Till
Styrelsen i S:t Erik Försäkrings AB

Årsplan för funktionen för regelefterlevnad år 2022

S:t Erik Försäkrings AB, nedan Bolaget, har uppdragit åt Wesslau Söderqvist Advokatbyrå i Stockholm KB att upprätthålla funktionen för regelefterlevnad enligt 10 kap. 4 och 16 §§ försäkringsrörelselagen (2010:2043).

Inom ramen för uppdraget planerar funktionen för regelefterlevnad att under år 2022 vidta de åtgärder som beskrivs nedan. Planerade åtgärder kan komma att ändras till följd av ändringar i den verksamhet som Bolaget bedriver, ändringar i för Bolaget relevanta regelverk eller andra omständigheter som bedöms vara av väsentlig betydelse för Bolagets verksamhet. Årsplanen har fastställts av Bolagets styrelse den […] 2021.

För uppdraget ansvarar advokat Johan Grenefalk.

1 Riskanalys

Årsplanen har utarbetats utifrån en analys av de risker som Bolagets verksamhet är förknippad med. Följande förhållanden har särskilt beaktats av funktionen för regelefterlevnad:

- Förändringar i regelverk tillämpliga på Bolagets tillståndspliktiga verksamhet,
- affärsområden, rutiner och processer där regelefterlevnaden, vid tillsyn från Finansinspektionen eller annan myndighet, visat sig vara bristfällig hos Bolaget eller andra bolag med liknande verksamhet som Bolaget,
- affärsområden, rutiner och processer hos Bolaget där de ekonomiska konsekvenserna för Bolaget vid bristande regelefterlevnad kan antas vara särskilt stora, t.ex. på grund av att Bolaget kan ha ekonomiska incitament att avvika från gällande regelverk eller på grund av att regelavvikelser

riskerar att leda till betydande straffavgifter eller skadeståndsskyldighet gentemot kunder och/eller motparter,

- affärsområden, produkter, rutiner och processer hos Bolaget som är nya eller nyligen har varit föremål för förändringar eller omorganisationer, samt

- affärsområden, produkter, rutiner och processer hos Bolaget som tidigare varit föremål för anmärkningar från funktionen för regelefterlevnad eller som inte varit föremål för kontroll på länge.

De överväganden som gjorts i riskbedömningen inför år 2022 rör särskilt eventuella förändringar med anledning av Eiopas riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik, nedan IKT-riktlinjer. Funktionen för regelefterlevnad avser att under det första kvartalet utföra kontroll för att säkerställa att Bolaget har en ändamålsenligt IKT-strateg och rutiner för att analysera IKT- och säkerhetsrisker. Vidare avser funktionen för regelefterlevnad att följa upp Bolagets interna rutiner och riktlinjer för outsourcing samt hantering av molntjänster som dels uppföljning på föregående års fokusområde, dels då det går hand i hand med granskningen av informations- och kommunikationsteknik.

Riskanalysen har dokumenterats särskilt, se bilaga 1.

Årsplanen nedan har utformats för att, med hänsyn till arten och omfattningen av Bolagets verksamhet samt dess komplexitet, hantera de riskmoment som identifierats av funktionen för regelefterlevnad.

2 Informationsgivning m.m.

2.1 Löpande informationsgivning

Funktionen för regelefterlevnad ska löpande bevaka dels förändringar i lagar, förordningar, föreskrifter och allmänna råd samt andra nationella och internationella regelverk och rekommendationer som gäller för Bolagets tillståndspliktiga verksamhet, dels utveckling inom branschen såsom handelsbruk, praxis och sedvänja. Bolagets verkställande direktör, styrelse och anställda ska löpande underrättas om för verksamheten relevant information. Informationsgivning ska ske på det sätt som är mest effektivt i varje enskilt fall, såsom per telefon, via e-post eller vid fysiska möten.

Informationen ska tillställas den verkställande direktören samt styrelsen. Ovanstående information ska vidarebefordras till andra relevanta personer inom Bolaget.

2.2 Närvaro vid styrelsesammanträden

Funktionen för regelefterlevnad ska medverka vid Bolagets ordinarie styrelsesammanträden och där avge relevant information avseende Bolagets regelefterlevnad samt besvara styrelsens frågor. Vid sammanträdena ska funktionen åtminstone lämna lämplig information om följande förhållanden:

- Omfattningen av uppdraget för funktionen för regelefterlevnad,
- innehållet i den riskanalys som ligger till grund för denna årsplan,
- regelförändringar och nyheter, domar och myndighetsbeslut, inkl. sanktionsbeslut från Finansinspektionen, samt andra händelser och förhållanden som är av betydelse för Bolagets tillståndspliktiga verksamhet,
- resultatet av genomförd uppföljning av Bolagets regelefterlevnad, samt
- eventuella avvikelser från tillämpliga regler och principiella och övriga viktiga frågor som rör verksamheten och anställdas agerande.

