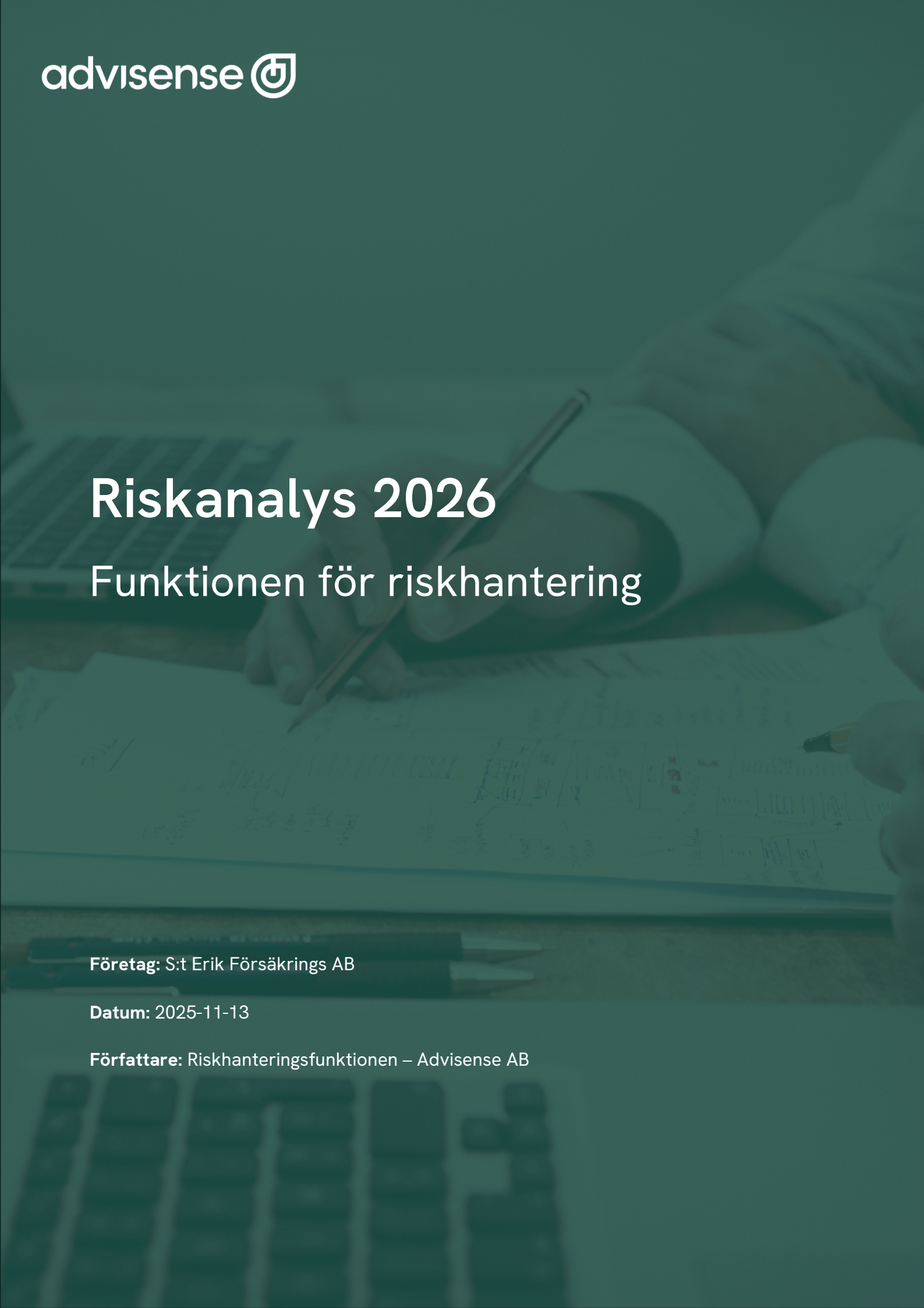


Riskanalys 2026

Funktionen för riskhantering

Företag: S:t Erik Försäkrings AB

Datum: 2025-11-13

Författare: Riskhanteringsfunktionen – Advisense AB

Innehållsförteckning

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

1. Inledning

Denna rapport sammanfattar resultatet av riskanalysen för S:t Erik Försäkrings AB (”Bolaget”) inför planeringen av Riskhanteringsfunktionens årsplan för 2026. Syftet är att ge styrelsen en helhetsbild av bolagets huvudsakliga riskområden och deras relativa betydelse, samt att skapa underlag för prioritering av uppföljning och kontroller under kommande år.

