2024.01 – Intern styrning och kontroll med fokus på compliancefunktionen

Från: Internrevisionen, Grant Thornton Sweden AB
Till: Styrelse & VD på S:t Eriks Försäkrings AB

2025-01-14

CONFIDENTIAL/FOR INTERNAL USE ONLY

Inledning och bakgrund

Bakgrund till granskningen

I egenskap av försäkringsföretag verkar S:t Eriks Försäkrings AB (”S:t Erik” eller ”Bolaget”) inom en dynamisk och komplex regulatorisk miljö, där styrning, intern kontroll och riskhantering är grundläggande för verksamheten. Bolaget har att följa en rad regler som gäller för den tillståndspliktiga verksamheten. Det är centralt att Bolaget säkerställer ett gott anseende och förtroende i förhållande till Bolagets intressenter såsom kunder, tillsynsmyndigheter, anställda, samarbetspartners, med flera. För att säkerställa detta är det av vikt att Bolaget har etablerat en god intern styrning och kontroll som bidrar till att företaget styrs på ett sunt och ansvarsfullt sätt vilket svarar upp mot förväntningar från Bolagets intressenter.

Syfte

Granskningen har syftat till att övergripande utvärdera ändamålsenligheten i Bolagets interna styrning och kontroll. Granskningen har särskilt inriktas mot det arbete som utförs av Bolagets funktion för regelefterlevnad då det är av stor vikt att denna funktion utför sitt arbete på ett adekvat sätt för att en god företagsstyrning ska kunna uppnås.

Omfattning

1. Styrande dokument
2. Roller och ansvar
3. Processer och rutiner
4. Utlagd verksamhet

Regulatorisk kontext

1. Kommissionens delegerade förordning (EU) 2015/35
2. Försäkringsrörelselag (2010:2043)
3. Finansinspektionens föreskrifter och allmänna råd om försäkringsrörelse (FFFS 2015:8)
4. Riktlinjer för företagsstyrningssystem (EIOPA-BoS14/253)

Sammanfattning av resultat

Internrevisionen har genomfört en granskning av intern styrning och kontroll med fokus på compliancefunktionen. Internrevisionens bedömning är att Bolagets arbete inom det granskade området är välfungerande i många avseenden. Samtidigt visar granskningen att det finns utrymme för förbättring. Den sammanfattande bedömningen efter granskningen är att det föreligger ett visst förbättringsbehov. För att förbättra intern styrning och kontroll inom området och minska riskerna rekommenderas åtgärder i linje med Interrevisionens rekommendationer.

Internrevisionen lämnar sex (6) rekommendationer baserat på iakttagelser som gjorts. En (1) av dessa bedöms vara av medium risk och fem (5) av låg risk.

#	Fokusområde	Rekommendation	Risknivå
2024.01.1	1. Styrande dokument	Bolaget bör tydliggöra kring strategi och arbetsprogram för regelefterlevnad samt säkerställa att dessa dokument fastställs av funktionen för regelefterlevnad	Låg
2024.01.2	1. Styrande dokument	Bolaget bör överväga att tydliggöra Bolagets processer för utlagd verksamhet i Bolagets riktlinjer för uppdragsavtal	Låg
2024.01.3	1. Styrande dokument	Bolaget bör överväga att uppdatera styrdokumentation för att bättre integrera aspekter som föreskrivs i EIOPAs riktlinjer	Låg
2024.01.4	3. Processer och rutiner	Bolaget bör vidta åtgärder för att förbättra spårbarhet i riskanalysen som utförs av funktionen för regelefterlevnad	Låg
2024.01.5	3. Processer och rutiner	Bolaget bör vidta åtgärder för att förbättra spårbarhet i arbetet som utförs av funktionen för regelefterlevnad	Medium
2024.01.6	4. Utlagd verksamhet	Bolaget bör vidta åtgärder för att förbättra spårbarhet i förhållande till riskanalysen som genomförs vid utläggning av verksamhet	Låg

2024.01.1 Bolaget bör tydliggöra kring strategi och arbetsprogram för regelefterlevnad samt säkerställa att dessa dokument fastställs av funktionen för regelefterlevnad

