

**Beslutsunderlag**

Utfärdat 2024-01-11

Diarienummer 0008/23

Handläggare: Petra Willquist

Telefon: 031-368 55 14

E-post: petra.willquist@gotalejon.goteborg.se

## Årsrapport internrevisionen 2023

### Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar årsrapport från internrevisionen.

### Sammanfattning

Enligt Försäkringsrörelselagen 10 kap, 4§ ska försäkringsföretag ha fyra centrala funktioner. Dessa utgörs av regelefterlevnadsfunktionen, riskhanteringsfunktionen, aktuariefunktionen och internrevisionsfunktionen. Dessa kontrollfunktioner ska utvärdera systemet för internrevision, regelefterlevnad och riskhantering. Funktionerna ska även utvärdera andra delar av företagsstyrningssystemet och rapportera resultatet och lämna rekommendationer efter utvärdering till företagets styrelse.

I internrevisionens årsrapport ges en samlad redovisning av de granskningar och status över åtgärder som genomförts 2023:

- Granskning av informationssäkerhet
- Granskning av beredskap och kontinuitet
- Granskning av utlagd verksamhet

Bolaget bedömer att arbetet med rekommendationerna fortskrider tillfredsställande.

### Bedömning ur ekonomisk dimension

Internrevisionens granskning är viktig ur ett ekonomiskt perspektiv då den syftar till att säkerställa långsiktig ekonomisk hållbarhet i bolaget, vilket i sin tur syftar till att ge Göteborgs stad en långsiktigt hållbar kostnadseffektiv riskhantering.

Granskningens rekommendationer visar på områden som behöver prioriteras. Åtgärderna medför dock inga förändrade planeringsförutsättningar för bolaget utan ryms inom ordinarie verksamhet.

### Bedömning ur ekologisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

### Bedömning ur social dimension

Brister i följsamhet mot bestämmelser, regelverk och riskaptit kan leda till ökad risk för minskat förtroende för bolagets verksamhet.

### Samverkan

Ingen samverkan har genomförts.

## **Bilagor**

1. Internrevisionens årsrapport 2023
2. Status internrevisionens rekommendationer 2024-01-11

## Ärendet

Ärendet omfattar redovisning av internrevisionens årsrapport 2023. Styrelsen ska besluta om åtgärder som ska vidtas med hänsyn till resultat och rekommendationer från internrevisionsfunktionen.

För att ta del av internrevisionens rapport hänvisas till bilaga 1.

## Beskrivning av ärendet

Enligt Försäkringsrörelselagen 10 kap, 4§ ska försäkringsföretag ha fyra centrala funktioner. Dessa utgörs av regelefterlevnadsfunktionen, riskhanteringsfunktionen, aktuariefunktionen och internrevisionsfunktionen. Dessa kontrollfunktioner ska utvärdera systemet för internrevision, regelefterlevnad och riskhantering. Funktionerna ska även utvärdera andra delar av företagsstyrningssystemet och rapportera resultatet och lämna rekommendationer efter utvärdering till företagets styrelse.

Detta ärende omfattar internrevisionens årsrapport för 2023. Enligt bolagets riktlinje för internrevisionsfunktionen ska resultat och rekommendationer rapporteras till styrelsen.

I internrevisionens årsrapport ges en samlad redovisning av de granskningar som genomförts 2023. I rapporten redovisas den status över åtgärder som Göta Lejon rapporterat i december 2023, se Tabell 1.

Tabell 1: Översikt av granskningar, bedömning och status avseende internrevisionens granskningar 2023.

Område	Bedömning	Status
Informationssäkerhet	Förbättring rekommenderas avseende informationsklassificering	Slutförd
	Förbättring rekommenderas avseende följsamhet mot IKT-riktlinjer	Pågående
Beredskap och kontinuitet	Förbättring rekommenderas	Slutförd
Utlagd verksamhet	Tillfredsställande	-

Årsrapporten redovisar även en historisk översikt av bedömningar från genomförda revisioner. Göta Lejons nuvarande status avseende internrevisionens rekommendationer återfinns i bilaga 2.

## Bolagets bedömning

Det är bolagets bedömning att arbetet med rekommendationerna fortskrider tillfredsställande.



