Internrevisionsrapport

2021.01 - Granskning av intern styrning och kontroll med fokus på aktuarie- och riskkontrollsfunktionen

S:t Erik Försäkrings AB

2022-02-21

Till: Styrelsen vid S:t Eriks Försäkrings AB

Från: Internrevisionen, Grant Thornton Sweden AB

Uppdragets omfattning och metodik

Inledning

För att ett försäkringsföretag ska kunna uppfylla sina åtaganden till kunderna behöver det ha tillräckligt med kapital för att hantera sina risker, ha en god intern styrning och en god kontroll över sina risker. En god intern kontroll ger förutsättningar för en ändamålsenlig och effektiv verksamhet där de väsentliga riskerna hanteras och lagar och regler efterlevs, vilket hjälper företaget att nå sina mål.

Internrevisionens uppdrag är att utvärdera systemet för internkontroll innefattande kontinuerligt utvärdera de centrala funktionerna. Under 2020 genomfördes en övergripande granskning av intern styrning och kontroll. Årets bevakning av internkontrollsystemet har syftat till att på en övergripande nivå utvärdera riskkontroll- och aktuariefunktionen uppdrag och leverans.

S:t Erik Försäkrings AB:s aktuariella tjänster, riskhanterings- och regelefterlevnadsfunktionen bedrivs på uppdragsavtal idag. Internrevision har utvärderat om strukturer och rutiner är ändamålsenliga samt om det finns förutsättningar för att dessa utförs på ett effektivt sätt av företagets kontrollfunktioner för riskkontroll och aktuariefunktioner.

Revisionsmål och omfattning

Granskningen syftar till att utvärdera tillförlitligheten och kvaliteten på det arbete som utförs inom företagets kontrollfunktioner för riskhantering och aktuarie med fokus på ändamålsenlighet av strukturer och rutiner. Årets granskning fokuserar på förändringar av centrala funktioner och omfattningen centreras till riskhanterings- och aktuariefunktionen.

Omfattning

1. Intern styrning och kontroll (styrande dokument, interna regler)
 1.1 Riskhantering
 1.2 Processer, strukturer och rutiner
 1.3 Outsourcing

2. Centrala funktioner (Aktuarie- och riskhanteringsfunktionen)
2.1 Riktlinjer
2.2 Processer och rutiner
2.3 Uppföljning och kontroll
2.4 Rapportering

Metod

Internrevisionen har inom granskningens omfattning utfört intervjuer och genomgångar med:

- Riskhanteringsfunktion Jonathan Björkman (FCG) - 2021-09-10
- Aktuariefunktion Ola Hestnes (Nordic Actuary AB) - 2021-09-10

Materialgranskning:
Internrevisionen har granskat ändamålsenlighet och efterlevnad av styrdokument, rutinbeskrivningar och andra relevanta interna dokument. Se ’Appendix B – Underlag som legat till grund för granskning’ för specificerad information om erhållna dokument.

Sammanfattning av granskningen

Om system och rutiner för den interna kontrollen är otillräckliga finns risk för att organisationens mål inte uppnås. Detta kan exponera S:t Erik Försäkrings AB för risker hänförliga till regulatoriska krav vilket kan leda till regulatoriska anmärkningar och sanktioner, ekonomiska förluster samt ryktes- och förtroenderisk.
Den sammanfattande bedömningen efter granskningen av Bolagets styrning och intern kontroll med fokus på risk- och aktuariefunktionen är Tillfredställande
Med hänsyn till Bolagets storlek, riskaptit, verksamhetens komplexitet och riskexponering bedöms bolagets hantering inom flera områden vara ändamålsenlig då Bolaget bland annat uppvisat följande:

- Styrdokument och interna regler
  + Bolaget har riktlinjer och instruktioner för riskhanterings- och regelefterlevnadsfunktionen, med innehållande uppgifts- och ansvarsbeskrivningar samt funktionernas ställning, rättigheter och befogenheter.
- Utförande av ansvarsområden och rapportering
  + Det finns en tydlig spårbarhet i utförda kontroller avseende rapportering och uppföljning utifrån kravställningen för de centrala nyckelfunktionerna som på ett överskådligt sätt presenteras till styrelsen
- Lämplighet och anseende
  + Riskhantering- och aktuariefunktionen innehar tillfredställande lämplighet och anseende.

Internrevision lämnar två rekommendationer baserat på iakttagelser som gjorts på områden den interna kontrollen kan stärkas eller utvecklas.
Åtgärder har inhämtats och kommer följas upp av internrevisionen genom rutin för uppföljning av lämnade rekommendationer.

