Internrevisionsrapport

2022.02 – Företagsstyrning avseende informations- och kommunikationsteknik (IKT)

S:t Erik Försäkrings AB
2022-12-06

Utgivare: Internrevisionen, Grant Thornton Sweden AB

Mottagare: Styrelse och VD, S:t Erik Försäkrings AB

KONFIDENTIELL/FÖR INTERN ANVÄNDNING

Granskningens bakgrund och omfattning

Inledning och bakgrund

Komplexiteten ökar inom IKT-området, och förekomsten av IKT-relaterade incidenter (inbegripet cyberincidenter) blir allt vanligare. Vidare blir de negativa konsekvenserna av sådana incidenter för företags operativa verksamhet allt allvarligare. Av detta skäl är hantering av IKT-risker av avgörande betydelse för att företag ska kunna uppnå sina strategiska, företagsmässiga, operativa och anseendemål. I försäkringssektorn, både inom traditionella och innovativa affärsmodeller, ökar dessutom tilltron på IKT för tillhandahållandet av försäkringstjänster och IKT spelar ofta en central roll för företagens normala operativa funktionssätt. Detta gör företags verksamhet sårbar för IT-säkerhetsincidenter, däribland cyberattacker. Det är därför viktigt att se till att företag är tillräckligt förberedda för att hantera sina IKT-risker.

Syfte och omfattning

Internrevisionen har övergripande granskat och utvärderat ändamålsenligheten i S:t Erik Försäkrings AB:s (”Bolaget”) företagsstyrning avseende informations- och kommunikationsteknik. Vidare har granskningen omfattat Bolagets styrning för att hantera IKT-risker som en del av företagets allmänna riskhanteringssystem. Granskningen har avgränsats till att endast på en övergripande nivå, med ett riskbaserat förhållningssätt behandla de fokusområden som redovisas till höger.

Fokusområden:

- IKT strategi och IKT i företagsstyrningssystemet
- IKT-risker i riskhanteringssystemet
- Policy och åtgärder för informationssäkerhet
- Informationssäkerhetsfunktion
- Säkerhet för IKT-verksamhet
- Granskningar, bedömning och testning av informationssäkerhet
- Utbildning och medvetenhet avseende informationssäkerhet
- Hantering av IKT-incidenter och IKT-problem
- IKT-ändringshantering
- Hantering av driftskontinuitet, kontinuitetsplanering och återställningsplaner
- Utkontraktering av IKT-tjänster och IKT-system

Regulatorisk referens:

- Direktiv 2009/138/EG (Solvens II direktivet), artiklarna 41 och 44
- EIOPA:s Riktlinjer för säkerhet och företagsstyrning avseende informations och kommunikationsteknik Bos – 20/600

Sammanfattning av resultat

IKT-risker har ökat de senaste åren till följd av ökad digitalisering och utgör idag betydande risker för företag. IKT-risker som inte identifieras och hanteras kan få allvarlig negativ påverkan på företags verksamhet. Av denna anledning är effektiv och välfungerande hantering av IKT-risker grundläggande för att företag ska uppnå sina mål. S:t Erik Försäkrings AB har inom ramen för sitt företagsstyrningssystem identifierat IKT-risker och har etablerat rutiner, processer och kontroller för att hantera IKT-risker. Dessa rutiner, processer och kontroller har dokumenterats i Bolagets styrdokument i form av t.ex. Bolagets IKT-riktlinjer.

Bolaget är, vad gäller IKT, i stor utsträckning beroende av Stockholms stad. I tillägg till detta använder sig Bolaget även av ett system vid namn Insman för att hantera försäkringsärenden. Detta system tillhandahålls av en extern systemleverantör. Mot denna bakgrund kan konstateras att Bolaget i stor utsträckning är beroende av andra parter för sin IKT-verksamhet, varför det blir centralt för Bolaget att säkerställa att dessa parter har adekvata och ändamålsenliga processer, rutiner och kontroller för att hantera IKT-risker. Internrevisionen har, inom ramen för genomförd granskning, uppmärksammat att det finns ett pågående arbete med att hantera IKT-risker på Bolaget. Inom ramen för detta arbete har Bolaget bl.a. anställt en person med kunskap inom IKT som internrevisionen uppfattar ska vara med och driva Bolagets arbete inom området.