# Internrevisionens årsrapport 2023

Försäkrings AB Göta Lejon

Januari 2023



# Bakgrund och inledning

## Uppdrag

Vi har granskat Försäkrings AB Göta Lejons styrning, riskhantering och kontroll utifrån, av styrelsen, fastställd revisionsplan samt instruktion för internrevision. Revisionsplanen är baserad på de krav som ställs på internrevisionen gentemot Solvens 2, Försäkringsrörelselagen samt gentemot EIOPA:S riktlinjer för IKT och företagsstyrningssystem.

## Genomförande

Genom intervjuer, granskning av underlag samt egna stickprov har vi utvärderat den interna kontrollen, effektiviteten och ändamålsenligheten i bolagets processer.

Vi har haft ett bra samarbete med verksamheten och erhållit efterfrågat material samt återkoppling inom överenskommen tid.

## Rapportering

Efter varje genomförd granskning har våra slutsatser sammanställts i en rapport. Slutsatserna har kommunicerats skriftligen till berörd personal.

Denna rapport är en sammanfattning av de granskningar och rapporteringar som utförts under 2023. De bedömningar som lämnas här och i övrig rapportering avser endast den del av verksamheten som granskats. I granskningen har vi utgått från status vid granskningstillfället.

Under året har tre rapporter avlämnats till verksamheten, med totalt tre nya iakttagelser.



# Samlad bedömning och lämnade rapporter avseende 2023

Nedan presenteras 2023 års rapporter, baserat på den internrevisionsplan som antogs av styrelsen i början av 2023.

Vår övergripande bedömning inom granskningsområdena är att bolagets interna kontroll och styrning fungerar bra, bolaget är riskmedvetet och arbetar kontinuerligt med tillpassning till regelverk. Emellertid har vi identifierat områden för förbättring inom två av granskningsområdena.

	Område	Bedömning
2023:1	Informationssäkerhet	Förbättringar rekommenderas
2023:2	Beredskap och kontinuitet	Förbättringar rekommenderas
2023:3	Utlagd verksamhet	Tillfredsställande

## Syfte och genomförd granskning

Internrevisionen har genomfört en granskning för att bedöma bolagets rutiner och processer inom arbetet med informationssäkerhetsrisker. Vi har även utvärderat bolagets uppföljning av efterlevnad gentemot EIOPA:s riktlinjer om IKT.

## Sammanfattande bedömning

Verksamhetens arbete för att implementera och förvalta IKT-riktlinjerna från EIOPA är pågående. Bolaget har genomfört en GAP-analys gentemot IKT-riktlinjerna, återstående GAP är dokumenterade i ärendehanteringssystemet Stratsys. För närvarande återstår en del arbete rörande informationsklassificering.

## Årets iakttagelser

### • Informationsklassificering

Vi gör iakttagelsen att det saknas en övergripande tidsplan för när arbetet med informationsklassificering skall vara avklarat, samt tidsplaner för eventuella delmål.

Vi rekommenderar verksamheten att upprätta en övergripande målbild med delmål och budget för när de vill vara klara med informationsklassificeringen. Avrapportering av status och framdrift i arbetet bör ske löpande till styrelsen.

### • Åtgärdsplaner för fastställda GAP inom IKT-riktlinjerna

Vi gör iakttagelsen att det inte finns någon överblick över vilka resurser som krävs, tidsplan eller prioriteringsordning för återstående GAP.

Vi rekommenderar verksamheten att sammanställa en åtgärdsplan för att åtgärda återstående GAP. Denna plan bör innehålla prioriterade aktiviteter med ansvarig och datum för uppföljning och slutförande.

## Verksamhetens svar

Bolaget instämmer i iakttagelserna och har tagit fram en plan för arbetet med ansvar och datum. Prioritering av aktiviteter sker löpande.

### Status enligt verksamheten december 2023

Plan för informationsklassificering är framtagen och samtliga processägare har klassat information i sin respektive process. Åtgärden är avklarad.

Plan för att stänga återstående GAP är framtagen. Samtliga gap kommer att gås igenom under Q1 2024 av bolagets riskkommitté tillsammans med processägare IT. Ca 25% av återstående GAP har stängts.