Riskhanteringsfunktionen tillämpar ett riskbaserat arbetssätt, vilket innebär att fokus läggs på områden där sannolikheten och konsekvensen av potentiella brister bedöms vara störst. Riskanalysen är därför inte en kartläggning av alla risker i verksamheten, utan en prioritering av de mest väsentliga områdena för den andra försvarslinjens arbete. Bedömningarna görs med utgångspunkt i bolagets aktuella riskregister, incidentrapportering, genomförda riskworkshops och dialoger med verksamheten.

2. Metod och bedömningsskala

Riskbedömningen baseras på sannolikhet och konsekvens, men med fokus på den kvarvarande (netto-)risken efter befintliga kontroller och processer. Syftet är inte att identifiera brister, utan att avgöra vilka riskområden som är mest väsentliga att följa upp. En hög risknivå kan därför antingen indikera svag kontrollmiljö, eller att risken är affärskritisk och förtjänar särskild uppmärksamhet.

Bedömningen görs enligt följande skala:

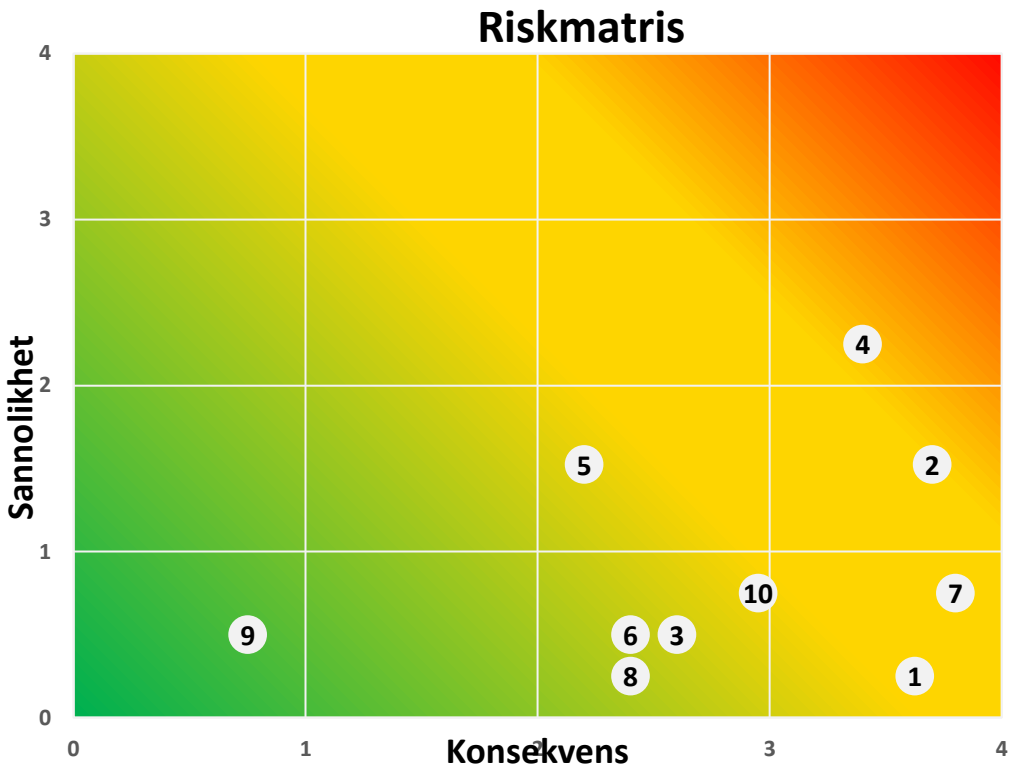
Risknivå	Beskrivning
Hög	Riskområdet bedöms som kritiskt och har hög påverkan på bolagets stabilitet eller regelefterlevnad och/eller kontrollmiljön bedöms som bristfällig eller otillräcklig. Potentiella händelser kan ge betydande påverkan på verksamhet, ekonomi eller efterlevnad. Bör prioriteras i årsplanen.
Medel	Området är väsentligt för bolagets verksamhet, men det finns etablerade kontroller och styrning. Dock kan förbättringsbehov eller ökad övervakning motiveras. Riskhanteringsfunktionen bör följa upp under året och inkludera området i flerårig planering.
Låg	Riskområdet bedöms vara välkontrollerat. Endast basövervakning krävs.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