#	Omfattning (område)	Rekommendationer	Risknivå
2021.01.1	1. Intern styrning och kontroll 1.3 Outsourcing	Avsaknad av dokumenterad riskanalys vid förnyad outsourcing	Låg
2021.01.2	2. Centrala funktioner 2.2 Processer och rutiner	Aktuariefunktionens arbete kan med fördel formaliseras i ett årshjul/aktivitetsplan	Låg

Internrevisionen har även följt upp status på lämnade rekommendationer 2020 då internrevisionen genomförde två granskningsinsatser och lämnade två rekommendationer, båda med risknivå Låg.

#	Rapport	Rekommendationer	Risknivå	Verksamhetens åtgärdsplan
2020.01.1	Granskning och utvärdering av intern styrning och kontroll	Säkerställ korrekt hänvisning i Bolagets "Riktlinjer för riskhantering S:T Eriks Försäkrings AB" till "Policy för ORSA inom S:T Erik Försäkrings AB" för att förtydliga att Bolagets har en formaliserad process för framtagning av regelbundna stresstester	Låg	Riktlinjer för riskhantering kommer uppdateras med en hänvisning. Ansvarig och deadline: Bolagsjurist Erik Fischer, Styrelsemötet 210305
2020.02.1	Granskning och utvärdering av funktionerna för riskhantering och regelefterlevnad	Säkerställ att Bolagets riskhanteringsfunktionen får de praktiska deltagandet av aktuariefunktionen som krävs för att på ett formaliserat sätt sammanställa en tillfredställande ORSA-rapport	Låg	Avstämning med funktionerna. Ansvarig och deadline: Bolagsjurist Erik Fischer, februari 2021

2021.01.1 Avsaknad av dokumenterad riskanalys vid förnyad outsourcing	Låg

Kriterium/ Kontrollmål

EIOPA-BoS-14/253

Riktlinje 60 – Kritiska eller viktiga operativa funktioner och aktiviteter

1.113.Företaget bör fastställa och dokumentera om en funktion eller aktivitet som omfattas av ett uppdragsavtal är en kritisk eller viktig funktion eller aktivitet baserat på om funktionen eller aktiviteten är nödvändig för företagets verksamhet, eftersom det utan funktionen eller aktiviteten inte skulle kunna tillhandahålla tjänster åt sina försäkringstagare.

Riktlinje 63 – Styrdokument för uppdragsavtal

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.

Riktlinjer för uppdragsavtal i S:t Erik försäkring AB

Riskanalys skall genomföras av bolaget och, avseende kritiska eller viktiga funktioner, vara ett underlag för styrelsens beslut om outsourcing. Vid förnyad outsourcing ska ny riskanalys genomföras om riskerna har ändrats. VD ansvarar för: att styrelsen tillställs en riskanalys inför beslut om outsourcing avseende kritiska eller viktiga funktioner.

Instruktion för funktionen för riskhantering

Riskhanteringsfunktionen ska löpande kontrollera att riskanalyser utförts tillfredsställande inför outsourcing respektive affärsbeslut. Verksamheten ansvarar för att genomföra och tillhandahålla riskanalys för uppdragsavtal respektive affärsbeslut.

Observation

S:t Eriks försäkring har identifierat nio funktioner/aktiviteter som kritiska och sju av dessa verksamheter bedrivs på uppdragsavtal. Bolaget har tillsatt nya outsourcingparters för aktuariefunktion och riskfunktion vilka båda bedöms som kritiska funktioner. Nordic Actuary AB ansvarar sedan 2020-09-01 för utförande av aktuariefunktionen i S:t Erik Försäkring AB och FCG tillträdde som ny riskfunktion i januari 2021. Internrevisionen har efterfrågat riskanalyser för dessa outsourcingarrangemang som hänvisas i bolagets egen riktlinje för uppdragsavtal och fått som svar att ingen förnyad riskanalys har utförts utan de risker som är hänförliga till outsourcing av funktionerna hanteras genom upphandlingsunderlag inom ramen för LOU. Således motsvarar praktiken inte de fastställda riktlinjer.

Risk

Avsaknad av överskådliga riskanalyser leder till att risker hänförliga till outsourcingarrangemang inte identifieras och hanteras samt försvårar styrelsens översyn och riskfunktionens kontroll.

