Tjänsteutlåtande
Utfärdat: 2024-11-08
Diarienummer 0084/24

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

Uppföljning av status på rekommendationer från kontrollfunktioner

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar status för rekommendationer från externa kontrollfunktioner.

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. Statusrapporten visar hur bolaget har arbetat med rekommendationerna från kontrollfunktionerna men även auktoriserade revisorers granskning utifrån försäkringsrörelselagen. Bolaget har i dagsläget sju öppna rekommendationer.

Bedömning ur ekonomisk dimension

Kontrollfunktionerna övervakar och utvärderar driften av bolaget inom ramen för intern kontroll. Funktionerna granskar hanteringen av risk i förhållande till riskaptiten i verksamheten, som definieras av styrelsen. Vidare granskas även utformning och effektivitet av bolagets riskhantering, regelefterlevnad, riskkontroll och styrningsprocesser. Samtliga granskningar är viktiga ur ett ekonomiskt perspektiv då de 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 förbättras. 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. Uppföljning rekommendationer från kontrollfunktionerna 2024:2

Ärendet

Styrelsen ska säkerställa att rekommendationer från bolagets kontrollfunktioner följs upp och avslutas inom rimlig tid.

För att ta del av kontrollfunktionernas rekommendationer och bolagets nuvarande rapporterade status för arbetet 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. Utöver de centrala funktionerna granskar de auktoriserade revisorerna även bolaget utifrån försäkringsrörelselagen. Detta ärende behandlar således rekommendationer från granskningar från fem granskande funktioner.

Bolaget har i dagsläget fem öppna rekommendationer. Antalet öppna rekommendationer per år för utfärdade och samt utfärdande funktion visas i Tabell 1.

Tabell 1: Antal öppna rekommendationer från resp kontrollfunktion fördelat per år för utfärdande. Siffran inom parentes anger antalet vid uppföljningen i juni 2024.

Kontrollfunktion	2021	2022	2023	2024
Regelefterlevnad				
Auktoriserade revisorer	2 (2)			2 (2)
Internrevision		0 (2)	1 (1)	
Riskhantering				
Aktuariefunktion				

Rekommendationerna behandlar följande områden:

- Informations- och kommunikationsteknik/Informationssäkerhet/IT: 3 st
- Betalningar: 2 st

Göta Lejon arbetar löpande med att åtgärda utfärdade rekommendationer. Rekommendationerna uppdateras i bolagets styrnings- och ledningssystem Stratsys minst 2 gånger per år.

Bolagets bedömning

Det är bolagets bedömning att arbetet med rekommendationerna fortskrider tillfredsställande.

Uppföljning rekommendationer från externa revisorer 2024:2

Göta Lejon

2024

Innehållsförteckning

1 Rekommendationer och åtgärder

Nedan redovisas pågående rekommendationer utfärdade av centrala funktioner och auktoriserade revisorer.

1.1 2021 - Auktoriserade revisorer - Rapport kvartal 1

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Slutdatum
Det saknas styrande dokument med tydliga roller och ansvar. EY rekommenderar att: kartlägga vilka centrala IT processer som finns inom Göta Lejon, utveckla ett ramverk för de principer och riktlinjer som ska gälla inom de centrala IT processerna samt formalisera roller och ansvar. Implementera styrande dokument inom organisationen genom information och utbildning	Röd	Genomföra följande förbättringsaktiviteter av IT-processen: Kartläggning av centrala IT-processer, utveckling av ett ramverk för de principer och riktlinjer som ska gälla inom de centrala IT-processerna, inkl formalisering av roller och ansvar, implementering av styrande dokument inom organisationen genom information och utbildning.	75% genomfört	*Hanna Svantesson*	IT-processer är kartlagda och ska läggas in i systemet för bolagets processer (2c8) Principer och riktlinjer för kontroll finns i form av behörighetskontroller och testschema Egenkontrollplanen innehåller kontroll att behörighetskontroller har utförts. Egenkontrollen utförs av bolagscontroller. Roller och ansvar fastslagna avseende behörighetskontroll i Insman. Roll och ansvar fastslagna avseende utveckling i Insman. Styrande dokument är under framtagande. Ständiga förbättringar sker i nuläget främst genom informationssäkerhetsarbetet men kommer även att förbättras genom bolagets arbete med processorientering. Rekommendationen bedöms kunna stängas under hösten 2024.	2024-09-30

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Slutdatum
Det saknas verktyg och hjälpmedel för utförande och tillsyn av IT intern kontroll EY rekommenderar bolaget att: utveckla ett RACM eller liknande verktyg för en holistisk bild av organisationens IT generella kontroller samt utveckla mallar för att underlätta kontrollutförandet samt öka kvalité och spårbarhet i dokumentation.	Röd	Framtagande av översikt av bolagets generella kontroller avseende IT samt utveckling av mallar för att underlätta kontrollutförandet. Framtagande av rutiner för att öka kvalité och spårbarhet i dokumentation.	75% genomfört	*Hanna Svantesson*	Översikt av de viktigaste kontrollerna har genomförts och är infogade i egenkontrollplan. Kontrollplanen innehåller ansvar för initiering, utförande, åtgärd samt specifikation av frekvens och dokumentation. Det kvarstår att koppla kontrollerna till IT-processens flöde. Detta kommer att utföras i bolagets arbete med processorientering. Rekommendationen bedöms kunna stängas under hösten 2024.	2024-09-30

