S:t Erik FÖRSÄKRING EN DEL AV STOCKHOLMS STAD

STATUSRAPPORT
IKT-RISKHANTERING

Uppföljning av åtgärdsplan och digital operativ motståndskraft

Status per 24 augusti 2026

Till:	Styrelsen och verkställande direktören för S:t Erik Försäkrings AB
Avsändare:	Advisense, Riskhanteringsfunktionen
Rapportdatum:	7 september 2026
Konfidentiell status:	Konfidentiell internt och externt

Innehåll

Sammanfattning

Denna rapport redovisar riskhanteringsfunktionens uppföljning av de åtgärder som identifierades i den årliga översynen av S:t Erik Försäkrings AB:s IKT-riskhanteringsramverk. Uppföljningen bygger på verksamhetens rapporterade status per den 24 augusti 2026 samt tidigare incidentunderlag.

Den tidigare översynen bedömde Bolagets övergripande IKT-riskprofil som låg till medel och den samlade mognadsnivån för digital operativ motståndskraft som Etablerad. I den aktuella uppföljningen har verksamheten inte rapporterat några väsentliga förändringar i IKT-miljön, några nya eller förändrade IKT-risker eller någon risk som ligger utanför fastställd riskaptit.

Övergripande IKT-risknivå	**Låg till medel – oförändrad bedömning**
Samlad mognadsnivå	**Etablerad – ingen grund för uppgradering ännu**
Rapporterad åtgärdsstatus	**2 av 10 genomförda; 8 av 10 pågående enligt plan**
Verifierad stängning	**0 av 10 inom denna uppföljning**
Väsentliga förändringar / nya IKT-risker	Inga rapporterade
Stödjande underlag i statusfilen	Inga evidenshänvisningar eller bilagor angivna

Riskhanteringsfunktionens samlade slutsats

Utvecklingen går i rätt riktning och samtliga öppna åtgärder uppges löpa enligt plan. Merparten av åtgärderna befinner sig dock fortfarande i planerings- eller utvecklingsfas. Den samlade mognadsnivån bedöms fortsatt vara Etablerad.

1 Bakgrund, syfte och avgränsning

Riskhanteringsfunktionen genomförde under första kvartalet 2026 en översyn av Bolagets IKT-riskhanteringsramverk i enlighet med DORA artikel 6.5 och det rapportformat som anges i RTS 2024/1774 artikel 27. Rapporten upprättades den 9 mars 2026 och fastställdes av styrelsen den 13 mars 2026.

Översynen visade att Bolaget hade etablerat ett proportionerligt och i huvudsak ändamålsenligt ramverk. Samtidigt identifierades utvecklingsområden avseende oberoende uppföljning, kvantifierad riskaptit, BIA, beroendekartläggning, leverantörsverifiering samt testning av incident- och kontinuitetsförmågan.

Syftet med denna rapport är att ge styrelsen en samlad bild av genomförandestatusen, bedöma kvarstående risker och ange vilka åtgärder som behöver prioriteras inför utgången av 2026.

1.1 Underlag

- Rapport om översyn av IKT-riskhanteringsramverket för S:t Erik Försäkrings AB, upprättad 9 mars 2026 och fastställd av styrelsen 13 mars 2026.
- Den ifyllda statusuppföljning av åtgärdsplan och internrevisionens rekommendationer, status per 24 augusti 2026.
- Incidentöversikt och incidentrapporter för perioden 1 januari–31 juli 2026.

1.2 Avgränsning och verifieringsnivå

Uppföljningen baseras på den status som första försvarslinjen har lämnat. Bedömningen kan verifiera att aktiviteter har initierats och rapporterats, men inte att kontrollernas utformning eller operativa effektivitet fullt ut har styrkts.

Viktig statusprincip

I rapporten används uttrycket ”rapporterad som genomförd” för åtgärder som verksamheten markerat som klara. ”Verifierad och stängd” används först när riskhanteringsfunktionen har fått tillräckligt underlag för att bedöma att åtgärden är ändamålsenligt genomförd.