3. Utfall av genomförd riskanalys

Riskanalysen 2025/2026 visar att den övergripande risknivån i bolaget är låg till medel. De flesta riskområden bedöms vara välhanterade genom befintliga rutiner, processer och kontroller. Det finns dock områden som fortsatt bedöms som medelstora, där riskhanteringsfunktionen föreslår uppföljning under 2026.

Den övergripande risknivån för S:t Erik Försäkrings AB bedöms vara låg. Två riskområden, IKT-risker kopplade till DORA och återförsäkringsrisker, bedöms som medel och föreslås därför följas särskilt under 2026. Bedömningen baseras på den sammanvägda analysen av konsekvens, sannolikhet och kontrollmiljö enligt den metod som presenteras i tabellen nedan.



Id	Beskrivning	Bedömning
10	Kredit och motpartsrisk	**Låg**
9	Marknadsrisk	**Låg**
3	Operativ risk	**Låg**
6	Affärsrisk	**Låg**
8	Likviditetsrisk	**Låg**
1	Försäkringsrisk	**Låg**
4	IKT-risker och efterlevnad av DORA	**Medel**
7	Klimatrisker	**Låg**
2	Återförsäkringsrisk	**Medel**
5	Regelefterlevnad	**Låg**

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

4. Identifierade risker

Under detta avsnitt beskrivs de risker som Riskhanteringsfunktionen har bedömt i verksamheten.

4.1. Försäkringsrisk

Riskvärdering: Låg

4.1.1. Definition

Med försäkringsrisk avses att skadeutfallet blir större än vad som är förväntat. Försäkringsrisken uppkommer dels vid prissättning av försäkringspremier (premierisk), dels vid uppskattning av bolagets åtagande för inträffade och kommande skador (reservsättningsrisk).

4.1.2. Riskvärdering

Bolaget tecknar idag direktförsäkring mot egendom, ansvar och olycksfall. Stora skadekostnader kan få stor påverkan på bolagets resultat. Riskerna hanteras genom att premier sätts i förnyelseprocessen i samband med upphandling av återförsäkringsprogrammen. Reservsättningen följer tydliga och uppsatta processer och rutiner som regelbundet följs upp av aktuariefunktionen.

Riskfunktionen bedömer risken som låg.

4.2. Återförsäkringsrisk

Riskvärdering: Medel

4.2.1. Definition

Risken att bolaget påverkas negativt av brister i återförsäkringsprogrammet eller motparternas finansiella ställning. Med återförsäkringsrisk avses risken för förlust ifall återförsäkringsprogrammen inte täcker de skadekostnader som förväntas av bolaget, samt risken för att återförsäkringslösning inte går att finna enligt bolagets behov.

4.2.2. Riskvärdering

Bolaget begränsar sin egen riskexponering genom att teckna återförsäkring för sina produkter. Vid teckning av sina återförsäkringsprogram har bolaget tydliga processer samt använder sig av erfarna återförsäkringsmäklare och har krav på motparters rating. Försäkringen tecknas inte ifall inte återförsäkringen är på plats vilket betyder att återförsäkringen spelar en betydande roll för bolagets

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

verksamhet. Ifall återförsäkringsprogrammen inte täcker de skadekostnader som förväntas kan förlusten för Bolaget bli omfattande. Risken bedöms väl hanterad på bolaget och följs upp av både bolaget och riskhanteringsfunktionen löpande.