Låg

1. Styrande dokument

Kriterium	**Artikel 270.1 Kommissionens delegerade förordning (EU) 2015/35** *Ett försäkrings- och återförsäkringsföretags funktion för regelefterlevnad ska fastställa en strategi och ett arbetsprogram för regelefterlevnad. Strategin ska beskriva funktionens ansvarsområden, befogenheter och rapporteringsskyldigheter. Arbetsprogrammet ska beskriva funktionens planerade aktiviteter med beaktande av försäkrings- och återförsäkringsföretags samtliga relevanta verksamhetsområden och deras exponering för risken för bristande regelefterlevnad.*
Observation	Bolaget har etablerat en struktur med styrdokument för Bolagets funktion för regelefterlevnad som bland annat innefattar av styrelsen fastställda riktlinjer för funktionen för regelefterlevnad (”*RIKTLINJER FÖR S:T ERIK FÖRSÄKRINGS FUNKTION FÖR REGELEFTERLEVNAD*”). Vidare arbetar funktionen för regelefterlevnad efter en plan som fastställts av styrelsen vilken grundas på en riskanalys som funktionen har genomfört. Vid granskning har Internrevisionen dock inte kunnat identifiera någon tydlig strategi och arbetsprogram som fastställts av funktionen för regelefterlevnad enligt artikel 270.1 i förordning (EU) 2015/35. I detta avseende har Bolaget uppgett att strategin och arbetsprogrammet framgår av den offentliga upphandlingen, riktlinjer för funktionen för regelefterlevnad samt funktionens riskmatris och årsplan. Internrevisionen uppfattar dock att i vart fall vissa av dessa hänvisade dokument fastställs av andra än Bolagets funktion för regelefterlevnad (se t.ex. Bolagets riktlinjer för funktionen för regelefterlevnad som fastställs av styrelsen och inte funktionen för regelefterlevnad).
Risk	Vad som har påpekats ovan bedöms vara förknippat med en risk för otydlig styrning i förhållande till funktionen för regelefterlevnads strategi och arbetsprogram. Det kan finnas en otydlighet i om funktionen för regelefterlevnad fastställt en strategi och ett arbetsprogram och vad dessa i sådant fall består i.
Rekommendation	Bolaget rekommenderas se över styrningsstrukturen kopplat till funktionen för regelefterlevnad och säkerställa att Bolagets funktion för regelefterlevnad fastställt en strategi och ett arbetsprogram för regelefterlevnad som svarar mot artikel 270.1 i förordning (EU) 2015/35. Om Bolaget avser att inkorporera strategin och arbetsprogrammet i andra dokument, eller ser att andra dokument svarar mot strategin och arbetsprogrammet rekommenderas Bolaget dokumentera det i sina styrande dokument (exempelvis i Bolagets riktlinjer för funktionen för regelefterlevnad). Detta för att skapa en tydlighet i styrningsstrukturen beträffande strategi och arbetsprogram för regelefterlevnad. Bolaget rekommenderas också säkerställa att det är funktionen för regelefterlevnad som har fastställt strategin och arbetsprogrammet (datum för fastställande, vem som fastställt, periodicitet för översyn och fastställande samt andra viktiga aspekter bör dokumenteras).
Ledningens åtgärdsplan:	Vår tolkning är att funktionen för regelefterlevnad omfattar både den som de facto jobbar m frågorna, dvs vår uppdragstagare, samt den beställaransvarige. Genom att beställaransvarig sitter i styrelsen så när styrelsen fattar beslut gör även funktionen det. Riktlinjen kommer att uppdateras med en strategi som beskriver hur riskanalys och årsplan och arbetsprogram hänger ihop.
Ansvarig och deadline:	Regelefterlevnadsansvarig, maj 2025 (då riktlinjerna tas).

