Beslutsunderlag
Utfärdat: 2023-09-01
Diarienummer 0008/23

Handläggare: Petra Willquist

Telefon: 031-368 55 14
E-post: petra.willquist@gotalejon.goteborg.se

Rapport från Internrevisionen

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar rapport 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.

Internrevisionen har under första kvartalet granskat bolagets arbete med informationssäkerhet. Internrevisionen rekommenderar bolaget att upprätta uppföljningsbara aktivitets- och handlingsplaner inklusive resursåtgång och/eller budget för ett strukturerat, ändamålsenlig informationssäkerhets- och IKT-arbete. Göta Lejon har tagit fram handlingsplaner i styrning och ledningssystemet Stratsys där arbetet resurssatts, planerats i tid och följs upp.

Bedömning ur ekonomisk dimension

Internrevisionens granskning 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 högre. 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. Rapport internrevisionen kvartal 1, Granskning inom informationssäkerhet, internrevisionsrapport 2023:1
2. Uppföljning rekommendationer internrevision kvartal 1
3. Uppföljning av informationssäkerhetsarbete kvartal 2 2023

Ärendet

Styrelsen ska besluta om åtgärder som ska vidtas med hänsyn till resultat och rekommendationer från internrevisionsfunktionen avseende informationssäkerhet.

För att ta del av internrevisionens rapport och bolagets uppföljning hänvisas till bilaga 1, 2 och 3.

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 behandlar rekommendationer internrevisionens granskning. Enligt bolagets riktlinje för internrevisionsfunktionen resultat och rekommendationer rapporteras till styrelsen.

Internrevisionens rekommendationer återfinns tillsammans med bolagets uppföljning i bilaga 2. Rekommendationerna avser informationsklassificering och gap mot riktlinjer. Internrevisionen rekommenderar bolaget att upprätta uppföljningsbara aktivitets- och handlingsplaner inklusive resursåtgång och/eller budget för ett strukturerat, ändamålsenlig informations-säkerhets- och IKT-arbete. Göta Lejon har tagit fram handlingsplaner i styrning och ledningssystemet Stratsys där arbetet resurssatts, planerats i tid och följs upp. Handlingsplanerna återfinns i bilaga 3.

Bolagets bedömning

Det är bolagets bedömning att arbetet med rekommendationerna fortskrider tillfredsställande.

Granskning inom informationssäkerhet

Internrevisionsrapport 2023:1

Försäkrings AB Göta Lejon

13 juni 2023

Till Styrelse och VD Annika Forsgren

För kännedom till Säkerhetschef Petra Willquist och vVD Ekonomichef Björn Wennerström

1. Sammanfattande bedömning

Verksamhetens arbete för att implementera och förvalta IKT-riktlinjerna från EIOPA är pågående. För närvarande återstår en del arbete rörande informationsklassificering.

Bolaget har genomfört en GAP-analys gentemot IKT-riktlinjerna, återstående GAP är dokumenterade i ärendehanteringssystemet Stratsys. Vidare har en GAP-analys inom informationssäkerhetsområdet genomförts, med stöd av verktyg från MSB (Myndigheten för samhällsskydd och beredskap) och Informationssäkerhet.se, i syfte att stärka arbetet i verksamheten och höja mognaden inom informationssäkerhetsområdet. Däremot finns inte en tydlig målbild eller plan för när i tid man ska vara i hamn med att stänga GAP som identifierats gentemot IKT-riktlinjerna. Det finns inte heller någon plan för hur man skall prioritera återstående aktiviteter.

För iakttagelserna ovan angavs resursbrist vara huvudsaklig orsak till att verksamheten inte kommit i mål med det planerade arbetet. Vi noterar att man inte etablerat någon översikt av resursåtgång, exempelvis budget över estimerade arbetstimmar för att slutföra respektive arbete. Det sker inte heller någon löpande rapportering av framdriften inom respektive område gentemot styrelsen.

Vi rekommenderar bolaget att upprätta uppföljningsbara aktivitets- och handlingsplaner inklusive resursåtgång och/eller budget för ett strukturerat, ändamålsenlig informationssäkerhets- och IKT-arbete.

Rapporten i sin helhet och dess iakttagelse har klassificerats i enlighet med kriterierna i Appendix 1.

Tillfredsställande	**Sammanfattande bedömning av det granskade området:**	**Förbättringar rekommenderas** En eller flera brister i den interna kontrollen noterade som, om åtgärder inte vidtas, kan resultera i en utökad risknivå.
Förbättringar rekommenderas		
Förbättringar behövs		
Otillfredsställande		

2. Inledning

2.1 Syfte

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.

Granskningen har genomförts i enlighet med fastställd internrevisionsplan för 2023.

2.2 Genomförande

Vi har emottagit och övergripande analyserat de underlagen som finns specificerade i Appendix 2.

Utöver dokumentgranskning har vi genomfört intervjuer för att utvärdera verksamhetens arbete inom området. Vi har inte tagit egna stickprov.