Bedömningen är medel eftersom exponeringen mot vissa återförsäkrare är relativt stor. Riskhanteringsfunktionen har kontrollerat kreditbetyg vid rapportdatum, vilket visar stabila nivåer, men rekommenderar fortsatt bevakning.

Riskfunktionen bedömer risken som medel.

4.3. Operativ risk

Riskvärdering: Låg

4.3.1. Definition

Med operativ risk avses risken att Bolaget förlorar pengar till följd av icke ändamålsenliga eller misslyckade processer, mänskliga eller maskinella fel, felaktiga system eller externa händelser.

4.3.2. Riskvärdering

Bolagets operativa risker följs löpande upp minst årligen i workshop med riskhanteringsfunktionen, bolagets ledning och verksamhetskunnig personal. För risker över bolagets aptit identifieras åtgärder för hantering av risken.

Risknivån bedöms som låg tack vare väletablerade rutiner, internkontroller och tydliga attestflöden.

4.4. Information och kommunikationsrisker (IKT-risker)

Riskvärdering: Medel

4.4.1. Definition

IKT-risker definieras som risk för förlust till följd av otillräckliga eller felaktiga interna processer eller externa händelser, inklusive cyberattacker eller otillräcklig fysisk säkerhet, negativt påverkar tillgängligheten, integriteten eller konfidentialiteten i informations- och kommunikationstekniska system, eller den information som används för att tillhandahålla Bolagets tjänster.

4.4.2. Riskvärdering

Bolaget är beroende av stadens interna IT-system samt externt upphandlat försäkringssystem för att kunna upprätthålla verksamheten. Detta ställer krav på att Bolaget har kontroller av stadens och externa leverantörers skyddsåtgärder på plats mot bl.a. bedrägerier och olaglig användning av känsliga uppgifter och

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

personuppgifter, konfidentialitet, integritet och tillgänglighet för data och IT-system och fysisk säkerhet. Bolaget har beredskapsplaner och kontinuitetsplaner på plats.

Risk för brister i styrning, incidenthantering eller efterlevnad av DORA:s krav på rapportering och resiliens. Bedömningen baseras på att bolaget i nuläget har begränsad erfarenhet av att tillämpa DORA-metodiken vid bedömning av kritiska IKT-incidenter, samt beroendet av externa IT-leverantörer. Utbildning och tydligare rutiner för incidentbedömning rekommenderas under 2026.

Riskfunktionen bedömer risken som medel.

4.5. Regelefterlevnadsrisk

Riskvärdering: Låg

4.5.1. Definition

Regelefterlevnadsrisken är risken för felaktig hantering på grund av brister i efterlevnad av lagar, förordningar och andra externa föreskrifter samt interna instruktioner och riktlinjer som reglerar hur verksamheten ska bedrivas.

4.5.2. Riskvärdering

Riskhanteringsfunktionen övervakar regelefterlevnadsriskerna som följs upp löpande av regelefterlevnadsfunktionens arbete. Inga väsentliga brister har identifierats av kontrollfunktionerna.

Risken för överträdelser av interna eller externa regler bedöms som låg.

4.6. Affärsrisk

Riskvärdering: Låg

4.6.1. Definition

Affärsrisker är risker för förluster till följd av effekter av strategiska beslut, en sämre intjäning eller rykten.

4.6.2. Riskvärdering

Då bolaget är ett skadecaptive som ägs av staden och försäkrar stadens risker anses affärsrisken som begränsad.

Riskfunktionen bedömer risken som låg.

4.7. Klimatrisker

Riskvärdering: Låg

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

4.7.1. Definition

Klimatrelaterade risker avser risken för förluster relaterade till klimatförändringar. Detta omfattar både fysiska risker, såsom skyfall, stormar och översvämningar, samt omställningsrisker, det vill säga risken för finansiella effekter till följd av förändrad reglering, teknik eller beteende i samhället.

4.7.2. Riskvärdering

Bolaget försäkrar egendom, ansvar och olycksfall för Stockholms stad. De fysiska riskerna bedöms vara påtagliga och kan i ett givet skadeutfall innebära stora bruttoskador, särskilt vid skyfall eller extrema väderhändelser.