2024.01.2 Bolaget bör överväga att tydliggöra Bolagets processer för utlagd verksamhet i Bolagets riktlinjer för uppdragsavtal

Låg

1. Styrande dokument

Kriterium	**EIOPA-BoS14/253** *1.116.Företag som ingått eller överväger att ingå uppdragsavtal bör i sitt styrdokument ange företagets ansatser och processer för uppdragsavtal, från början till dess att avtalet löper ut. Detta omfattar särskilt* *a) processen för att bestämma om en funktion eller aktivitet är kritisk eller viktig;* *b) hur en lämplig tjänsteleverantör väljs ut och hur och hur ofta dess utförande och resultat bedöms;* *c) information som ska ingå i det skriftliga avtalet med tjänsteleverantören, med beaktande av kraven i kommissionens delegerade förordning 2015/35;* *d) beredskapsplaner, inbegripet tillvägagångssätt för att avsluta uppdragsavtal som omfattar kritiska eller viktiga funktioner eller aktiviteter.*
Observation	Bolaget har upprättat riktlinjer för uppdragsavtal (”RIKTLINJER FÖR UPPDRAGSAVTAL I S:T ERIK FÖRSÄKRING AB”) vilka lyfter en rad viktiga aspekter i förhållande till utlagd verksamhet. Internrevisionen har dock inte kunnat identifiera någon tydlig information som avser tillvägagångssätt för att avsluta uppdragsavtal som omfattar kritiska eller viktiga funktioner eller aktiviteter i Bolagets riktlinjer för uppdragsavtal.
Risk	Vad som har påpekats ovan bedöms vara förknippat med en risk för att processer och rutiner inte är tillräckligt tydligt dokumenterade och förklarade i Bolagets styrdokumentation, vilket kan vara förknippat med en ökad operativ risk.
Rekommendation	Bolaget rekommenderas se över sina riktlinjer för uppdragsavtal och överväga om tillvägagångssätt för att avsluta uppdragsavtal som omfattar kritiska eller viktiga funktioner eller aktiviteter tydligare kan beskrivas.
Ledningens åtgärdsplan:	Vad avser avslutande av uppdrag kommer riktlinjen att kompletteras med mer detaljerade beskrivningar av hur detta de facto sker.
Ansvarig och deadline:	Regelefterlevnadsfunktionen, maj 2025 (då riktlinjerna antas).

2024.01.3 Bolaget bör överväga att uppdatera styrdokumentation för att bättre integrera aspekter som föreskrivs i EIOPAs riktlinjer

Låg

1. Styrande dokument

Kriterium	**EIOPA-BoS14/253** *1.34. Företaget bör anpassa alla styrdokument som är en del av företagsstyrningssystemet till varandra samt till dess affärsstrategi. Alla styrdokument bör åtminstone ange* *a) vilka mål som eftersträvas;* *b) vilka uppgifter som ska utföras och vilken person eller funktion som ansvarar för dem;* *c) vilka processer och rapporteringsrutiner som ska tillämpas;* *d) att det ska finnas en skyldighet för berörda organisationsenheter inom företaget att informera riskhanterings-, internrevisions-, regelefterlevnads- och aktuariefunktionerna om eventuella omständigheter som är relevanta för deras respektive uppgifter.*
Observation	Inom ramen för den aktuella granskningen har Internrevisionen tagit del av, och gått igenom, ett antal av Bolagets styrdokument. I detta avseende kan konstateras att dokumenten i många fall svarar upp mot kriterier i EIOPA-BoS14/253 eftersom de exempelvis generellt anger ett syfte / mål, uppgifter som ska utföras, ansvar och roller, m.m.. Det noteras dock att vissa styrdokument inte tydligt i alla avseende följer vad som föreskrivs i 1.34. EIOPA-BoS14/253. Exempelvis anger följande styrdokument inte något om skyldigheten för berörda organisationsenheter inom företaget att informera riskhanterings-, internrevisions-, regelefterlevnads- och aktuariefunktionerna om eventuella omständigheter som är relevanta för deras respektive uppgifter: • Riktlinjer för uppdragsavtal (”*RIKTLINJER FÖR UPPDRAGSAVTAL I S:T ERIK FÖRSÄKRING AB*”). • Riktlinjer för funktionen för regelefterlevnad (”*RIKTLINJER FÖR S:T ERIK FÖRSÄKRINGS FUNKTION FÖR REGELEFTERLEVNAD*”). • Riktlinjer för lämplighetsprövning (”*RIKTLINJER FÖR LÄMPLIGHETSPRÖVNING AV STYRELSE, LEDNING OCH NYCKELFUNKTIONER I S:T ERIK FÖRSÄKRINGS AB*”).
Risk	Vad som har påpekats ovan bedöms kunna vara förknippat med en risk för att Bolagets styrdokument inte i alla avseende svarar mot EIOPAs riktlinjer och därmed best practice vad gäller styrdokumentationens innehåll och struktur. Avsaknad av information om skyldigheten att informerar centrala funktioner om eventuella omständigheter som är relevanta för deras respektive uppgifter kan öka risken för att relevant information inte kommer de centrala funktionerna tillhanda.
Rekommendation	Bolaget rekommenderas överväga att se över styrdokumentationen och uppdatera denna så att den bättre följer vad 1.34. EIOPA-BoS14/253 föreskriver.
Ledningens åtgärdsplan:	Nämnda styrdokument kommer att justeras om hänvisning till centrala funktioner saknas.
Ansvarig och deadline:	Bolagsjurist. Q2 2025 (då bolagets riktlinjer normalt fastställs årsligen)