Internrevisionens bedömning är att Bolagets arbete med intern styrning och kontroll avseende IKT delvis är formaliserat. För att förflytta sig mot en mer formaliserad nivå rekommenderas stärkande åtgärder främst kopplat till uppföljning, utvärdering och övervakning relaterat till IKT-verksamhet. Den sammanfattande bedömningen efter granskningen är att det föreligger **förbättringsbehov.**.

Internrevisionen lämnar tre rekommendationer baserat på iakttagelser som gjorts. Rekommendationerna är klassade som **Medium risk,** vilket implicerar ett utvecklingsområde / brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en medium residual risk som ensam, eller i kombination med andra brister, kan påverka, processer och / eller kontroller, leda till anmärkningar från tillsynsmyndigheter alternativt indikera betydande potential för effektivisering. Det rekommenderas att ledningen vidtar åtgärder mot bakgrund av rekommendationen inom en rimlig tidsram.

#	Fokusområde	Rekommendation	Risknivå
2022.02.1	Policy och åtgärder för informationssäkerhet	Bättre överensstämmelse mellan styrdokument och praktiskt utförande bör säkerställas	Medium
2022.02.2	Hantering av driftskontinuitet, kontinuitetsplanering och återställningsplaner	Testning av kontinuitets-/avbrottsplan bör säkerställas	Medium
2022.02.3	Utkontraktering av IKT-tjänster och IKT-system	Effektiv och ändamålsenlig övervakning, uppföljning och utvärdering av IKT-leverantörer bör etableras	Medium

2022.02.1 Bättre överensstämmelse mellan styrdokument och praktiskt utförande bör säkerställas

Medium

Policy och åtgärder för informationssäkerhet

Kriterium	IKT-RIKTLINJER I S:T ERIK FÖRSÄKRINGS AB, avsnitt 8 (1 st.) *”Bolaget ska regelbundet genomföra en kartläggning över Bolagets affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar). Syftet med kartläggningen är att identifiera deras betydelse och ömsesidiga beroendeförhållanden beträffande IKT-risker och säkerhetsrisker.”* IKT-RIKTLINJER I S:T ERIK FÖRSÄKRINGS AB, avsnitt 13 (1 st.) *”Bolagets styrning, system och processer för IKT-risker och säkerhetsrisker ska vid behov genomgå revision. Är systemet kritiskt ska revision utföras minst årligen. Sådan revision ska utföras av revisorer eller motsvarande med tillräcklig kunskap, kompetens och expertis inom IKT-risker och säkerhetsrisker för att kunna lämna en oberoende försäkran om deras effektivitet till Bolagets styrelse och vd.”* RIKTLINJER FÖR RISKHANTERING I S:T ERIK FÖRSÄKRINGS AB, avsnitt 6.2 (3 st.) *”Varje identifierad risk skall ha en riskägare, d.v.s. en person som är ansvarig för att övervaka riskens utveckling och kontrollera att beslutade åtgärder efterlevs. Bolaget ska föra ett riskregister som utgör en sammanställning av alla väsentliga riskgrupper och undergrupper, med angivande av vem som är riskägare, riskaptit, ytterligare risklimiter samt i vilka styrdokument relevanta element i riskhanteringssystemet framgår för respektive riskgrupp eller undergrupp.”*
Observation	Internrevisionen noterar att vad som finns beskrivet i Bolagets IKT-riktlinjer och riktlinjer för riskhantering inte i alla avseende speglar vad Bolaget faktiskt gör. I detta avseende noteras särskilt att Bolaget enligt 8.1 i Bolagets IKT-riktlinjer ska genomföra en kartläggning för att bl.a. identifiera ömsesidiga beroendeförhållanden beträffande IKT-risker, något som Internrevisionen uppfattar att Bolaget inte gjort i praktiken. Vidare noteras att Bolaget inte tidigare utfört någon revision av styrning, system och processer för IKT-risker, samt att IKT-risker inte tilldelats en specifik person som riskägare.
Risk	Internrevisionen bedömer att det faktum att vad som föreskrivs i styrdokument inte efterlevs i praktiskt hänseende kan innebära en ökad risk för otydligheter och bristande struktur i intern styrning och kontroll. Vidare kan avsaknaden av revision avseende IKT-risker och kartläggning enligt avsnitt 8.1 respektive 13 i bolagets IKT-riktlinjer innebära en ökad risk för att IKT-risker inte identifieras och hanteras på ett tillfredställande sätt.
Rekommendation	Internrevisionen rekommenderar att Bolaget ser över praktiskt utförande och vad som föreskrivs i styrdokument för att säkerställa en överrensstämmelse. I detta avseende uppfattar internrevisionen att Bolaget t.ex. vad gäller riskägare avser använda sig av en verksamhetsfunktion som riskägare, varför det i detta fall kan vara lämpligt att uppdatera formuleringen i Bolagets riktlinjer för riskhantering istället för att justera det praktiska utförandet. I andra fall kan det vara möjligt att ha kvar skrivningar i styrdokument och istället justera praktiskt utförande beroende vad Bolaget bedömer lämpligt. Om Bolaget har för avsikt att ha kvar skrivningen om revision som refererats ovan bör Bolaget säkerställa att i vart fall kritiska system identifieras och genomgår årlig revision. Liknande gäller för skrivningen om kartläggning som också referats ovan där Bolaget bör säkerställa att skrivningen efterlevs i praktiken om Bolaget avser har kvar formuleringen i nuvarande form.
Ledningens åtgärdsplan:	Den nya funktionen IT-ansvarig kommer att se över och utarbeta precesser för kontroll, revision m.m. och dessa kommer att stämmas av mot gällande styrdokument. Vid behov kommer styrdokumenten att revideras. Arbetet kommer att ske i samverkan med regelefterlevnadsfunktionen och riskhanteringsfunktionen.
Ansvarig och deadline:	IT-ansvarig under 2023.