1.2 2023 - Internrevision kvartal 1 - Informationssäkerhet

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Slutdatum
Åtgärdsplaner för fastställda GAP inom IKT-riktlinjerna 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.	Gul	Stäng samtliga GAP avseende IKT-riktlinje	75% genomfört	*Petra Willquist*	Bolaget arbetar löpande med att stänga gap. Det finns överlapp mellan detta arbete och kommande arbete med Dora-regelverket vilket innebär att bolaget behöver prioritera mellan vilka åtgärder som behöver genomföras. Slutdatum för denna rekommendation har därför flyttats fram.	2024-10-31

1.3 2024 - Auktoriserade revisorer

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Slutdatum
Framtagning av avtal som specificerar regler och villkor för hantering av koncernbankkontot, inklusive riktlinje för tillgång till medel för betalningar Under granskningen av Försäkrings AB Göta Lejons ekonomiska och administrativa rutiner har det uppmärksammats att bolaget för närvarande inte har ett eget bankkonto utan istället hanterar sina transaktioner genom ett koncernmellanhavande med moderbolaget. Detta arrangemang innebär att bolaget utför betalningar från moderbolagets koncernbankkonto. Det har dock observerats att det inte finns några formellt dokumenterade avtal eller riktlinjer som reglerar bolagets rättigheter och skyldigheter i förhållande till tillgången och användningen av detta konto, särskilt när det gäller uttag av medel för att täcka egna skulder eller andra finansiella åtaganden. Det rekommenderas därför att Försäkrings AB Göta Lejon och dess moderbolag utarbetar och formaliserar ett avtal som tydligt specificerar reglerna och villkoren för hanteringen av koncernbankkontot. Detta bör inkludera, men inte begränsas till, riktlinjer för hur och när Försäkrings AB Göta Lejon får tillgång till medel för betalningar.	N/A	Översyn av befintliga styrdokument/avtal avseende koncernkontot. Och eventuellt ta fram avtal/riktlinjer.	75% genomfört	*Björn Wennerström*	Avtalsförslag finns framtaget. Revisorerna har godkänt förslaget. Underskrifter är på gång.	2024-12-31

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar	Slutdatum
Filen avseende återförsäkringsprogrammet var inte helt uppdaterad vilket ledde till en beloppsmässigt felaktig betalning. Vi rekommenderar därför att Försäkrings AB Göta Lejon stärker sina rutiner och avstämningar av återförsäkringsfilen för att säkerställa att betalning och bokföring sker till rätt belopp. Försäkrings AB Göta Lejon har betalat fel belopp avseende en återförsäkringspremie eftersom man missat att uppdatera sin fil avseende återförsäkringsprogrammet. Först betalade bolaget för lite eftersom de betalade det som var 2022 års premie och sedan upptäcktes felet och en kompletterande betalning är gjord. Felet visar dock på bristande kvalitet i den underliggande återförsäkringsfilen över återförsäkringsprogrammet.	Gul	Förbättra rutiner och avstämningar av underlag vid betalning av återförsäkringspremie.	75% genomfört	*Björn Wennerström*	En uppdaterad rutin är på plats. Rutinen ska dokumenteras.	2024-12-31

2 Nyligen avslutade rekommendationer

Sedan föregående uppföljning (2024-05-28) har nedanstående rekommendationer avslutats.

2.1 2021 - Auktoriserade revisorer - Rapport kvartal 1

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar
Periodisk genomgång av användare med priviligierad access genomförs ej EY rekommenderar att: 1. Göta Lejon implementerar en formaliserad process för periodisk genomgång av högre behörigheter samt dokumenterar hur kontrollen ska genomföras. Kontrollen bör fokusera på genomgång av höga behörigheter på rollnivå i samtliga kritiska instanser i Göta Lejons IT-miljö. Vidare bör den periodiska genomgången av höga behörigheter ske med högre frekvens jämfört med övriga användarbehörigheter, minst halvårsvis. Genomgången bör utgå ifrån en systemgenererad lista av användare. Listan bör granskas av relevanta chefer eller ansvariga inom organisationen. Genomgången bör dokumenteras och godkännas av utförarna samt arkiveras för att säkerställa spårbarhet.	Röd	Rapport EY kvartal 1 2021 Göta Lejon implementerar en formaliserad process för periodisk genomgång av högre behörigheter samt dokumenterar hur kontrollen ska genomföras. Kontrollen bör fokusera på genomgång av höga behörigheter på rollnivå i samtliga kritiska instanser i Göta Lejons IT-miljö. Vidare bör den periodiska genomgången av höga behörigheter ske med högre frekvens jämfört med övriga användarbehörigheter, minst halvårsvis. Genomgången bör utgå ifrån en system-genererad lista av användare. Listan bör granskas av relevanta chefer eller ansvariga inom organisationen. Genomgången bör dokumenteras och godkännas av utförarna samt arkiveras för att säkerställa spårbarhet.		*Hanna Svantesson*	En formaliserad process för kontroll av behörigheter är införd och följs.

2.2 2022 - Internrevision kvartal 2 - ERSA

Rekommendationer	Kontrollfunktionens bedömning	Aktiviteter	Status	Ansvarig	Kommentar
ERSA-rapporten 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”. Risk Risk för felaktiga beräkningar om bolaget inte kan säkerställa datakvalitén i solvensberäkningarna. 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.	Gul	Utveckling av avsnittet avseende datakvalité och formalisering av en process med kontroller för att säkerställa att dataunderlaget i solvensberäkningen uppfyller kraven på datakvalité.		*Björn Wennerström*	ERSA riktlinjen har uppdaterats avseende datakvalitet. Avsnittet ”Datakvalitet” har lagts till riktlinjen. Avsnittet beskriver krav på datakvalitet och spårbarhet samt hur detta säkerställs. Avsnittet innehåller även en förteckning över datakällor till ERSAn.