3 Råd och stöd

Funktionen för regelefterlevnad ska under året ge råd och stöd till relevanta personer hos Bolaget så att verksamheten bedrivs i enlighet med gällande regelverk. Sådant rådgivande och stödjande arbete ska bl.a. ske genom att funktionen finns tillgänglig för Bolagets anställda, verkställande direktör och styrelse per telefon, via e-post och för fysiska möten, för att besvara frågor som kan uppkomma i Bolagets verksamhet såvitt avser regelefterlevnad.

Funktionen för regelefterlevnad ska utgöra ett stöd för Bolaget i det fall Bolaget på eget initiativ avser att genomföra ändringar i interna regeldokument och rutiner. Funktionen för regelefterlevnad ska därför lämna kommentarer avseende sådana planerade ändringar i regeldokument som Bolaget har rapporterat. Med regeldokument avses de interna regler, riktlinjer, policyer, instruktioner m.m. som Bolaget ska upprätta för sin verksamhet enligt de regelverk som gäller för Bolagets tillståndspliktiga verksamhet.

4 Uppföljning av Bolagets regelefterlevnad

Funktionen för regelefterlevnad ska under året följa upp Bolagets regelefterlevnad. Uppföljningen av regelefterlevnaden ska ske löpande och de åtgärder som vidtas ska vara anpassade till Bolagets relevanta risker samt omvärldsfaktorer som kan medföra ett ökat behov av fördjupade kontroller i särskilda delar av verksamheten.

Funktionen för regelefterlevnad ska utifrån nedanstående uppföljningsåtgärder bedöma Bolagets regelefterlevnad och rapportera till företagsledningen enligt avsnitt 5 nedan.

4.1 Metod

Uppföljningen innefattar bl.a. genomgång av relevanta interna regler och andra styrdokument för verksamheten samt styrelseprotokoll och styrelserapporter från verkställande direktören och andra funktioner hos Bolaget, intervjuer med relevanta personer hos Bolaget och andra kontroller för att följa upp att externa och interna regler efterlevs samt genomgång av dokumentation som upprättas i verksamheten.

Uppföljningen ska i betydande utsträckning utföras på plats i Bolagets lokaler. När så är ändamålsenligt kan funktionen för regelefterlevnad istället genomföra uppföljningen på distans genom att inhämta och granska skriftligt material samt genom att ställa frågor till relevanta personer per telefon eller via e-post.

4.2 Planerade åtgärder

Funktionen för regelefterlevnad kommer att följa upp regelefterlevnaden inom Bolagets tillståndspliktiga verksamhet genom kvartalsvisa kontroller. De områden som ska följas upp samt de kontrollåtgärder som ska vidtas har bestämts utifrån den riskanalys som beskrivits i avsnitt 1 ovan.

4.2.1 Områden som kontrolleras minst årsvis

Funktionen för regelefterlevnad har identifierat följande områden där det finns risker för avvikelser från gällande regelverk som är väsentliga för Bolaget och Bolagets kunder. Områdena anges nedan och kommer att följas upp enligt den angivna tidplanen.

Kvartal 1

Område	*Kontroll*	*Metod*
Övrig regelefterlevnad	IT-säkerhet och informationssäkerhet inkl. cyberrisker.	Intervju med relevanta personer hos Bolaget för att följa upp risker kopplade till informationssäkerhet och IT. Kontrollen omfattar uppföljning av Eiopas riktlinjer om IKT-risker.
	Avbrottsfri verksamhet.	Granskning av Bolagets rutiner för att bibehålla en avbrottsfri verksamhet.

Mot bakgrund av Eiopas nya IKT-riktlinjer avser funktionen för regelefterlevnad att under årets första kvartal utföra en utökad kontroll avseende Bolagets informationssäkerhet och interna IKT-riktlinjer, inklusive avbrottsfri verksamhet och cybersäkerhet. Kontrollen syftar till att säkerställa att Bolaget efterlever Eiopas nya IKT-riktlinjer. Funktionen för regelefterlevnad kommer därmed bl.a. följa upp Bolagets IKT-strategi och arbete med att analysera bl.a. IKT-risker. Funktionen för regelefterlevnad kommer vidare begära in och granska Bolagets interna IKT-riktlinjer.