2022.02.2 Testning av kontinuitets-/avbrottsplan bör säkerställas	Medium
Hantering av driftskontinuitet, kontinuitetsplanering och återställningsplaner	
Kriterium	EIOPA-BoS-20/600, Riktlinje 23 – Testning av planer *74. Företag bör testa sina kontinuitetsplaner och se till att driften av deras kritiska affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar) liksom IKT-tillgångar och deras ömsesidiga beroendeförhållanden (också de som tillhandahålls av tjänsteleverantörer) testas regelbundet utifrån företagens riskprofil.*
Observation	Internrevisionen noterar att Bolaget upprättat en kontinuitets-/avbrottsplan som omfattar Bolagets IKT-verksamhet och som innehåller beskrivningar av riskscenarion och åtgärder som ska vidtas vid materialisering av risker. Det noteras dock att Bolaget inte testat kontinuitets-/avbrottsplanen.
Risk	Internrevisionen bedömer att den uteblivna testningen av kontinuitets-/avbrottsplanen kan innebära en ökad risk bristfällig beredskap och kontinuitet i händelse av att negativa riskscenarion materialiseras. Vidare finns risk för att Bolaget inte kan hantera oförutsedda negativa händelser på ett tillfredställande sätt och att oförutsedda negativa händelser får allvarligare konsekvenser än vad som annars hade behövt vara fallet.
Rekommendation	Internrevisionen rekommendera att Bolaget etablerar en process för att på regelbunden basis genomföra tester av Bolagets kontinuitets-/avbrottsplan. Vad gäller testningen skulle Bolaget kunna ta utgångpunkt i de riskscenarion som beskrivs i Bolagets kontinuitets-/avbrottsplan och lägga till ytterligare scenarion i det fall detta bedöms lämpligt. Testningen rekommenderas vidare vara riskbaserad och ge företräde för testning av de riskscenarion som bedöms vara mest sannolika och få allvarligast konsekvenser. Slutligen bör Bolaget i relevanta styrdokument såsom t.ex. i Bolagets kontinuitets-/avbrottsplan eller IKT-riktlinjer ställa krav på genomförandet av testning av kontinuitets-/avbrottsplan på lämplig basis såsom t.ex. årvis. I anslutning till detta bör Bolaget även ange övriga relevanta utgångpunkter för testningen av kontinuitets-/avbrottsplan.
Ledningens åtgärdsplan:	IT-funktionen kommer att se över processer och kontinuitetsplanerna i samverkan med staden och de centrala funktionerna.
Ansvarig och deadline:	IT-ansvarig under 2023.