# 2023:2 Beredskap och Kontinuitet

Förbättringar rekommenderas

## Syfte och genomförd granskning

Granskningens har syftat till att bedöma bolagets beredskap för störningar i verksamheten samt förmåga att driva den affärskritiska verksamheten i händelse av störningar. Granskningen har även syftat till att utvärderat bolagets efterlevnad avseende beredskap och kontinuitet gentemot Solvens 2, Försäkringsrörelselagen samt gentemot EIOPA:s riktlinjer för företagsstyrningssystem (EIOPA-BoS-14/253).

## Sammanfattande bedömning

Bolaget bedöms vara riskmedvetet och arbeta proaktivt för att kunna driva den affärskritiska verksamheten i händelse av störningar. Därtill bedöms rutinerna för att identifiera risker, uppdatera krislednings-/kontinuitetsplanen samt genomföra och följa upp utlagd verksamhet vara goda och svara upp mot gällande regelverk.

Emellertid saknas specifika överlämningsplaner för återtagande av utlagt verksamhet alternativt byte av tjänsteleverantör.

## Årets iakttagelser

- **Överlämningsplaner**

Specifika överlämningsplaner för återtagande av utlagt verksamhet alternativt byte av tjänsteleverantör saknas. Enligt riktlinje 63d i EIOPA:s riktlinjer för företagsstyrningssystem ska det finnas en exitstrategi för utlagd verksamhet.

Bolaget rekommenderas utarbeta specifika överlämningsplaner för utlagt verksamhet som beskriver de åtgärder som behöver vidtas vid återtagande av utlagt verksamhet alternativt byte av tjänsteleverantör.

## Verksamhetens svar

Bolaget avser att utveckla kontinuitetsplanen för att förbättra processen för återuppbyggnad.

## Status enligt verksamheten december 2023

Kontinuitetsplanen har uppdaterats med information om återuppbyggnad vid avbrott i leverans av utlagd verksamhet. Åtgärden är avklarad.



# 2023:3 Utlagd verksamhet

Tillfredsställande

## Syfte och genomförd granskning

Syftet har varit att bedöma bolagets hantering av utlagd verksamhet samt utvärdera bolagets efterlevnad inom området gentemot Solvens 2 (2015/35) och Försäkringsrörelselagen (2010:2043).

Vi har emottagit underlag som har övergripande analyserats. Utöver dokumentgranskning, har vi genomfört intervjuer för att utvärdera verksamhetens arbete inom området samt tagit stickprov av huvudavtal respektive tilläggsavtal med iFacts och Intraservice.

## Sammanfattande bedömning

Verksamheten bedöms ha goda rutiner och processer vid utläggning av verksamhet samt uppföljning av utlagd verksamhet. Verksamheten har rutiner är dokumenterade och bedöms svara upp mot gällande lag- och regelverkskrav. Vi har också noterat att där huvudavtal inte levt upp till gällande krav har dessa kompletterats med tilläggsavtal.

## Årets iakttagelser

Inga nya iakttagelser lämnas.

## Verksamhetens svar

Verksamheten instämmer med resultatet av granskningen.

# Historisk översikt av sammanfattande bedömningar

	2020	2021	2022	2023
Riskkontroll	◆	◆	◆	
Compliance	◆	◆	◆	
Aktuariefunktionen	◆	◆	◆	
Datakvalitet	◆			
Förmånsrättigheter				
ORSA			◆	
Kontinuitets- och beredskapsplan		◆		◆
Rapportering enligt regelverket (FRL) – extern rapportering	◆			
Styrelsens lämplighet och kompetens			◆	
Skaderegleringsprocessen		◆		
Utlagd verksamhet				◆
Återförsäkring			◆	
Informationssäkerhet				◆

## Bedömning av området

- ◆ = Tillfredsställande
- ◆ = Förbättringar rekommenderas
- ◆ = Förbättringar behövs
- ◆ = Otillfredsställande

# Bilaga 1 - Bedömningskriterier

Den sammanfattande bedömningen av den interna styrningen och kontrollen av det granskade området klassificeras i fyra nivåer enligt nedan.