2 Övergripande status för åtgärdsplanen

Den detaljerade åtgärdsplanen från IKT-översynen omfattar sex utvecklingsområden, samtliga ursprungligen bedömda med allvarlighetsgrad Medel. Därutöver omfattar uppföljningen fyra rekommendationer från internrevisionen, varav en med riskklassificering Medel och tre med riskklassificering Låg.

Verksamheten har rapporterat två av totalt tio åtgärder som genomförda och åtta som pågående enligt plan. Ingen åtgärd har rapporterats som försenad eller ej påbörjad. I avsaknad av uppdaterade slutdatum utgår rapporten från de ursprungliga tidsplanerna.

2.1 Åtgärder från IKT-översynen

Åtgärd	Kundens rapporterade status	Riskhanteringsfunktionens bedömning
Styrning – oberoende kontroll Etablera oberoende uppföljning och kontroll av IKT-riskhantering inom riskfunktionen.	**Genomförd**	
Styrning – riskaptit och KRI Utvärdera behov av kvantitativa trösklar, inklusive RTO/RPO.	**Pågående enligt plan Klassningarnas RTO/RPO ska ses över och föras in i avbrottsplanen.**	Arbetet är relevant men ännu inte färdigställt. Beslutade värden, mätmetod, ägare, rapporteringsfrekvens och eskaleringsnivåer behöver framgå.
Identifiera – BIA Tydliggöra och dokumentera Bolagets BIA-metod.	**Pågående enligt plan Möjlig integrering i avbrottsplanen. En generell BIA-beskrivning har lämnats.**	Det generella metodstödet behöver omsättas i en bolagsspecifik och beslutad metod med kritiska funktioner, konsekvenskriterier, RTO/RPO, roller och uppdateringsfrekvens.
Identifiera – beroendekartläggning Tydliggöra samband mellan process, system och leverantör.	**Pågående enligt plan Brainstorming mellan IT-ansvarig, bolagsjurist och VD.**	Arbetet befinner sig i en tidig fas. En sammanhållen och förvaltad beroendekarta har inte visats i uppföljningen.
Skydda/upptäcka – leverantörsverifiering Kravställa strukturerad säkerhets- och incidentrapportering.	**Pågående enligt plan Arbete avses ske via CERT Stockholm, stadens nya LIS 2.0 och kontakt med ansvarig funktion inom staden.**	Inriktningen är relevant. Det behöver tydliggöras vilka rapporter som ska erhållas, med vilken frekvens, hur avvikelser ska följas upp och hur Bolaget sparar evidens.
Åtgärda/återställa – testning Införa och genomföra årlig testplan för incidenthantering och avbrottsplan.	**Pågående enligt plan Aktiviteten ska läggas in i årshjul, planeras, genomföras och dokumenteras.**	Åtgärden är ännu inte operativt genomförd. Testplan, scenario, deltagare, mål, resultat, brister och åtgärdsuppföljning behöver dokumenteras.

2.2 Internrevisionens rekommendationer

Rekommendation	Kundens rapporterade status	Riskhanteringsfunktionens bedömning
Dokumenterat ansvar enligt DORA artikel 5.3 Tydliggöra ansvar för övervakning av IKT-tredjepartsarrangemang.	**Genomförd – rapporterad**	
Riktlinjer för IKT-tjänster som stödjer kritiska eller viktiga funktioner.	**Pågående enligt plan.**	Uppdaterat styrdokument och genomförd gapkontroll mot tillämpliga krav behöver lämnas för verifiering.
Informationsregister – rutiner, roller och FI-rapportering.	**Pågående enligt plan**	Processägare, uppdateringsrutin, kvalitetssäkring och rapporteringskalender behöver dokumenteras.
Dokumentation av koppling mellan affärsfunktioner och IKT-/informationstillgångar.	**Pågående enligt plan**	Bör samordnas med beroendekartläggningen så att en gemensam, spårbar och underhållen dokumentation etableras.