Intervjuerna genomfördes via Microsoft Teams med Säkerhetschef Petra Willquist samt med vice VD och Ekonomichef Björn Wennerström

Granskningen har genomförts av Björn Widing och Sebastian Lennartsson i april-maj 2023.

3. Iakttagelser och rekommendationer

3.1 Informationsklassificering

Medel

Verksamheten har påbörjat arbetet att klassificera samtliga informationstillgångar, arbetet drivs av Säkerhetschef tillsammans med systemansvarig och processägare för respektive process. Verksamheten uppger i intervju att en stor del arbetet är återstående och anger resursbrist som en av orsakerna till att arbetet ännu inte slutförts.

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

Risk

Utan konkreta uppsatta tidsplaner och målbild för informationsklassificeringsarbetet finns risk att man inte uppnår IKT-strategin eller arbetar med informationssäkerhet och IKT-riktlinjerna på ett önskvärt vis. Risk för att man inte är medveten om förhöjd risk genom att man inte efterlever riktlinjerna i EIOPA-BoS-20/600.

Vidare finns risk för att arbetet med informationsklassificering sker med otillräckliga resurser eller i annan riktning än den som avsetts av styrelsen.

Rekommendation

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.

Verksamhetens svar:

Beslutade åtgärder: Bolaget instämmer i iakttagelserna och har tagit fram en plan för arbetet med ansvar, resurser och budget.

Ansvarig: Petra Willquist

Deadline: 2023-12-31

3.2 Åtgärdsplaner för fastställda GAP inom IKT-riktlinjerna

Låg

Verksamhetens har genomfört en GAP-analys gentemot riktlinjerna från EIOPA inom IKT- och säkerhetsrisker. Fastställda GAP från denna har sammanställts och uppdaterats löpande i ärendehanteringssystemet Stratsys.

Vi gör däremot iakttagelsen att det inte finns någon tidsplan eller prioriteringsordning för återstående GAP. Det finns heller ingen överblick över vilka resurser som krävs, budget eller tidsestimat för åtgärderna.

Risk

Risk att verksamheten inte kommer i mål med efterlevnad inom önskvärd tid, samt att framdrift och status i implementeringsarbetet av IKT-riktlinjerna inte kommer till ledningens och styrelsens kännedom. Risk för personberoende eller att fel aktiviteter prioriteras.

Utan konkreta uppsatta planer och aktiviteter samt rapportering och uppföljning av dessa finns risk att man inte hanterar IKT riktlinjerna på ett önskvärt vis. Vidare finns risk att arbetet sker med otillräckliga resurser eller i annan riktning än den som avsetts av styrelsen.

Rekommendation

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.

Verksamhetens svar:

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

Ansvarig: Petra Willquist

Deadline: 2024-06-10

KPMG AB

Björn Widing	Sebastian Lennartsson
Internrevisor	Internrevisor

Appendix 1 Kriterier för utvärdering

Den sammanfattande bedömningen av effektivitet och ändamålsenlighet i den interna styrningen och kontrollen avseende granskad process/område klassificerar internrevisionen i fyra nivåer enligt nedan.

Klassificering av internrevisionsrapporter	
Tillfredsställande	Inga väsentliga brister i den interna kontrollen har identifierats. Mindre förbättringsmöjligheter noterade vilka bör beaktas inom en rimlig tidsram.
Förbättringar rekommenderas	En eller flera brister i den interna kontrollen noterade som, om åtgärder inte vidtas, kan resultera i en utökad risknivå.
Förbättringar behövs	En eller flera väsentliga brister i den interna kontrollen noterade som, om åtgärder inte vidtas, kan resultera i en oönskad risknivå.
Otillfredsställande	En eller flera kritiska brister i den interna kontrollen vilka innebär att organisationen exponeras för en oacceptabel risknivå.

Den sammanfattande bedömningen av effektivitet och ändamålsenlighet i den interna styrningen och kontrollen avseende enskilda iakttagelser i granskningen klassificerar internrevisionen i tre nivåer enligt nedan.

Klassificering av enskilda iakttagelser i granskningen	
Låg prioritet	Iakttagelsen bedöms troligen inte kunna resultera i finansiella eller operationella förluster men kan inrymma möjligheter att förbättra effektivitet och ändamålsenlighet. Korrigerande åtgärder rekommenderas.
Medelprioritet	Iakttagelsen är av återkommande karaktär eller bedöms kunna resultera i finansiella eller operationella förluster om inga åtgärder vidtas. Korrigerande åtgärder bör hanteras inom rimlig tidsperiod.
Hög prioritet	Iakttagelsen kan på kort tid resultera i finansiell eller operationell förlust inom området om den inte åtgärdas. Rekommenderar att åtgärd snarast implementeras.