## Sammanfattande bedömning

<b>Tillfredsställande</b>	Den interna kontrollen bedöms i allt väsentligt fungera tillfredsställande. Mindre förbättringsmöjligheter kan ha noterats.
<b>Förbättring rekommenderas</b>	Den interna kontrollen bedöms kunna förbättras. En eller flera brister har noterats som kan innebära en utökad risknivå.
<b>Förbättring behövs</b>	Den interna kontrollen bedöms ha förbättringsbehov. En eller flera väsentliga brister har noterats som kan innebära en oönskad risknivå.
<b>Otillfredsställande</b>	Den interna kontrollen bedöms vara otillfredsställande. En eller flera kritiska brister har noterats som kan innebära en oacceptabel risknivå.

Bedömningen av enskilda iakttagelser i granskningen klassificeras i tre nivåer enligt nedan.

## Bedömning av enskilda iakttagelser

<b>Låg prioritet</b>	Iakttagelsen bedöms troligen inte påverka måluppfyllnaden eller resultera i finansiella eller operationella förluster. Förbättringsmöjligheter avseende ändamålsenlighet och effektivitet kan finnas. Åtgärder rekommenderas.
<b>Medelprioritet</b>	Iakttagelsen bedöms kunna påverka måluppfyllnaden eller resultera i finansiella eller operationella förluster. Åtgärder bör vidtas inom rimlig tidsperiod.
<b>Hög prioritet</b>	Iakttagelsen bedöms påverka måluppfyllnaden eller på kort tid resultera i finansiella eller operationella förluster. Åtgärder bör snarast vidtas.



**Björn Widing**

Internrevisor

073-583 61 96

[bjorn.widing@kpmg.se](mailto:bjorn.widing@kpmg.se)



[kpmg.se](https://www.kpmg.se)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG AB, a Swedish limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

**Document Classification: KPMG Confidential**

# **Status internrevisionens rekommendationer**

---

Göta Lejon

2024



## Innehållsförteckning

<b>1 Rekommendationer och åtgärder .....</b>	<b>3</b>
1.1 2022 - Internrevision kvartal 1 - Återförsäkring .....	3
1.2 2022 - Internrevision kvartal 2 - ERSA.....	4
1.3 2022 - Internrevision kvartal 4 - Nyckelfunktionerna .....	4
1.4 2023 - Internrevision kvartal 1 - Informationssäkerhet .....	6
<b>2 Nyligen avslutade rekommendationer .....</b>	<b>7</b>
2.1 2022 - Internrevision kvartal 4 - Nyckelfunktionerna .....	7
2.2 2023 - Internrevision kvartal 1 - Informationssäkerhet .....	7
2.3 2023 - Internrevision kvartal 2 - Kontinuitet- och beredskapsplan .....	8





# 1 Rekommendationer och åtgärder



## 1.1 2022 - Internrevision kvartal 1 - Återförsäkring



Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Aktiviteten beräknas vara slutförd
<p><b>Värdering av återförsäkringsgivare</b></p> <p>Bolaget saknar en rutin för att avge återförsäkring till nya motparter.</p> <p>Risk Avsaknad av rutiner för nya motparter kan innebära en risk för ofullständigt återförsäkringsprogram eftersom det kan vara svårt att få full täckning för återförsäkringsprogram.</p> <p>Rekommendation Vi rekommenderar bolaget att upprätta rutiner för att avge återförsäkring till nya motparter vilken kan användas om återförsäkringsprogram inte är möjligt att täckas av kända återförsäkringsgivare inom gällande riskaptit.</p>	<p> Gul</p>	<p>Översyn av rutiner för att avge återförsäkring till nya motparter, som ska kunna användas om återförsäkringsprogram inte är möjligt att täckas av kända återförsäkringsgivare inom gällande riskaptit.</p>	<p> 75% genomfört</p>	<p>Linda Nilunger</p>	<p>Bolaget ser inte behovet av en rutin för att avge återförsäkring till nya motparter. Det finns en riktlinje för återförsäkring. Bolaget handlar dessutom upp enligt LOU och måste alltid följa detta regelverk. Det tillkommer ofta nya motparter för att uppnå full täckning av återförsäkringsprogrammen. Bolaget ställer samma krav på gamla motparter som det gör på nya.</p>	<p>2024-03-31</p>