Funktionen för regelefterlevnad kommer under det andra kvartalet även följa upp och granska följande områden.

Område	*Kontroll*	*Metod*
Rapportering	Rapportering till Finansinspektionen.	Begära in information och underlag avseende Bolagets rapportering.
Övrig regelefterlevnad	Efterlevnad av regler för riskhantering.	Granskning av Bolagets efterlevnad av interna regler för riskhantering.

Kvartal 2

Fokusområde	*Kontroll*	*Metod*
Övrig regelefterlevnad	Uppföljning av Bolagets organisation inkl. nyckelpersoner.	Begära in information om eventuella ändringar i Bolagets organisation.

Funktionen för regelefterlevnad kommer under det andra kvartalet även följa upp och granska följande områden.

Område	*Kontroll*	*Metod*
Försäkringsverksamhet	Aktuariefunktionen.	Genomgång av aktuariens arbetsuppgifter samt styrdokument vid möte.
Övrig regelefterlevnad	Efterlevnad av reglerna om skuldtäckning, försäkringstekniska avsättningar och reservsättning.	Platsbesök avseende Bolagets efterlevnad av reglerna om skuldtäckning, försäkringstekniska avsättningar och reservsättning.
	Efterlevnad av försäkringstekniska riktlinjer.	Granskning av Bolagets efterlevnad av försäkringstekniska riktlinjer.
	Efterlevnad av placeringspolicy.	Granskning av Bolagets placeringar m.m. i enlighet med placeringspolicyn.
	Efterlevnad av reglerna om återförsäkringsrisker.	Granskning av Bolagets efterlevnad av reglerna om återförsäkringsrisker.

Kvartal 3

Fokusområde	*Kontroll*	*Metod*
Outsourcing	Uppdragsavtal.	Begära in och granska Bolagets uppdragsavtal.

Funktionen för regelefterlevnad avser att under tredje kvartalet närmare granska området outsourcing och då med särskilt fokus på anmälan av kritiska avtal till Finansinspektionen.

Funktionen för regelefterlevnad kommer under det tredje kvartalet även att följa upp och granska följande områden.

Område	*Kontroll*	*Metod*
Outsourcing	Uppdragstagare.	Platsbesök (vid behov) hos relevanta uppdragstagare till Bolaget för uppföljning av styrning, kontroll och beredskap.
	Riktlinjer för uppdragsavtal inkl. uppföljning av uppdragstagare.	Begära in och granska Bolagets riktlinjer för uppdragsavtal samt matris för uppföljning.
Försäkringsverksamhet	Kunskap och kompetens (inkl. fortbildningskravet) enligt försäkringsdistributions-regelverket (IDD).	Granskning av Bolagets personal och dess kompetens och kunskapsnivå samt rutiner för fortbildning. Kontrollen kommer att fokusera på kravet på uppföljande kunskapstest.
Övrig regelefterlevnad	Styrelsens samlade kompetens.	Granskning av styrelsens samlade kompetens mot bakgrund av Finansinspektionens rapport på området.
	Intressekonflikter.	Platsbesök och genomgång avseende vilka intressekonflikter Bolaget har identifierat i verksamheten och hur dessa hanteras.

Kvartal 4

Fokusområde	*Kontroll*	*Metod*
Övrig regelefterlevnad	Framåtblickande bedömning av egna risker och det egna kapitalet (ORSA).	Intervju med relevanta personer för att följa upp Bolagets rutiner avseende framtagande av ORSA. Funktionen för regelefterlevnad kommer även beakta Eiopas förväntansdokument om klimatscenarios i försäkringsföretag.

Funktionen för regelefterlevnad avser att under fjärde kvartalet närmare följa upp Bolagets rutiner för att säkerställa styrelsens samlade kompetens (fit &proper). Funktionen för regelefterlevnad kommer särskilt kontrollera Bolagets anpassning enligt Finansinspektionens rapport Dnr 19-51 om styrelsens samlade kompetens i försäkringsbolag.

Funktionen för regelefterlevnad kommer under detta kvartal även att följa upp och granska följande områden.