Riskens nettopåverkan bedöms dock som låg eftersom bolaget har ett omfattande återförsäkringsskydd (stop-loss och katastrofskydd) som kraftigt begränsar bolagets exponering.

Klimatrelaterade analyser genomförs i huvudsak av moderbolaget, Stockholms stad, inom ramen för stadens övergripande klimatstrategi och skyfallsanalyser.

S:t Erik Försäkrings AB integrerar dessa resultat i sitt eget arbete, framför allt i ORSA-processen, där klimatrelaterade effekter analyseras enligt Finansinspektionens krav.

Eftersom de långsiktiga analyserna ingår i den planerade ORSA-processen krävs inga särskilda aktiviteter i den ordinarie årsplanen för 2026, utöver löpande bevakning av utvecklingen.

4.8. Likviditetsrisk

Riskvärdering: Låg

4.8.1. Definition

Med likviditetsrisk menas risken att Bolaget förlorar pengar till följd av att Bolaget inte kan möta betalningsförpliktelser i tid utan att kostnaden för att tillförskaffa likviditet ökar avsevärt.

4.8.2. Riskvärdering

Bolagets likviditetsrisk hanteras genom att bolaget löpande följer upp att tillräckliga medel finns tillgängliga för att hantera den löpande verksamheten för de nästkommande månaderna.

Bedöms som låg tack vare stabil kassahantering och låg skuldsättning.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

4.9. Marknadsrisk

Riskvärdering: Låg

4.9.1. Definition

Med marknadsrisk avses risken att Bolaget förlorar pengar till följd av rörelser på exempelvis aktie-, ränte- eller valutamarknaden.

4.9.2. Riskvärdering

Bolaget hanterar marknadsrisken genom att begränsa vilka finansiella tillgångar som bolaget innehar. Bedöms som låg då placeringsstrategin är mycket försiktig och riskaptiten begränsad.

4.10. Kredit och motpartsrisk

Riskvärdering: Låg

4.10.1. Definition

Med kreditrisk, även innefattande motpartsrisk, avses risken för att Bolaget förlorar pengar till följd av att en motpart inte kan fullfölja sina åtaganden.

4.10.2. Riskvärdering

Eventuella kreditsvårigheter hos återförsäkrare har potential till stora ekonomiska konsekvenser för bolaget. Bolaget hanterar denna risk genom att tillåta återförsäkring mot motparter vars kreditbedömning enligt S&P motsvarar A- eller bättre. Vidare kontrolleras kreditbedömningen löpande upp av verksamheten under året.

Risken för att en motpart inte fullföljer sina åtaganden bedöms som låg.

5. Uppföljning

Riskanalysen uppdateras årligen och rapporteras till VD och styrelse i samband med fastställandet av riskhanteringsfunktionens årsplan.

Särskild uppmärksamhet ska under 2026 ägnas åt:

- Uppföljning av DORA-relaterade krav och incidenthantering,
- Löpande kontroll av återförsäkrarnas rating och exponering.

Avvikelser eller förändringar i risknivåer rapporteras i riskfunktionen kvartalsvis till VD och årligen till styrelsen.

ADVISENSE
ÖSTERMALMSTORG 1
114 42, STOCKHOLM
SWEDEN

S:T ERIK FÖRSÄKRINGS AB

ÅRSPLAN
Riskhanteringsfunktionen
2026

Till: Styrelsen för S:t Erik Försäkrings AB

Avsändare: Riskhanteringsfunktionen – Advisense AB
Datum: 2025-11-13

1 Bakgrund

Årsplanen är funktionen för riskhanterings (”**Riskfunktionen**”) främsta arbetsverktyg för kommande år. Årsplanen beskriver vilket arbete som kommer att utföras i S:t Erik Försäkrings AB (”**Bolaget**”) under året. En årsplans omfattning och inriktning sätter ambitionsnivån för i vilken utsträckning Riskfunktionen ska kontrollera respektive bistå med stöd till verksamheten. Ambitionsnivån i årsplanen bör relatera till styrelsens och VD:s tro om verksamhetens förmåga att efterleva regler, interna riktlinjer och principer samt Bolagets kultur.