2024.01.4 Bolaget bör vidta åtgärder för att förbättra spårbarhet i riskanalysen som utförs av funktionen för regelefterlevnad

Låg

3. Processer och rutiner

Kriterium	**Artikel 266 Kommissionens delegerade förordning (EU) 2015/35** *Internkontrollsystemet ska säkerställa att försäkrings- och återförsäkringsföretaget efterlever tillämpliga lagar och andra författningar, att företagets verksamhet är ändamålsenlig och effektiv med hänsyn till dess mål och att ekonomisk och icke-ekonomisk information är tillgänglig och tillförlitlig.* **10 kap. 16 § FRL.** *Funktionen för regelefterlevnad ska* *1. rapportera till styrelsen och den verkställande direktören i fråga om efterlevnaden av* *a) bestämmelserna i denna lag och föreskrifter som har meddelats med stöd av lagen,* *b) bestämmelser som har meddelats av Europeiska kommissionen med anledning av Solvens II-direktivet, och* *c) de riktlinjer och rekommendationer som har meddelats med anledning av det direktivet av Europeiska försäkrings- och tjänstepensionsmyndigheten, Finansinspektionen och, om företaget har inrättat en sekundäretablering i ett land inom EES, den behöriga myndigheten i det landet,* *2. lämna råd till företagets styrelse och den verkställande direktören om förebyggande av bristande efterlevnad av bestämmelser enligt 1,* *3. bedöma konsekvenserna av förändringar i bestämmelser, riktlinjer och rekommendationer enligt 1, och* *4. identifiera och bedöma risker för bristande efterlevnad av bestämmelser, riktlinjer och rekommendationer enligt 1.*
Observation	Bolagets funktion för regelefterlevnad har genomfört en riskanalys för 2024 där funktionen listat områden med risk för regelavvikelser. Analysen har utgjort underlag när det kommer till att avgöra vilka områden funktionen ska prioritera i sitt arbete. Varje område i riskanalysen har bedömts utifrån sannolikhet och konsekvens. Det noteras dock att det inte finns några dokumenterade skäl eller motiveringar i anslutning till varje område som anger varför ett visst område fått en viss konsekvens eller sannolikhet. Vidare är riskanalysen daterad (framgår när denna senast uppdaterats), men det finns ingen information om vem/vilka som upprättat riskanalysen.
Risk	Vad som påepkats ovan bedöms kunna innebära en mindre risk för brister i spårbarhet avseende det arbete som utförs av Bolagets funktion för regelefterlevnad. Detta kan göra det svårare att följa upp och utvärdera funktionens arbete.
Rekommendation	Bolaget rekommenderas överväga att vidta åtgärder för att förbättra dokumentation och spårbarhet i riskanalysen som utförs av Bolagets funktion för regelefterlevnad. I detta avseende rekommenderas att skäl och motivering till att olika områden riskbedömts på ett visst sätt bättre dokumenteras (t.ex. genom att lägga till en till kolumn i riskbedömningen där detta kan dokumenteras). Vidare rekommenderas att det tydligare dokumenteras i riskanalysdokumentet vem det är som upprättat dokumentet. Om dokumentet upprättats av flera personer eller upprättats av en person och kvalitetskontrollerats av en annan kan detta med fördel också dokumenteras i själva dokumentet. Detta för att säkerställa spårbarhet i det arbete som utförs.
Ledningens åtgärdsplan:	Rek översänds till regelefterlevnadsfunktionen för kompletteringar i riskanalysen.
Ansvarig och deadline:	Johan Grenefalk. Q2 2025.