2022.02.3 Effektiv och ändamålsenlig övervakning, uppföljning och utvärdering av IKT-leverantörer bör etableras	Medium

Utkontraktering av IKT-tjänster och IKT-system

Kriterium	EIOPA-BoS-20/600, Riktlinje 25 – Utkontraktering av IKT-tjänster och IKT-system *81. Företag bör övervaka och försäkra sig om dessa tjänsteleverantörers efterlevnadsnivå med avseende på deras mål och åtgärder för säkerhet samt prestandamålen.* IKT-RIKTLINJER I S:T ERIK FÖRSÄKRINGS AB, 7.2 Beroende gentemot tjänsteleverantörer (1 st.) *”När IKT-tjänster och IKT-system utkontrakteras ska Bolaget se till att relevanta krav för sådana tjänster och system uppfylls, utan att det påverkar tillämpningen av dessa interna IKT-riktlinjer samt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer.”* IKT-RIKTLINJER I S:T ERIK FÖRSÄKRINGS AB, 12 Granskning, bedömning och testning (2 st.) *”System tillhandahållna genom Stockholm Stad testas regelbundet i egen regi. Bolaget avser att regelbundet kontrollera att sådana tester utförs samt efterfråga information om incidenter, skador eller annat som kan påverka Bolagets informationssäkerhetsarbete.”*
Observation	Internrevisionen uppfattar att Bolaget har arbetat för att säkerställa adekvat kravställning i avtal med externa parter som Bolaget är beroende av vad gäller IKT. Vidare har Bolaget informerat om att det pågår ett arbete med att etablera formella rutiner och riktlinjer för att övervaka, följa upp och utvärdera IKT-leverantörers kontroller, rutiner och processer. Internrevisionen noterar dock att det för närvarande inte sker någon formell uppföljning, utvärdering och övervakning av IKT-leverantörer.
Risk	Internrevisionen bedömer att bristen på uppföljning, utvärdering och övervakning av IKT-leverantörer kan innebära att dessa leverantörer inte efterlever den kravställning som finns mot dem vad gäller åtgärder för hantering av IKT-risk, samt att dessa leverantörer i övrigt inte har adekvata kontroller, rutiner och processer för att hantera IKT-risk. Detta kan innebära att Bolagets IKT-risker inte hanteras på ett adekvat sätt.
Rekommendation	Internrevisionen rekommenderar att Bolaget fortsätter arbetet med etablera formella processer för att övervaka, följa upp och utvärderar IKT-leverantörernas kontroller, rutiner och processer för att hantera IKT-risk. Bland områden som Bolaget skulle kunna följa upp, utvärdera och övervaka märks bl.a. IKT-leverantörers styrdokument (avseende informationssäkerhet), Informationssäkerhetsfunktion, åtkomstkontroll, systemövervakning, granskningar, bedömning och testning av informationssäkerhet, utbildning och medvetenhet avseende informationssäkerhet, hantering av IKT-incidenter och IKT-problem, IKT-ändringshantering, hantering av driftskontinuitet, kontinuitetsplanering och hanterings- och återställningsplaner.
Ledningens åtgärdsplan:	IT-funktionen kommer fortsatt att arbeta mot leverantörer för att upprätta adekvata processer för uppföljning och kontroll. Bolaget har idag en mall för kontraktsuppföljning som kommer att utökas.
Ansvarig och deadline:	IT-funktionen under 2023.