1.1 Ansvarsfördelning

Det är VD och den operativa verksamheten (första försvarslinjen) som ansvarar för alla risker i verksamheten. Det är även den första försvarslinjen som ska hantera de risker som uppstår. Riskfunktionen, som är en del av den andra försvarslinjen, har till uppgift att kontrollera och bedöma om den första försvarslinjen äger och hanterar riskerna på ett effektivt och lämpligt sätt. Riskfunktionen ska vidare lämna råd och stöd till VD och den operativa verksamheten i syfte att förbättra detta arbete.

1.2 Vilka risker adresseras i denna årsplan?

Riskfunktionen ska arbeta riskbaserat. Det innebär att funktionens arbete främst ska vara inriktat mot de områden där de största riskerna för brister kan antas finnas. Det innebär omvänt att Riskfunktionen inte kan fokusera på Bolagets samtliga risker. Det finns således ett antal risker som inte kommer att adresseras i årsplanen.

Årsplanen bygger på den riskanalys som Riskfunktionen har gjort. De största förmodade riskerna bemöts i årsplanen genom konkreta aktiviteter såsom kontroller, råd och stöd-aktiviteter eller utbildningar. Det innebär vidare att de risker som inte identifierats/tagits med i riskanalysen inte kommer mitigeras genom aktiviteter i årsplanen. Det ska vidare förtydligas att Riskfunktionen t.ex. inte ansvarar för risker relaterade till skattefrågor, bolagsjuridik, redovisnings- och revisionsfrågor[1] eller konkurrensrättsliga frågor.

För 2026 har en riskanalys genomförts i syfte att kartlägga var de största riskerna kan finnas i Bolagets tillståndspliktiga verksamhet. I riskanalysen har även riskerna prioriterats inbördes utifrån förmodad allvarlighet. I årsplanen beskrivs vilka aktiviteter som ska utföras, vilken typ av aktivitet som avses samt kort om hur aktiviteten ska utföras. Årsplanen kan komma att ändras under verksamhetsåret ifall interna eller externa händelser uppstår eller om prioriteringen av andra skäl behöver ändras. I avsnitt 2 nedan följer årsplanen för Bolaget för verksamhetsåret 2026.

[1] Vid sidan av intern styrning och kontroll.

2 Årsplan för riskhanteringsfunktionen 2026

2.1 Löpande aktiviteter

Nr	Aktivitet	Beskrivning av aktivitet	Period
1	Kontroll av solvens	Kontroll av solvenspositionen samt uppföljning av dess utveckling över tid.	Kvartal
2	Risk- och åtgärdsuppföljning	Uppföljning av risker samt planerade åtgärder	Kvartal
3	Riskanalys inför större beslut	I samband med att affärsbeslut fattas eller outsourcing beslutas kontrollera att tillfredsställande riskanalyser utförts.	Vid behov
4	Styrdokument	Översyn och eventuell revidering av riskrelaterade styrdokument.	År
5	Utbildning	Utbildning av personal eller styrelse inom till exempel riskrelaterade regelverk, riskhantering och kontroll av risker.	Vid behov
6	Incidentuppföljning	Uppföljning av inträffade incidenter, kontroll av incidentrapportering samt stödja verksamheten i att utarbeta förbättringsåtgärder.	Kvartal

2.2 Periodiska aktiviteter

Nr	Aktivitet	Beskrivning av aktivitet	Period
1	Kvartalsrapport	Riskhanteringsfunktionen ska till minst fyra av styrelsens möten avlägga en aktuell sammanfattande riskrapport.	Kvartalsvis
2	ORSA-process	Riskhanteringsfunktionen ska biträda styrelse och VD i genomförandet av bolagets ORSA-process i enlighet med ”Policy för ORSA”, och utföra de uppgifter som framgår där.	Enligt ORSA-process
3	Kvalitativ rapportering	Riskhanteringsfunktionen ska administrera processen och bistå i författningen av SFCR och RSR rapporteringen till Finansinspektionen.	Kvartal 1
4	Årsrapport	Årsrapport som beskriver funktionens arbete under 2025 och redogör för hur den årsplanen genomförts.	Kvartal 1
5	Riskregister	Uppdatering av bolagets riskregister för operativa risker och affärsrisker.	Kvartal 4
6	Incidentrapport	Skriftlig incidentrapport med en samlad analys av inträffade incidenter, uppföljning av vidtagna åtgärder och förslag till ytterligare förbättringar.	Kvartal 4
7	Årsplan	Framtagande av förslag till årsplan för verksamhetsåret 2027.	Kvartal 4