Område	*Kontroll*	*Metod*
Rapportering	Rapportering från centrala funktioner enligt gällande regler.	Begära in kopior av avrapportering från funktionen för riskhantering, aktuariefunktionen och internrevision.
Övrig regelefterlevnad	Intern kontroll (dualitet, avstämning m.m.).	Granskning av Bolagets rutiner avseende intern kontroll.
Försäkringsverksamhet	Skadereglering.	Platsbesök för att diskutera Bolagets rutiner vid skadereglering.
	Produktgodkännande.	Uppföljning av Bolagets rutiner för produktgodkännande.
GDPR	Gallringsrutiner.	Uppföljning av Bolagets rutiner för gallring.
	Hantering av personuppgifter inkl. konsekvensbedömningar och gallringsrutiner.	Granskning av Bolagets interna rutiner och riktlinjer för hantering av personuppgifter.

4.2.2 Områden som kontrolleras minst en gång per treårsperiod

Funktionen för regelefterlevnad har identifierat följande områden där riskerna för avvikelser från gällande regelverk inte bedöms vara väsentliga i Bolagets verksamhet. Avsikten är att dessa områden ska följas upp minst en gång under en treårscykel. Av dessa har funktionen för regelefterlevnad för avsikt att kontrollera följande områden under året.

Område	*Kontroll*	*Metod*
Rapportering	Övrig extern ekonomisk rapportering (t.ex. årsredovisning).	Granskning av Bolagets externa ekonomiska rapportering.
Övrig regelefterlevnad	Ersättningspolicy och ersättningssystem.	Granskning av Bolagets ersättningspolicy och ersättningssystem.
Försäkringsverksamhet	Standardiserade produktfaktablad.	Granskning av Bolagets hemsida och de där angivna produktfaktabladen.
	Information till försäkringstagare.	Uppföljning av Bolagets rutiner för informationsgivning.
	Bedömning av försäkringstagare och försäkringsbehov.	Uppföljning av rutinerna för bedömning av försäkringstagare och försäkringsbehov.

4.2.3 Kontroller med anledning av nya och förändrade regelverk

Funktionen för regelefterlevnad ska i nära anslutning till att ett nytt regelverk införs eller att ett befintligt regelverk förändras genomföra kontroller för att säkerställa att Bolagets verksamhet är förenlig med och/eller att Bolaget vidtagit eller planerat lämpliga åtgärder för att anpassa sig till regelverket. Sådana kontroller kommer under året att utföras beträffande bl.a. nedanstående nya regler och uttalanden:

- Eiopas riktlinjer om uppdragsavtal med molntjänstleverantörer (EIOPA-Bos-20-002).
- Eiopas riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik (EIOPA -BoS-20/600).
- Eiopas förväntansdokument om tillsynen av klimatscenarios i försäkringsföretags egen risk- och solvensbedömning (EIOPA-BoS-21-127).

5 Rapportering

5.1 Avvikelser från gällande regelverk

Om funktionen för regelefterlevnad vid fullgörandet av sitt uppdrag har uppmärksammat avvikelser från de regler som gäller för Bolagets verksamhet ska detta omedelbart rapporteras till styrelsen och den verkställande direktören. Rapporten ska innehålla en redogörelse för den specifika avvikelsen jämte förslag på åtgärder som bör vidtas för att åtgärda avvikelsen.

5.2 Kvartalsrapport

Funktionen för regelefterlevnad ska senast en månad efter slutet av föregående kalenderkvartal avge en skriftlig rapport till den verkställande direktören och styrelsen.

Rapporten ska innehålla uppgifter om vidtagna åtgärder enligt denna årsplan, eventuella händelser som under kalenderkvartalet i väsentligt avseende påverkat riskanalysen enligt avsnitt 1 och de förändringar i årsplanen som detta medför samt gjorda iakttagelser under det föregående kalenderkvartalet.

5.3 Slutrapport

Funktionen för regelefterlevnad ska senast en månad efter slutet av föregående kalenderår avge en skriftlig rapport till den verkställande direktören och styrelsen. Rapporten ska innehålla uppgifter om vidtagna åtgärder samt en samlad bedömning av Bolagets regelefterlevnad.

Vid slutet av året ska en årsplan lämnas för funktionen för regelefterlevnads arbete under nästkommande kalenderår.