## 1.2 2022 - Internrevision kvartal 2 - ERSA

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Aktiviteten beräknas vara slutförd
<p><b>ERSA-rapporten</b></p> <p>Bolagets riktlinjer saknar en tydlig beskrivning av processen för att säkerställa datakvalité i ERSA. EIOPAs riktlinjer för egen risk- och solvensbedömning sätter ramarna för innehållet i en ERSA-rapport, under metoder och tillvägagångsätt inbegrips även krav på datakvalité. Bolaget beskriver i riktlinje för egen risk och solvensanalys (avsnitt 2.9) "ERSA-processen ställer samma krav på datakvalitet och spårbarhet som övriga processer inom bolaget.". Vidare uttalar sig aktuarien i aktuariefunktionens årsrapport om datakvalité som låg risk med "risk för felkällor i dataunderlaget".</p> <p>Risk Risk för felaktiga beräkningar om bolaget inte kan säkerställa datakvalitén i solvensberäkningarna.</p> <p>Rekommendation Vi rekommenderar bolaget att utveckla avsnittet avseende datakvalité och formalisera en process med kontroller för att säkerställa att dataunderlaget i solvensberäkningen uppfyller kraven på datakvalité.</p>	 Gul	<p>Utveckling av avsnittet avseende datakvalité och formalisering av en process med kontroller för att säkerställa att dataunderlaget i solvensberäkningen uppfyller kraven på datakvalité.</p>	 25% genomfört	<p><i>Björn Wennerström</i></p>	<p>Riskhanteringsfunktion en håller på att titta på detta.</p>	<p>2024-03-31</p>

## 1.3 2022 - Internrevision kvartal 4 - Nyckelfunktionerna

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Aktiviteten beräknas vara slutförd
<p><b>Riskhanteringsfunktionen - incidentrapportering</b></p> <p>Bolaget har osedvanligt få iakttagelser rapporterade i sitt incidentrapporteringsregister.</p> <p>Risk Bolaget riskerar att inte förmedla inträffade incidenter, således även risker och eventuella brister till andra linjens riskhanteringsfunktion</p> <p>Rekommendation Då kritisk funktion eller aktivitet så som skador är utlagd på extern leverantör bör uppföljning av leverantör ses över för att säkerställa att rapportering av incidenter utförs i enlighet med process. Bolaget rekommenderas att uppdra åt riskhanteringsfunktionen att se över process och genomförande av incidentrapportering.</p>	 Orange	<p>Uppdra åt riskhanteringsfunktionen att se över process och genomförande av incidentrapportering. Då kritisk funktion eller aktivitet så som skador är utlagd på extern leverantör bör uppföljning av leverantör ses över för att säkerställa att rapportering av incidenter utförs i enlighet med process.</p>	 25% genomfört	<p><i>Björn Wennerström</i></p>	<p>Riskhanteringsfunktion en håller på att titta på detta.</p>	<p>2023-12-31</p>

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Aktiviteten beräknas vara slutförd
<p><b>Aktuariefunktionen - osäkerhet och känslighetsanalys</b></p> <p>Aktuariefunktionen bör i Aktuarieintyg utveckla sin bedömning av osäkerheten i de försäkringstekniska avsättningarna med en känslighetsanalys baserad på parameterval, i synnerhet med betoning på lämplighet och val av svansskattningar för Trafik och Ansvarsförsäkring. Solvens 2 förordningen (2015/35) artikel 264 beskriver att bolaget minst årligen ska validera sina beräkningar vilket innefattar 1.e. att de antaganden som används vid beräkningen av försäkringstekniska avsättningar är ändamålsenliga och realistiska. I enlighet med artikel 22 (a) innebär detta att bolaget ska kunna förklara och motivera val samt den osäkerhet som är förknippade med antagandet samt relevanta alternativa antaganden. I enlighet med artikel 265 1 b ska valet av antaganden dokumenteras och 265 3 vad dokumentationen ska omfatta. Vidare beskriver artikel 272 1. de uppgifter aktuariefunktionen ska fullgöra varav b. bedöma graden av osäkerhet i skattningar. Sammantaget med bakgrund av regelverk och av portföljens andel i Trafik- och Ansvarsförsäkring kan bolaget med fördel utveckla dessa delar i dokumentation och rapportering till styrelse.</p> <p>Risk Bolagets ledning riskerar att inte inneha full insyn i de antaganden och den osäkerhet som föreligger i bolagets skattning av FTA samt inte uppfylla externa regelverkskrav.</p> <p>Rekommendation Bolaget rekommenderas att utveckla känslighetsanalys och kvantifiera osäkerhet i FTA med val av svansskattningar och dokumentation på underliggande antaganden i Aktuarieintyg.</p>	Gul	Utveckla känslighetsanalys och kvantifiera osäkerhet i FTA med val av svansskattningar och dokumentation på underliggande antaganden i Aktuarieintyg	 25% genomfört	<i>Björn Wennerström</i>	Aktuarien behöver komplettera med detta i årets aktuarieintyg.	2023-12-31
<p><b>Riskhanteringsfunktionens årsplan</b></p> <p>Riskhanteringsfunktionens årsplan saknar referens till den treårsplan som årsplanen ska vara baserad på enligt Riktlinje för riskhantering.</p> <p>Risk Saknar årsplanen en koppling till funktionens treårsplan finns det risk för att funktionens inplanerade aktiviteter inte blir gjorda över en treårsperiod.</p> <p>Rekommendation Vi rekommenderar att årsplanen refererar till den treårsplan som är lagd för funktionens arbete.</p>	Gul	Se till att årsplanen för riskhanteringsfunktionen refererar till den treårsplan som är lagd för funktionens arbete.	 25% genomfört	<i>Björn Wennerström</i>	Kommer att ske i nästa års plan som tas i januari 2024.	2023-12-31



Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Aktiviteten beräknas vara slutförd
<p><b>Aktuariefunktionens arbete</b></p> <p>Tidigare internrevision har granskat bolagets försäkringstekniska beräkningsunderlag och har noterat ett antal brister. Följande delar bör läggas till eller förtydligas:</p> <ul style="list-style-type: none"> <li>• Datum samt notering när den är fastställd</li> <li>• Ändringshistorik</li> <li>• Tydliga hänvisningar</li> <li>• Beräkningsformler och metoder beskrivs endast på en övergripande nivå</li> </ul> <p>Rekommendation 2019 Tidigare internrevisions rekommendation är att bolaget uppdaterar försäkringstekniskt beräkningsunderlag.</p> <p>Internrevisionens bedömning 2022 Det föreligger fortfarande brister i bolagets FTB som bör uppdateras med utestående korrigeringar noterade ovan. Avseende hänvisningar och beräkningsformler bör FTB referera till parametervalsdocument eller på övrigt sätt dokumenterade val av parametrar och beskrivning av metoder så att beräkningar ska kunna återskapas.</p>	Orange	Uppdatera bolagets FTB som bör uppdateras med utestående korrigeringar. Avseende hänvisningar och beräkningsformler bör FTB referera till parametervalsdocument eller på övrigt sätt dokumenterade val av parametrar och beskrivning av metoder så att beräkningar ska kunna återskapas. Tidigare internrevisions rekommendation är att bolaget uppdaterar försäkringstekniskt beräkningsunderlag	25% genomfört	<i>Björn Wennerström</i>	Aktuarien har fått detta i uppdrag. Försäkringstekniskt beräkningsunderlag (FTB) ska uppdateras.	2023-12-31

## 1.4 2023 - Internrevision kvartal 1 - Informationssäkerhet




Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Aktiviteten beräknas vara slutförd
<p><b>Åtgärdsplaner för fastställda GAP inom IKT-riktlinjerna</b></p> <p>Vi rekommenderar verksamheten att sammanställa en åtgärdsplan för de fastställda GAP som återstår för att efterleva IKT-riktlinjerna. Denna plan bör innehålla prioriterade aktiviteter med ansvarig och datum för uppföljning och slutförande. Verksamheten kan med fördel även utvärdera behovet av att sätta en övergripande budget, exempelvis estimerade arbetstimmar, för att säkerställa att arbetet tillskrivs tillräckliga resurser. Regelbunden avrapportering av status och framdrift i arbetet bör ske, i förslagsvis riskråd eller styrelse.</p>	Gul	Stäng samtliga GAP avseende IKT-riktlinje	25% genomfört	<i>Petra Willquist</i>	Arbete med att stänga gap pågår löpande.	2024-06-10