3 Riskhanteringsfunktionens bedömning per förmåga

Bedömningen nedan följer samma förmågestruktur som den ursprungliga översynen. Den utgår från rapporterad status, den information som lämnats om genomförandet samt graden av tillgänglig verifiering.

3.1 Styrning

Det är positivt att både den oberoende kontrollfunktionen och det dokumenterade ledningsansvaret för IKT-tredjepartsarrangemang har rapporterats som genomförda. Dessa åtgärder adresserar två centrala styrningsfrågor från den tidigare översynen.

Samtidigt saknas i den lämnade statusen dokumentation som visar mandat, ansvarsfördelning mellan försvarslinjerna, kontrollplan, rapporteringsvägar och hittills genomförda oberoende kontroller. Arbetet med kvantitativ riskaptit och KRI är pågående och har ännu inte resulterat i beslutade tröskelvärden.

Bedömning – Styrning

Förmågan bedöms fortsatt som Etablerad. För att närma sig nivån God behöver de rapporterade styrningsförbättringarna kunna verifieras och KRI/RTO/RPO operationaliseras i ordinarie rapportering och eskalering.

3.2 Identifiera

Arbetet med BIA och beroendekartläggning uppges vara pågående enligt plan. Den bifogade BIA-fliken innehåller generell vägledning om att identifiera kritiska processer, störningsscenarier, konsekvenser, varaktighet och riskreducerande åtgärder. Den visar däremot inte en bolagsspecifik metod eller ett genomfört resultat.

För att åtgärden ska anses genomförd behöver Bolaget dokumentera hur kritiska eller viktiga funktioner kopplas till processer, information, system, integrationer, leverantörer och underleverantörer. BIA:n bör innehålla fastställda konsekvenskriterier, maximalt tolererbar avbrottstid, RTO/RPO, manuella reservrutiner, ägarskap, godkännande och uppdateringsintervall.

Bedömning – Identifiera

Förmågan bedöms fortsatt som Etablerad. Arbetet har initierats, men de viktigaste leverablerna – bolagsspecifik BIA och sammanhållen beroendekarta – har ännu inte visats.

3.3 Skydda och upptäcka

Bolaget avser att stärka verifieringen av leverantörernas skydds- och detektionsförmåga genom CERT Stockholm, stadens nya LIS 2.0 samt dialog med ansvarig funktion inom Stockholms stad. Detta är i linje med den tidigare identifierade verifierbarhetsutmaningen.

Uppföljningen visar dock ännu inte vilka rapporter, nyckeltal eller kontrollresultat som ska erhållas, hur ofta rapporteringen ska ske eller hur avvikelser ska eskaleras och följas upp. De interna revisionsrekommendationerna om riktlinjer och informationsregister är också fortfarande öppna.

Bedömning – Skydda och upptäcka

Förmågan bedöms fortsatt som Etablerad. Kontrollmiljön bedöms finnas i praktiken, men Bolagets självständiga verifierbarhet är ännu inte tillräckligt dokumenterad.

3.4 Åtgärda och återställa

Bolaget avser att föra in testning i årshjulet och därefter planera, genomföra och dokumentera övningar. Detta innebär att åtgärden ännu främst är planerad och att någon genomförd, dokumenterad testning inte har redovisats i uppföljningen.

För att stärka den digitala operativa motståndskraften bör testplanen omfatta incidenthanteringsprocessen, manuella reservrutiner, avbrottsplaner och återställning av kritiska system. Resultaten bör jämföras med fastställda RTO/RPO och leda till dokumenterade åtgärder.

Bedömning – Åtgärda och återställa

Förmågan bedöms fortsatt som Etablerad. Planer finns, men den praktiska återställningsförmågan har ännu inte verifierats systematiskt genom dokumenterade tester.

4 IKT-relaterade incidenter och lärdomar

Under perioden 1 januari–17 augusti 2026 har sex händelser registrerats i incidentöversikten. Fyra av dessa bedöms vara faktiska incidenter och två avser testregistreringar.