2024.01.5 Bolaget bör vidta åtgärder för att förbättra spårbarhet i arbetet som utförs av funktionen för regelefterlevnad

Medium

3. Processer och rutiner

Kriterium	**Artikel 266 Kommissionens delegerade förordning (EU) 2015/35** *Internkontrollsystemet ska säkerställa att försäkrings- och återförsäkringsföretaget efterlever tillämpliga lagar och andra författningar, att företagets verksamhet är ändamålsenlig och effektiv med hänsyn till dess mål och att ekonomisk och icke-ekonomisk information är tillgänglig och tillförlitlig.* **10 kap. 16 § FRL.** *Funktionen för regelefterlevnad ska* *1. rapportera till styrelsen och den verkställande direktören i fråga om efterlevnaden av* *a) bestämmelserna i denna lag och föreskrifter som har meddelats med stöd av lagen,* *b) bestämmelser som har meddelats av Europeiska kommissionen med anledning av Solvens II-direktivet, och* *c) de riktlinjer och rekommendationer som har meddelats med anledning av det direktivet av Europeiska försäkrings- och tjänstepensionsmyndigheten, Finansinspektionen och, om företaget har inrättat en sekundäretablering i ett land inom EES, den behöriga myndigheten i det landet,* *2. lämna råd till företagets styrelse och den verkställande direktören om förebyggande av bristande efterlevnad av bestämmelser enligt 1,* *3. bedöma konsekvenserna av förändringar i bestämmelser, riktlinjer och rekommendationer enligt 1, och* *4. identifiera och bedöma risker för bristande efterlevnad av bestämmelser, riktlinjer och rekommendationer enligt 1.*
Observation	Inom ramen för den genomförda granskningen har Internrevisionen närmare undersökt regelefterlevnadsfunktionens arbete och hur funktionens arbete dokumenteras. En del i detta har bestått i ett stickprov på kontrollen avseende outsourcing som funktionen avrapporterade i sin Q2-rapport för 2024. Inom ramen för stickprovet begärde Internrevisionen in underlag såsom arbetsdokument som dokumenterar funktionens arbete. Vid kontroll av detta underlag noterades att dokumentationen i arbetsdokument var sparsam och att information såsom vilka specifika regelverkskrav som kontrollerats, när kontroll skett och av vem samt vilka exakt dokument som kontrollerats saknades i arbetsdokumentet.
Risk	Vad som har påpekats ovan bedöms kunna vara förknippat med en svaghet när det kommer till spårbarheten i arbetet som utförs av Bolagets funktion för regelefterlevnad. Detta kan försvåra när det gäller att följa upp och utvärdera funktionens arbete, både för Internrevisionen och för tillsynsmyndigheter såsom FI.
Rekommendation	Bolaget rekommenderas vidta åtgärder för att säkerställa att det arbete som utförs av Bolagets regelefterlevnadsfunktion dokumenteras på ett sätt som säkerställer god spårbarhet i funktionens arbete. I detta avseende menar Internrevisionen att följande information med fördel kan inkluderas i arbetsdokument som funktionen upprättar: • Vilka specifika externa regler och riktlinjer (exempelvis lagar, förordningar, föreskrifter, riktlinjer, etc.) som kontrollen baserats på, gärna på en nivå där det blir tydligt vilka exakta delar av externa regler som varit utgångspunkt (t.ex. kapitel och paragrafer i svensk lag och föreskrifter från FI, artiklar i EU-förordningar, etc.). • Vilka specifika dokument som granskats och slutsatser baserats på. • Någon typ av information kring vem som utfört arbetet och när. I tillägg till ovan kan även intervjuanteckningar med information om närvarande, när intervjun skedde etc. upprättas vid kontroller som inkluderar intervju som ett arbetsmoment. Slutsatser i arbetsdokument som baseras på vad som framkommit vid intervju kan med fördel hänvisa till mötesanteckningar från intervjuer.
Ledningens åtgärdsplan:	Funktionen för regelefterlevnad kommer tillsammans med Bolaget se över detta och implementera en tydligare spårbarhet i såväl arbetsdokument som i avrapportering i enlighet med er rekommendation ovan.
Ansvarig och deadline:	Johan Grenefalk. Q1 2025.