## 2 Nyligen avslutade rekommendationer

### 2.1 2022 - Internrevision kvartal 4 - Nyckelfunktionerna



Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar
<p><b>Regelefterlevnadsfunktionen - Styrdokument</b></p> <p>Bolagets styrdokument innehåller felaktigt ansvarsutkrävande från internrevision. I riktlinjer för regelefterlevnad under rubrik "efterlevnad" anges - "Internrevisionsfunktionen ansvarar för att riktlinjen efterlevs.", denna uppgift bör åligga bolagets internt och inte en kontrollfunktion.</p> <p>Risk Bolagets riskerar felaktigt delegerat ansvar för regelefterlevnad.</p> <p>Rekommendation Formalisera ansvar för efterlevnad av regelefterlevnad internt inom bolaget, förslagsvis styrelsemedlem och uppdatera riktlinjer i enlighet med detta.</p>	 Gul	<p>Formalisera ansvar för efterlevnad av regelefterlevnad internt inom bolaget, förslagsvis styrelsemedlem och uppdatera riktlinjer i enlighet med detta.</p>		<p><i>Björn Wennerström</i></p>	<p>Vice ordförande är utsedd till beställansvarig.</p>

### 2.2 2023 - Internrevision kvartal 1 - Informationssäkerhet

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar
<p><b>Informationsklassificering</b></p> <p>Vi rekommenderar verksamheten att upprätta en övergripande målbild samt delmål med tillhörande tidsplaner för när de vill vara klara med informationsklassificeringen. Med fördel kan detta sedan knytas an till uppföljningsbara aktivitets- och handlingsplaner med de aktiviteter som ska genomföras inom ramarna för respektive mål. Vidare rekommenderas verksamheten att upprätta en budget avseende de resurser som krävs för att nå i mål med arbetet inom de angivna tidsramarna. Avrapportering av status och framdrift i arbetet bör ske löpande till styrelsen.</p>	 Orange	<p>Klassificera bolagets information</p>		<p><i>Petra Willquist</i></p>	<p>Samtliga processägare har klassat information i sin respektive process.</p>
		<p>Ta fram planering för slutförande av informationsklassificering.</p>		<p><i>Petra Willquist</i></p>	<p>Plan är framtagen</p>

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar
<p><b>Åtgärdsplaner för fastställda GAP inom IKT-riktlinjerna</b></p> <p>Vi rekommenderar verksamheten att sammanställa en åtgärdsplan för de fastställda GAP som återstår för att efterleva IKT-riktlinjerna. Denna plan bör innehålla prioriterade aktiviteter med ansvarig och datum för uppföljning och slutförande. Verksamheten kan med fördel även utvärdera behovet av att sätta en övergripande budget, exempelvis estimerade arbetstimmar, för att säkerställa att arbetet tillskrivs tillräckliga resurser. Regelbunden avrapportering av status och framdrift i arbetet bör ske, i förslagsvis riskråd eller styrelse.</p>	 Gul	<p>Ta fram planering för aktiviteter för att stänga GAP i syfte att efterleva IKT-riktlinjer</p>		<p><i>Petra Willquist</i></p>	<p>Plan är framtagen. Samtliga gap kommer att gås igenom under Q1 2024 av bolagets riskkommitté tillsammans med processägare IT.</p>

## 2.3 2023 - Internrevision kvartal 2 - Kontinuitet- och beredskapsplan

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar
<p><b>Överlämningsplaner för återtagande av utlagd verksamhet alternativt byte av tjänsteleverantör</b></p> <p>Specifika överlämningsplaner för återtagande av utlagd verksamhet alternativt byte av tjänsteleverantör saknas. Enligt riktlinje 63d i EIOPA:s riktlinjer för företagsstyrningssystem ska det finnas en exitstrategi för utlagd verksamhet. Avsaknaden av sådana planer försvårar bedömningen av när byte av tjänsteleverantör är lämpligt samt försvårar ett eventuellt byte.</p>	 Gul	<p>Utveckla kontinuitetsplanen för att förbättra processen för återuppbyggnad avseende avbrott i leverans av utlagd verksamhet.</p>		<p><i>Petra Willquist</i></p>	<p>Kontinuitetsplanen har uppdaterats med information om återuppbyggnad vid avbrott i leverans av utlagd verksamhet.</p>