2.3 DORA-relaterade aktiviteter

För 2026 fokuserar Riskhanteringsfunktionen särskilt på uppföljning av IKT-risker i enlighet med DORA och Finansinspektionens vägledning om proportionerlig tillämpning.
Aktiviteterna nedan är anpassade till bolagets storlek, verksamhetens komplexitet och den risknivå som identifierats i riskanalysen.

Nr	Riskkategori	Aktivitet	Beskrivning av aktivitet	Period
1	IKT-risker	IKT-riskworkshop	Genomföra en workshop med IT-ansvarig och verksamhetsföreträdare för att identifiera och bedöma IKT-risker, inklusive risker kopplade till incidenthantering, tredjepartsberoenden och kontinuitet. Resultatet utgör underlag för DORA-översynen och ORSA-processen. Riskfunktionen följer upp att första linjen har identifierat och hanterar relevanta IKT-risker.	Årsvis
2	IKT-risker	Uppföljning av IKT incidenthantering	Granska rapportering och analys av inträffade IKT-incidenter, inklusive bedömning av om incidenter klassats korrekt utifrån DORA-kriterier.	Kvartalsvis
3	IKT-risker	Granskning av leverantörs- och tredjepartsrisker	Kontrollera att uppföljning av leverantörer med kritiska IKT-tjänster sker och att riskbedömningar uppdateras.	Årsvis
4	IKT-risker	Utvärdering av IKT-testramverk	Översiktligt bedöma att tester av operativ resiliens (t.ex. återställning, åtkomst, säkerhet) sker enligt plan och att resultat samt identifierade brister används i förbättringsarbete.	Årsvis
5	IKT-risker	Bedömning av kontinuitetsplaner	Säkerställa att IKT-kontinuitets- och återställningsplaner finns och testas i rimlig omfattning, samt att resultat återkopplas till ledning. Bedömningen görs i samverkan med IT-funktion vid behov.	Årsvis
6	IKT-risker	Granskning av förändringsrisker	Bedöma riskhanteringen vid införande av nya leverantörer, större systemuppdateringar eller förändringar i ansvarsfördelning.	Vid behov
7	IKT-risker	Bidrag till ORSA-processen	Säkerställa att IKT-relaterade risker inkluderas i ORSA och att analysen är proportionerlig och relevant i förhållande till bolagets exponering.	Enligt ORSA planen
8	IKT-risker	Riskrapportering	Sammanställa DORA-relaterade observationer, incidenter och status i riskrapporteringen till VD och styrelsen.	Kvartalsvis
9	IKT-risker	Årlig översyn av IKT-riskhanteringsramverket (DORA-review)	Genomföra den formella oberoende översynen enligt artikel 6.5 DORA. Inkluderar bedömning av styrning, riskprocesser, incidenthantering, testning, kontinuitet, leverantörer och rapportering. Resultatet rapporteras till VD och styrelsen.	Årsvis
10	IKT-risker	Uppföljning av åtgärder	Följa upp genomförandet av identifierade förbättringsåtgärder från incidenter, internrevisioner eller DORA-översynen.	Årsvis
11	IKT-risker	Stöd och rådgivning	Bidra till ökad medvetenhet och förståelse kring DORA och IKT-riskhantering, exempelvis genom utbildningar eller workshops.	Vid behov

3 Tidsestimat 2026

Det bedöms att genomförandet av ovanstående aktiviteter kommer att omfatta cirka 180 timmar, varav cirka 50 timmar avser IKT-relaterade aktiviteter i enlighet med den DORA-relaterade aktivitetslistan ovan.

Angivet timantal utgör en preliminär uppskattning och kan komma att justeras beroende på faktisk arbetsbelastning och prioriteringar under året.