Rekommendation

Internrevisionen rekommenderar att bolaget dokumenterar riskanalyser för samtliga kritiska funktioner. Internrevisionen rekommenderar även att bolaget vid förnyad outsourcing dokumenterar innehållande grund för klassificering för att definiera kritisk eller viktig outsourcing samt dokumentera riskanalyser i enlighet med bolagets egna riktlinjer, alternativt ändrar i riktlinjen.

Om bolaget inte anser att en förnyad riskanalys anses nödvändig bör detta ställningstagande dokumenteras.

2021.01.2 Aktuariefunktionens arbete kan med fördel formaliseras i ett årshjul/aktivitetsplan	Låg

Kriterium/ Kontrollmål	*EIOPA-BoS-14/253* *1.12 När det gäller aktuariefunktionen fokuserar dessa riktlinjer snarare på vad aktuariefunktionen gör, inte hur. Eftersom syftet med aktuariefunktionen är att tillhandahålla ett mått på kvalitetssäkringen genom expertråd om aktuariella tekniker är det särskilt viktigt att ta fram specifik teknisk vägledning om aktuariefunktionens uppgifter, ansvar samt andra aspekter.* *Instruktion för aktuariefunktion: Aktuarien ska minst årligen lämna en skriftlig rapport till styrelsen med dokumentation av det arbete som utförts, resultat, identifiering av brister samt rekommendationer om åtgärder.*
Observation	Bolagets instruktion för aktuariefunktionen ”Instruktion för Aktuariefunktionen i S:t Erik Försäkrings AB” anger att på ett tydligt sätt aktuariens uppgifter och rapporteringsskyldigheter. Här ingår bland annat att genomföra särskilda försäkringstekniska utredningar och beräkningar, lämna information till riskhanteringsfunktionen om försäkringsrisker samt att delta i och vara behjälplig med aktuariekompetens i samband med årsbokslut. Det har under granskning konstaterats att instruktionens beskrivning över aktuariens kontroller är föremål för förtydligande då denna anger att aktuarien skall genomföra de kontroller som framgår av gällande regelverk och att aktuarien och verksamheten ska planlägga arbetet i samråd. Detta i kombination med att aktiviteter som aktuariefunktionen avser genomföra under kommande år inte finns dokumenterade i en årlig plan leder till att delar av aktuariefuktionens arbete under året hanteras ad-hoc. För att möjliggöra för en effektiv kontraktsuppföljning från ledningen krävs att arbetet är formaliserat och går att följa på ett överskådligt sätt (COSO monitoring).
Risk	Bristande formalisering av den centrala funktionens arbete riskerar att leda till att kontroller inte utförs eller utförs bristfälligt samt att personberoende uppstår. När det saknas en dokumenterad årlig plan så kan det medföra sämre förutsättningar för vd och styrelse att på ett överblickbart sätt få information om vilka aktiviteter som planeras ske under året, eller få information om aktiviteter som eventuellt behöver omprioriteras.
Rekommendation	Internrevisionen rekommenderar att aktuariefunktionen tar fram en plan för att fastställa kommande års arbete där det framgår vilka aktiviteter som kommer ske under året, vilka aktiviteter som ska presenteras för vilken mottagare och att vd och styrelse informeras om planen.

Appendix A – Gradering av observationer och rapporter

Revisionsrapport

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
Tillfredställande	Iakttagelser med låg risknivå

Iakttagelser

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

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 B – Underlag som legat till grund för granskning

- 6 AFR - St Erik – 2020
- Nordic Actuary
- 2. 2020 Q4 Sammanfattande riskrapport SEF
- 3. Riskhanteringsfunktionens årsrapport SEF 20210305
- 4. 2021 Q1 Sammanfattande riskrapport SEF
- 10. Aktivitetsplan 2021 riskhanteringsfunktionen St Erik Försäkring
- Riskanalys outsourcing av riskhanteringsfunktionen
- Riskregister St Erik Försäkring 20211108
- Instruktion för aktuariefunktionen 210521
- Instruktion för funktionen för riskhantering 210521
- Instruktion för hantering av reservsättningsrisker 210521
- Instruktion för tecknings och återförsäkringsrisker 210521
- Riktlinje för intern styrning och kontroll 210521
- Riktlinje för riskhantering 210305
- Riktlinje för uppdragsavtal 210521
- STYRDOKUMENTLISTA 210521 SEF
- Styrelseprotokoll 1 2021
- Styrelseprotokoll 2 2021 per capsulam
- Styrelseprotokoll 3 2021

Grant Thornton

An instinct for growth™

Hilkka Nyberg
Director Internal Audit

T +46 8 563 072 67
M +46 76 127 58 33
E hilkka.nyberg@se.gt.com