Appendix A - Granskningens tillvägagångssätt och metodik

Intervjuer:

Internrevisionen har inom granskningens omfattning utfört intervjuer med:

- Erik Fischer (tf. VD & Bolagsjurist) & Johan Gagner (IT-ansvarig)

Dokumentgranskning:

Internrevisionen har utifrån en riskbaserat arbetssätt granskat ändamålsenlighet och efterlevnad av styrdokument, rutinbeskrivningar och andra relevanta interna dokument. Se Appendix C för specificerad information om erhållna dokument.

Genomgångar och testning:

Inom ramen för granskningen har internrevisionen gått igenom styrdokument, samt kontroller, processer och rutiner för IKT.

Bedömningskriterier:

Alla utfärdade observationer klassificeras i enlighet med följande bedömningsskala **Låg, Medium, Hög, Mycket hög**.

En sammanfattande bedömning av det granskade området görs i enlighet med skalan **Tillfredsställande, Förbättringsbehov, Väsentliga förbättringsbehov** och **Otillfredsställande.**

Se Appendix B för ytterligare beskrivning av gradering av observationer och rapporter.

Appendix B – Gradering av observationer och rapporter

Granskningsrapport

Internrevisionen bedömer intern kontroll och styrning inom det granskade området som "Tillfredställande", "Förbättringsbehov", "Väsentliga förbättringsbehov", eller "Otillfredsställande" utifrån följande:

Otillfredsställande	Iakttagelser med mycket hög eller extrem risknivå
Väsentliga förbättringsbehov	Iakttagelser med hög risknivå
Förbättringsbehov	Iakttagelser med medium risknivå
Tillfredsställande	Iakttagelser med låg risknivå

Varje observation tilldelas en av följande risknivåer; låg, medium, hög eller mycket hög risknivå:

Observationer

Risk nivå	Kriterium
Mycket hög	Implicerar kritisk brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en mycket hög residual risk för att bristen kan leda till kritisk ekonomisk förlust, ineffektivitet och / eller offentlig eller juridisk inverkan. Ledningen bör adressera bristen genom att vidta åtgärder omedelbart och adressera den bakomliggande orsaken till bristen.
Hög	Implicerar väsentlig brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en hög residual risk för att bristen kan leda till väsentlig ekonomisk förlust, ineffektivitet och / eller offentlig eller rättslig inverkan. Ledningen bör adressera bristen genom att vidta åtgärder snarast.
Medium	Implicerar ett utvecklingsområde / betydande brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en medium residual risk som ensam, eller i kombination med andra brister, kan påverka funktionaliteten / integriteten hos system, processer och / eller kontroller, leda till anmärkningar från tillsynsmyndigheter alternativt indikera betydande potential för effektivisering. Ledningen bör adressera bristen genom att vidta åtgärder inom en rimlig tidsram.
Låg	Implicerar ett mindre utvecklingsområde / mindre brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad och som har en låg residual risk av kritisk påverkan på system, processer eller kontroller, men indikerar potentiell förbättring för effektiviteten i processer och / eller kontroller. Ledningen bör adressera bristen inom ramen för den dagliga verksamheten.

Appendix C – Dokument som legat till grund för granskning

- IKT-riktlinje SEF 220523
- IT Avbrottsplan St Erik Försäkring 220523
- IT Avbrottsplan Bilagor 220523
- Riskregister St Erik Försäkring 20221022 (1)
- Aa STYRDOKUMENTLISTA 220523 SEF (1)
- Riktlinje för uppdragsavtal 220523 (1)
- Riktlinje för riskhantering 220523
- genomfrandestatus_min_frvaltningbolag_report
- IT-program 2013-2018 Ett program for digital fornyelse (broschyr) 220523
- GSIT Stockholms Stad
- Riktlinje för incidentrapportering 220523
- Riktlinje för stadens it_ infrastruktur 2013 (broschyr) 220523
- Riktlinje informationssäkerhet 220523
- SIKT 2 Stockholms Stad
- 10 Uppföljning av uppdragsavtal 2022 (002)

Tack

Om du har några frågor om denna rapport eller dess innehåll, vänligen kontakta:

Peter Käll
Director Advisory – IT revision
T: +46 (0) 725 86 82 53
E: Peter.kall@se.gt.com

Grant Thornton