Datum	Händelse	Kort bedömning
2026-01-07	Avbrott i telefoniväxel för olycksfall	Kortare tillgänglighetsstörning; tjänsten återställdes samma dag.
2026-03-05	Avbrott i incidentrapporteringssystemet IA	Leverantörsrelaterat avbrott efter uppdatering; systemet låg nere cirka tre timmar.
2026-03-10	Problem med Min Sida	Fel efter proxyuppgradering; nyregistrerade skador överfördes inte korrekt till Insman. Hotfix genomfördes.
2026-05-28	Driftstopp i incidentrapporteringssystemet	Systemet var otillgängligt i sju dagar efter planerad uppdatering och hade fortsatta funktionsproblem.
2026-01-27 och 2026-06-17	Testregistreringar	Testposter; inga faktiska incidenter eller verksamhetspåverkan.

Verksamheten har i den kompletterande uppföljningen svarat att incidenterna inte har lett till förändringar i exempelvis förändringshantering, leverantörsuppföljning, kontinuitetsplanering, incidentklassificering eller testning.

Riskhanteringsfunktionen bedömer att avsaknaden av förändringar inte i sig behöver innebära en brist, men att analysen och ställningstagandet bör dokumenteras. Flera händelser har varit relaterade till systemuppdateringar eller externa leverantörer. Driftstoppet i incidentrapporteringssystemet under sju dagar är särskilt relevant för BIA, RTO/RPO, manuella reservrutiner, leverantörsrapportering och testplanering.

Rekommenderad incidentuppföljning

Genomför en dokumenterad lessons-learned-genomgång av 2026 års incidenter. Bedöm särskilt om fastställd eller förväntad återställningstid överskreds, om reservrutiner fungerade, om leverantörens rotorsaksanalys är tillräcklig och om förändrings- eller testkontroller behöver stärkas.

5 Samlad risk- och mognadsbedömning

Inga väsentliga förändringar i IKT-miljön, leverantörsberoendena, integrationerna eller de kritiska och viktiga funktionerna har rapporterats. Inte heller har nya eller förändrade IKT-risker rapporterats. Det finns därmed inget underlag i den aktuella uppföljningen som indikerar en väsentlig försämring av Bolagets IKT-riskprofil.

Samtidigt kvarstår huvuddelen av de utvecklingsområden som identifierades i den tidigare översynen. De öppna åtgärderna avser centrala förutsättningar för verifierbar digital operativ motståndskraft: mätbara toleranser, verksamhetsspecifik BIA, beroendekartläggning, leverantörsuppföljning, styrdokument, informationsregister och praktisk testning.

Bedömningsområde	Nivå	Motivering
Övergripande IKT-riskprofil	**Låg till medel**	Oförändrad miljö och inga nya risker har rapporterats, men beroende- och verifierbarhetsriskerna kvarstår.
Digital operativ motståndskraft	**Tillräcklig men utvecklingsbar**	Grundläggande strukturer finns, men flera centrala förmågor är ännu inte fullt dokumenterade eller testade.
Samlad mognadsnivå	**Etablerad**	Åtgärdsarbetet pågår, men underlaget ger inte tillräcklig grund för en uppgradering till God.
Behov av omedelbar eskalering	**Nej**	Ingen ny risk utanför riskaptit eller försening har rapporterats; Q4-leveranser och evidens behöver följas nära.

5.1 Kvarstående huvudsakliga risker

- Strukturell koncentration och beroende av Stockholms stads gemensamma IT-miljö och externa leverantörer.
- Begränsad självständig verifiering av skydds-, detektions- och återställningskontroller hos leverantörer.
- Otillräckligt dokumenterad koppling mellan kritiska funktioner, processer, system, information och leverantörer.
- Avsaknad av verifierad, bolagsspecifik BIA med beslutade RTO/RPO och tillhörande KRI-trösklar.
- Återställnings- och incidentförmågan har ännu inte verifierats genom en genomförd och dokumenterad årlig testplan.

6 Riskhanteringsfunktionens rekommendationer

1. Evidens och stängning: Komplettera statusloggen med dokumenthänvisningar, ansvarig, aktuellt slutdatum och kvarstående arbete. De två åtgärder som rapporterats som genomförda bör verifieras innan de stängs.