2024.01.6 Bolaget bör vidta åtgärder för att förbättra spårbarhet i förhållande till riskanalysen som genomförs vid utläggning av verksamhet

Låg

4. Utlagd verksamhet

Kriterium	**Artikel 274.3 Kommissionens delegerade förordning (EU) 2015/35** *Vid val av tjänsteleverantör enligt punkt 1 i fråga om kritiska eller viktiga operativa funktioner eller verksamheter ska förvaltnings-, lednings- eller tillsynsorganet säkerställa följande:* *(a) Att en detaljerad granskning görs för att kontrollera att den potentiella tjänsteleverantören har de kunskaper, den kapacitet och de rättsliga tillstånd som krävs för att utföra begärda funktioner eller verksamheter på ett tillfredsställande sätt och med hänsyn till företagets mål och behov.* *(b) Att tjänsteleverantören har vidtagit alla åtgärder för att säkerställa att det inte finns någon uttalad eller potentiell intressekonflikt som äventyrar uppfyllandet av det uppdragsgivande företagets behov.* *(c) Att ett skriftligt avtal ingås mellan försäkrings- och återförsäkringsföretaget och tjänsteleverantören, där företagets och tjänsteleverantörens respektive rättigheter och skyldigheter tydligt fastställs.* *(d) Att de allmänna villkoren i uppdragsavtalet klart anges för företagets förvaltnings-, lednings- eller tillsynsorgan och godkänns av detta organ.* *(e) Att uppdragsavtalet inte innebär någon överträdelse av lagstiftning, i synnerhet när det gäller uppgiftsskydd.* *(f) Att tjänsteleverantören omfattas av samma regler om säker och konfidentiell information avseende försäkrings- och återförsäkringsföretaget eller dess försäkringstagare eller förmånstagare som gäller för försäkrings- och återförsäkringsföretaget.* **Artikel 274.5 Kommissionens delegerade förordning (EU) 2015/35** *Ett försäkrings- och återförsäkringsföretag som ingår uppdragsavtal beträffande kritiska eller viktiga operativa funktioner eller verksamheter ska uppfylla följande krav:* *(a) Säkerställa att relevanta inslag i tjänsteleverantörens riskhanterings och internkontrollsystem har den ändamålsenlighet som krävs för efterlevnad av artikel 49.2 a och b i direktiv 2009/138/EG.* *(b) På ett ändamålsenligt sätt beakta de verksamheter som omfattas av uppdragsavtal i sitt eget riskhanterings- och internkontrollsystem, med tanke på efterlevnad av artikel 49.2 a och b i direktiv 2009/138/EG.* *(c) Kontrollera att tjänsteleverantören har de ekonomiska resurser som krävs för att korrekt och tillförlitligt utföra de tillkommande uppgifterna samt att alla de anställda hos tjänsteleverantören som kommer att medverka i utförandet av de funktioner eller verksamheter som omfattas av uppdragsavtal har de kvalifikationer och den lämplighet som krävs.* *(d) Säkerställa att tjänsteleverantören har ändamålsenliga beredskapsplaner för hantering av krissituationer eller störningar i verksamheten och där det finns behov regelbundet testar systemen för säkerhetskopiering, med hänsyn till de funktioner och verksamheter som omfattas av uppdragsavtal.*
Observation	Bolaget har etablerat en process där Bolaget arbetar med en riskanalys när verksamhet läggs ut genom uppdragsavtal. Internrevisionen uppfattar vidare att riskanalysen lyfter relevanta frågor. Det noteras dock att riskanalysdokumentet inte innehåller någon datering som visar när dokumentet upprättats. Vidare finns inte någon information om vem/vilka som upprättat riskanalysen i själva dokumentet.
Risk	Vad som har påpekats ovan bedöms vara förknippat med en risk för bristande spårbarhet som kan försvåra när det gäller att följa upp och utvärdera Bolagets arbete samt säkerställa att arbetet utförts av rätt person i rätt tid.
Rekommendation	Bolaget rekommenderas vidta åtgärder för att säkerställa att datering och vem som upprättat dokumentet framgår av riskanalysdokumentet (kan med fördel även framgå av andra viktiga dokument vid utläggning av verksamhet). Sådana åtgärder kan exempelvis bestå i att uppdatera mallen för riskanalysen så att denna inkludera fält som ska fyllas i avseende datering och vem som upprättat dokumentet.
Ledningens åtgärdsplan:	Justering kommer att ske.
Ansvarig och deadline:	Bolagsjurist. Q2 2025.