Appendix 2 Underlag

– Avtal (Kommungemensamma interna tjänster samt Interna tjänster)

– Avtal Ver nr 6801001220 iFacts

– Bilaga 1 Säkerhet

– Bilaga 3 Drift Verksamhetsspecifika system

– Bilaga 6 SLA-nivåer

– Bilaga 7 Kris och kontinuitetsplan Intraservice

– Försäkrings AB Göta Lejon risk och säkerhetsprogram

– Försäkrings AB Göta Lejons Krisledningsplan

– Gapanalys IKT_Captive

– Gap-analys uppdaterad april 2023 t o m riktlinje 15

– Göteborgs stads regel för chefers informationssäkerhetsansvar

– Göteborgs stads regel för IT-användare

– Göteborgs stads regel gällande driftsdokumentation för IT-baserade informations-system

– Göteborgs stads regler för användande av e-post

– Göteborgs stads riktlinje för informationssäkerhet

– Kontinuitetsplan 2023 - begränsad

– Kriskommunikationsplan

– Riktlinje EIOPA IKT

– Riktlinje för internrevision

– Riktlinje för riskhantering

– Riktlinje för utlagd verksamhet

– Riktlinje för utlagd verksamhet Bilaga 1

– Riktlinje för utlagd verksamhet Bilaga 2

– Riskanalys

– Riskanalys IKT-risker

- Riskpolicy
- Rutin för incidenthantering
- Strategi och mål informationssäkerhet Göta Lejon
- Tilläggsavtal
- Tilläggsavtal Göta Lejon och Intraservice
- Uppföljning gap-analys mot stadens riktlinje
- Utlagd verksamhet Checklista Utvärdering
- Årsrapport Försäkrings AB Göta Lejon 2022
- Översikt IKT-krav och motsv. styrande dokument

Uppföljning rekommendationer

Rapport	Rekommendationer	Aktiviteter
2023 - Internrevision kvartal 1 - Informationssäkerhet	**Informationsklassificering** **Beskrivning** 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.	**Klassificera bolagets information** **Status** **Ansvarig** *Petra Willquist* **Start- och slutdatum** 2023-08-26 2023-12-31 **Senast uppdaterad** 2023-08-26
		Ta fram planering för slutförande av informationsklassificering. **Status** **Ansvarig** *Petra Willquist* **Start- och slutdatum** 2023-08-26 2023-08-31 **Senast uppdaterad** 2023-08-26
	Åtgärdsplaner för fastställda GAP inom IKT-riktlinjerna **Beskrivning** 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.	**Ta fram planering för aktiviteter för att stänga GAP i syfte att efterleva IKT-riktlinjer** **Status** **Ansvarig** *Petra Willquist* **Start- och slutdatum** 2023-08-26 2023-08-31 **Senast uppdaterad** 2023-08-26
		Stäng samtliga GAP avseende IKT-riktlinje **Status** **Ansvarig** *Petra Willquist* **Start- och slutdatum** 2023-08-26 2024-06-10 **Senast uppdaterad** 2023-08-26

Uppföljning av informationssäkerhetsarbete

Göta Lejon
Kvartal 2 2023

Innehållsförteckning

1 Statusrapportering

Område	Startdatum + Slutdatum	Projektledare	Statusbedömning	Övergripande status & kommentar
Genomföra informationsklassning	2022-10-01 2023-12-31	**Projektledare** Petra Willquist	**Resurser** Enligt plan **Tidplan** Enligt plan **Kvalitet** Enligt plan	Pågående enligt plan Informationsklassningen fortsätter enligt plan. Bolaget har uppdaterat de interna bedömningskriterierna med anledning av förändrad klassningsmatris i stadens nya riktlinje för informationssäkerhet.
Stänga gap mot IKT-riktlinjer	2020-05-01 2024-06-10	**Projektledare** Petra Willquist	**Resurser** Enligt plan **Tidplan** Enligt plan **Kvalitet** Enligt plan	Pågående enligt plan Arbetet pågår enligt plan. Säkerhetschef, ekonomichef och processägare IT ska under hösten 2023 gå igenom samtliga gap.

2 Resursuppföljning

2.1 Genomföra informationsklassning - resursuppföljning

Område	Budgetuppskattning - tid	Projektorganisation
Genomföra informationsklassning	80 timmar	**Projektledare** Petra Willquist **Projektdeltagare** Hanna Svantesson, Annika Forsgren, Björn Wennerström, Magnus Svedmark, Cecilia Jansson, Linda Nilunger, Petra Willquist **Externa resurser** Inga

Projektdeltagare	Planerade h	Utfall h	Återstående h
Hanna Svantesson	20 h		
Annika Forsgren	8 h		
Björn Wennerström	8 h		
Magnus Svedmark	8 h		
Cecilia Jansson	8 h		
Linda Nilunger	8 h		
Petra Willquist	20 h		

2.2 Stänga gap mot IKT-riktlinjer - resursuppföljning

Område	Budgetuppskattning - tid	Projektorganisation
Stänga gap mot IKT-riktlinjer	80 timmar	**Projektledare** Petra Willquist **Projektdeltagare** Hanna Svantesson, Petra Willquist **Externa resurser** Inga

Projektdeltagare	Planerade h	Utfall h	Återstående h
Hanna Svantesson	40 h		
Petra Willquist	40 h		