Stockholm den […] 2021

Johan Grenefalk

Compliance - riskbedömning 2021 Bilaga 1

Bolag: S:t Erik Försäkrings AB

Verksamhet: Riksbolag, skadecaptive

Tillstånd: Koncession, annan förmögenhetsskada (direkt/indirekt), godstransport (direkt/indirekt), tilläggsförsäkring till livförsäkring (indirekt), försäkring mot brand och annan skada på egendom (direkt/indirekt), allmän ansvarighet (direkt/indirekt), olycksfalls- och sjukförsäkring (indirekt), olycksfall (direkt),

Konsekvens *	Sannolikhet**	Prioritet (K x S)	Uppföljning
Mycket allvarlig=4	Mycket hög=4	Mycket hög = 16 och mer	Löpande (minst 4 ggr/år)
Allvarligt = 3	Hög =3	Hög = 9 och mer	Löpande (minst 4 ggr/år)
Medel = 2	Medel = 2	Medel = 5-8 (samt om konsekvens=4)	Minst 1 ggr/år
Minimal = 1	Låg = 1	Låg = 1-4	Minst 1 ggr/treårsperiod

* Här avses primärt vilken relativ konsekvens en regelavvikelse kan förväntas få för Bolaget och kunderna. Hänsyn har dock där så är relevant också tagits till Bolagets förmåga att upprätthålla för verksamheten tillräckligt kapital samt Finansinspektionens möjligheter att utöva tillsyn.

** Här avses den relativa sannolikheten för att en regelavvikelse inträffar.

Senast uppdaterad: 211101

Områden med risk för regelavvikelser	Konsekvens	Sannolikhet	Prioritet	Kommentar/Åtgärd
Försäkringsverksamhet				
Försäkringskonsultation	3	2	6	
Återförsäkring	3	2	6	
Aktuariefunktion	3	2	6	
Skadereglering	4	2	8	
Information till försäkringstagare	3	2	6	
Bedömning av försäkringstagare och försäkringsbehov	3	2	6	
Standardiserat produktfaktablad	1	2	2	
Produktgodkännande (produktstyrnig)	3	2	6	
Administration				
Intern administration (skaderegister, ekonomi m.m.)	2	2	4	
Personaladministration m.m.	3	1	3	

Rapportering				
Rapportering till Finansinspektionen	3	2	6	
Övrig extern ekonomisk rapportering (t.ex. årsredovisning)	2	1	2	
Rapportering till kunder	2	2	4	
Marknadsföring och marknadsinformation	2	2	4	
Rapportering från centrala funktioner enligt gällande regler	3	2	6	

Outsourcing				
Uppdragavtal anpassade till verksamheten och Finansinspektionens regler	3	2	6	Riktlinjer från Eiopa om uppdragsavtal med molntjänstleverantörer
Uppföljning av uppdragstagares utförande av uppdrag samt dokumentation	3	2	6	
Beredskapsplaner	3	1	3	
Riktlinjer för uppdragsavtal inkl. matris för uppföljning	3	2	6	

Personuppgiftshantering (GDPR)				
Hantering av personuppgifter	3	2	6	
Interna rutiner och riktlinjer för hantering av personuppgifter	3	2	6	

Övrig regelefterlevnad				
Organisation och verksamhetsplan	3	2	6	
Efterlevnad av reglerna om intressekonflikter	3	2	6	
Kompetens och kunskapsnivå hos personalen/styrelsen	3	2	6	
Efterlevnad av reglerna om återförsäkringsrisker	3	2	6	
Efterlevnad av reglerna om förmånsregister, försäkringstekniska avsättningar och reservsättning	3	2	6	
Efterlevnad av reglerna om hantering av etiska frågor	3	1	3	
Efterlevnad av reglerna om riskhantering	3	2	6	
Efterlevnad av försäkringstekniska riktlinjer	3	2	6	
Ersättningspolicy och ersättningssystem	3	1	3	
Avbrottsfri verksamhet	3	2	6	

Efterlevnad av kapitalkrav	2	2	4	
Intern kontroll (dualitet, avstämning m.m.)	3	2	6	
Bedömning av egna risker och det egna kapitalet (ORSA)	3	2	6	Förtydliganden från Finansinspektionen avseende kraven för ORSA
Nyckelpersoner	3	2	6	
Aktuariefunktionen	3	2	6	
Centrala funktioner	3	2	6	
IT-säkerhet och informationssäkerhet, inkl. cybersäkerhet	3	2	6	Eiopas IKT-riktlinjer

Anpassning till nya och förändrade regelverk				
Eiopas riktlinjer om uppdragsavtal med molntjänstleverantörer (EIOPA-BoS-20-002)	3	2	6	
Eiopas riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik (EIOPA -BoS-20/600).	3	2	6	
Eiopas förväntansdokument om tillsynen av klimatscenarios i försäkringsföretags egen risk- och solvensbedömning (EIOPA-BoS-21-127).	3	2	6	