2. KRI, RTO/RPO och BIA: Fastställ en bolagsspecifik BIA-metod och beslutade RTO/RPO per kritisk eller viktig funktion. Definiera KRI, trösklar, rapporteringsfrekvens och eskaleringsnivåer.

3. Beroendekarta: Färdigställ och förvalta en sammanhängande karta mellan funktion, process, information, system, integration, leverantör och underleverantör.

4. Leverantörsverifiering: Formaliserad säkerhets-, incident-, kontinuitets- och testuppföljning bör etableras via stadens kontrollfunktion, CERT Stockholm och relevanta LIS-processer.

5. Testning och incidentlärande: Fastställ en årlig testplan, genomför minst en dokumenterad övning och koppla resultaten samt lärdomar från 2026 års incidenter till förbättringsåtgärder.

6. Internrevisionens öppna rekommendationer: Slutför uppdatering av styrdokument, informationsregisterprocess och koppling mellan affärsfunktioner och IKT-/informationstillgångar senast Q4 2026.

7 Föreslagen fortsatt rapportering

Riskhanteringsfunktionen föreslår att en förnyad status- och evidensuppföljning genomförs efter utgången av Q4 2026. Uppföljningen bör särskilt redovisa vilka åtgärder som har verifierats och stängts, eventuella förseningar, resultat från genomförda tester samt om mognadsnivån kan höjas från Etablerad mot God.

> **Nästa kontrollpunkt**
>
> Senast i samband med nästa årliga översynen av IKT-riskhanteringsramverket bör styrelsen få en verifierad slutstatus för samtliga tio åtgärder.

Bilaga 1 – Samlad åtgärdsstatus

Tabellen sammanfattar verksamhetens rapporterade status per den 24 augusti 2026. ”Verifierad” innebär att riskhanteringsfunktionen har fått tillräckligt underlag för att bedöma åtgärdens genomförande. Ingen åtgärd har verifierats inom ramen för denna uppföljning.

Nr	Åtgärd / rekommendation	Rapporterad status	Verifierad	Nästa verifieringsunderlag
1	Oberoende uppföljnings-/kontrollfunktion	**Genomförd – rapporterad**	**Delvis**	Mandat, ansvarsfördelning, kontrollplan, rapportering och utförda kontroller.
2	Kvantitativ riskaptit och KRI-trösklar	**Pågående enligt plan**	**Nej**	Beslutade RTO/RPO, KRI, trösklar, ägare och rapporteringsrutin.
3	Tydlig och dokumenterad BIA-metod	**Pågående enligt plan**	**Nej**	Bolagsspecifik metod, kriterier, resultat, ansvar och godkännande.
4	Beroendekartläggning process–system–leverantör	**Pågående enligt plan**	**Nej**	Fastställd karta, ägare, uppdateringsrutin och användning vid incident.
5	Strukturerad säkerhets- och incidentrapportering från leverantörer	**Pågående enligt plan**	**Nej**	Krav, rapportformat, frekvens, mottagna rapporter och avvikelsehantering.
6	Årlig testplan för incidenthantering och avbrottsplan	**Pågående enligt plan**	**Nej**	Fastställd plan, genomförd övning, resultat och åtgärdslogg.

7	Dokumenterat ledningsansvar enligt DORA artikel 5.3	**Genomförd – rapporterad**	**Nej**	Fastställt ansvar, samverkan och rapporteringsväg till styrelsen.
8	Riktlinjer för kritiska eller viktiga IKT-tjänster	**Pågående enligt plan**	**Nej**	Reviderat styrdokument och dokumenterad gapkontroll.
9	Informationsregister – rutiner, roller och FI-rapportering	**Pågående enligt plan**	**Nej**	Processbeskrivning, ansvar, kvalitetssäkring och rapporteringskalender.
10	Koppling affärsfunktion–IKT-/informationstillgångar	**Pågående enligt plan**	**Nej**	Spårbar dokumentation, ägarskap och uppdateringsrutin.