Appendix A - Granskningens tillvägagångssätt och metodik

Intervjuer

Internrevisionen har inom ramen för granskningen genomfört intervju med Johan Grenefalk (ansvarig compliance) samt ställt frågor till Erik Fischer (bolagsjurist).

Dokumentgranskning

Internrevisionen har med ett riskbaserat selektivt tillvägagångsätt granskat ändamålsenlighet och efterlevnad av styrdokument, rutinbeskrivningar och andra relevanta interna dokument. Se 'Appendix C – Mottagna dokument' för information om erhållna dokument.

Avgränsningar

Granskningen har genomförts med ett riskbaserat tillvägagångssätt, vilket innebär att ingen uttömmande granskning har gjorts av alla aspekter som rör de områden som omfattas. De resultat som presenteras är vägledande och en fördjupad granskning kan vara nödvändig för att närmare kunna bedöma risker och konsekvenser.

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

Väsentliga förbättringsbehov

Förbättringsbehov

Tillfredsställande

Observationer

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

Risknivå	Kriterium
Mycket hög	Implicerar kritisk brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en mycket hög residual risk, eftersom 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, eftersom bristen kan leda till väsentlig ekonomisk förlust, ineffektivitet och / eller offentlig eller rättslig inverkan. Ledningen bör adressera bristen genom att snarast vidta åtgärder.
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 – Mottagna dokument

- 1.3 Register outsourcing 240905
- 1.4 Riktlinje för funktionen för regelevterlevnad (compliance) 240524
- 1.5 Styrdokumentlista 240524
- 1.7 WSA 2021-
- 1.8 Uppföljning av uppdragsavtal 2023
- 1.9 Organisationsschema
- 1.10 Årsrapport 2023 Regelefterlevnad
- 1.10 Q1 2024 S_t Erik Försäkrings AB
- 1.10 Q2 2024 S_t Erik Försäkrings AB
- 1.11 Årsplan 2024
- 1.12 Riskmatris 2024
- 1.13 Styrelseprotokoll 1 2024
- 1.13 Styrelseprotokoll 2 2024 per capsulam
- 1.13 Styrelseprotokoll 3 2024
- 1.14 Riktlinje för lämplighetsprövning 240524
- 1.15 Bukettprövning SEF 2023 231003
- 1.15 Komplettering Carina regelefterlevnad
- 1.16 Slutbrev(3808288) (1)_TMP
- 1.17 Riskanalys Regelefterlevnadsfunktionen 2022
- Riktlinje för uppdragsavtal 240524
- Riktlinje för intern styrning och kontroll 240524
- Rapport vandelsprövning S_t Erik Försäkrings AB 230309
- Anmälan outsourcing 150326
- Anmälan om uppdragsavtal och molntjänster WSA-AKTIV.FID309978

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

Christer Runestam
Director Advisory – Head of Internal Audit
T +46 (0) 70 619 33 87
E christer.runestam@se.gt.com

Grant Thornton