
Förtydliga i Riktlinjer för uppdragsavtal rutiner/processer för informationsregistret, ansvar/roller samt krav på minst årlig rapportering och informationsplikt till FI enligt DORA artikel 28.3 (inkl. rapportering av antal nya arrangemang m.m. och information om avtal som stödjer kritiska eller viktiga funktioner). Åtgärdsplan är framtagen med deadline Q4 2026.

4. **Dokumentation av koppling affärsfunktion ↔ IKT-/informationstillgångar (Låg)**
Säkerställa att dokumentationen tydligt visar vilka IKT-tillgångar och informationstillgångar som stödjer respektive identifierad affärsfunktion i enlighet med DORA artikel 8.1. Åtgärdsplan är framtagen med deadline Q4 2026.

9. Slutsatser från översynen

Den genomförda översynen visar att S:t Erik Försäkring har etablerat ett proportionerligt och i huvudsak ändamålsenligt IKT-riskhanteringsramverk i relation till verksamhetens art, omfattning och komplexitet.

Den samlade mognadsnivån för Bolagets digitala operativa motståndskraft bedöms vara **Etablerad**. Ramverket fungerar i praktiken och stödjer identifierade kritiska funktioner, men utvecklingsområden kvarstår avseende verifierbarhet, dokumentation och systematisk uppföljning.

Bolagets digitala operativa motståndskraft är i hög grad beroende av Stockholms stads IT-miljö och centrala kontrollfunktioner. De identifierade förbättringsområdena är främst kopplade till:

- oberoende uppföljning,
- stärkt beroendekartläggning,
- systematisk testning och dokumenterad verifiering.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

Översynen indikerar inte några väsentliga strukturella brister i ramverket. De identifierade utvecklingsområdena är hanterbara och proportionerliga i förhållande till Bolagets riskprofil.

Genom att genomföra de föreslagna åtgärderna bedöms Bolaget kunna höja sin mognadsnivå från ***Etablerad*** **mot** ***God*** och ytterligare stärka sin förmåga att verifierbart uppfylla DORA:s krav.

Bilaga – detaljerad åtgärdsplan

Förmåga	**Identifierad brist**	**Allvarlig-hetsgrad**	**Åtgärd**	**Ansvar**	**Tidsplan**
Styrning	Avsaknad av oberoende kontroll	Medel	Etablera oberoende uppföljnings-/kontrollfunktion för IKT-riskhantering inom ramen för riskfunktionen	VD	Q2 2026
Styrning	Endast kvalitativ riskaptit i dagsläget	Medel	Utvärdera om det finns behov att kvantifiera riskaptit och fastställa KRI-trösklar (RTO/RPO m.fl.)	IT-ansvarig	Q4 2026
Identifiera	Otydlig BIA-process	Medel	Tydliggöra och dokumentera BIA-metod	IT-ansvarig	Q4 2026
Identifiera	Bristande beroendekartor	Medel	Utveckla beroendekartläggningar som tydliggör samband mellan process, system och leverantör.	IT-ansvarig	Q4 2026
Skydda / upptäcka	Begränsad verifiering av leverantörers skydd och detektion	Medel	Kravställa strukturerad säkerhets- och incidentrapportering från leverantörer via stadens kontrollfunktion.	IT-ansvarig	Q4 2026
Åtgärda/Återställa	Otillräcklig testning	Medel	Inför och genomför årlig testplan för incidenthantering och avbrottsplan	IT-ansvarig	Q4 2026

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN