Beslutsunderlag
Utfärdat 2022-05-30
Diarienummer 0057/22

Handläggare
Björn Wennerström
Telefon: 031-368 55 06
E-post: bjorn.wennerstrom@gotalejon.goteborg.se

Status rekommendationer från externa kontrollfunktionerna

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anta status för rekommendationer från externa kontrollfunktioner.

Sammanfattning

Statusrapporten visar hur bolaget har arbetat med rekommendationerna från kontrollfunktionerna. Det finns 22 stycken öppna rekommendationer.

Bedömning ur ekonomisk dimension

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

Bedömning ur ekologisk dimension

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

Bedömning ur social dimension

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

Samverkan

Ingen samverkan har genomförts.

Bilagor

1. Statusrapport rekommendationer från kontrollfunktionerna

Ärendet

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

Beskrivning av ärendet

Bolaget ska kvartalsvis genomföra granskningar av verksamheten. Enligt Försäkringsrörelselagen kap. 10 Företagsstyrning, ska kontrollfunktionerna 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.

Bolagets bedömning

Det är bolagets bedömning att arbetet med rekommendationerna fortskrider tillfredsställande. Rekommendationerna uppdateras minst 2 gånger per år.

Rekommendationer från kontrollfunktionerna - status

Göta Lejon
2022

Innehållsförteckning

1 Åtgärder

1.1 2019 Rapport kvartal 4, Internrevisionen

Rekommendationer	Status	Ansvarig	Kommentar
Rapport internrevisionen kvart 4 2019 Uppdatera FBU med ändringshistorik, framgå när expertbedömningar görs och beräkningsformler och metoder beskrivs endast på en övergripande nivå		*Björn Wennerström*	Det försäkringstekniska beräkningsunderlaget ligger hos aktuarien för uppdatering. Det mesta är klart redan förra året.

1.2 2020 Rapport Informationssäkerhet

Rekommendationer	Status	Ansvarig	Kommentar
Rapport informationssäkerhet 2020 Företaget bedöms ha relevanta organisatoriska och tekniska förutsättningar för ett strukturerat arbete med informationssäkerhet samt relaterade styrdokument och processdokumentation. Det saknas styrande dokument inom området för incidenthantering och kontinuitetshantering. Med hänsyn till företagets storlek samt medvetenhet inom området är bedömningen att avsaknaden av dessa styrdokument får en mindre inverkan på företagets riskhantering		*Petra Willquist*	iFACTS har skapat guidelines för incidenthantering och användarhantering. Dock har bolaget ej fått dessa ännu.
Rapport informationssäkerhet 2020 Det saknas en formell process för en regelbunden hantering och genomförande av riskanalyser avseende INSMAN. Företaget föreslås formalisera befintliga processer för riskanalysen för att säkerställa en riskbaserad strategi för informationssäkerhetsbeaktanden. Med fördel kan resultaten av genomförda penetrationstester (se också avsnitt Drifts- och kommunikationssäkerhet inkl. integrationshantering) byggas in i processen för riskanalysen. iFACTS föreslås också införa en formell och dokumenterad plan för kontinuitetshantering.		*Hanna Svantesson, Petra Willquist*	Ifacts har presenterat en ny process för riskanalys. Göta Lejon ska stämma av status på rekommendationen.
Rapport informationssäkerhet 2020 Styrningen för åtkomst bygger på ett strikt system av åtskilda och begränsade rättigheter. Det rekommenderas ett styrande dokument för ramverket för åtkomsthantering som formaliserar Det är oklart om det finns en formell processen för tilldelning, förändringar och borttag av användarkonton inom iFACTS.		*Hanna Svantesson*	Rapporten bedömer att inga allvarliga brister som kräver åtgärd har framkommit, riskindex är Tillfredsställande. Rekommendationen är en förbättringsmöjlighet som kan fångas upp leverantörsuppföljning längre fram.

Rekommendationer	Status	Ansvarig	Kommentar
Rapport informationssäkerhet 2020 Det saknas en underliggande riskanalys som stödjer val av driftlösning, både vad avser driften av INSMAN och driften av de interna systemen. Detta kan medföra att säkerhetsaspekter och säkerhetskopiering inte sker i enlighet med de risker som förekommer. Dock bör tilläggas att den valda lösningen för driften av INSMAN också påverkas av kundernas val så som backupfrekvens		*Hanna Svantesson*	Informationssäkerhetsarbetet ska fånga upp risker för och konsekvenser av dataförlust. Baserat på resultat från detta kan tolerans av dataförlust definieras och kommuniceras till leverantörer. Därefter kan eventuella behov för ändring och uppföljning diskuteras.
Rapport informationssäkerhet 2020 För INSMAN finns ett etablerat och strukturerat sätt att hantera incidenter i form av fel under utvecklings- och uppgraderingsprocessen. Däremot saknas en överordnad formell process för incidenthantering inom iFACTS som beskriver händelseförloppet vid inträffande av en incident som inte är kopplad till kundens datamiljö. iFACTS föreslås formalisera befintliga processer för informationssäkerhetsincidenter.		*Hanna Svantesson*	Förbättringsmöjlighet hos Ifacts avseende incidenthantering. Detta fångas upp i kommande leverantörsuppföljning.

1.3 2020 Rapport Aktuarien

Rekommendationer	Status	Ansvarig	Kommentar
Rapport aktuarien 2020 Prioritering av dataframtagandet från det nya skadesystemet så att störst möjlig kvalité i analysdata säkerställs. Möjlighet för att särskilja noll-skador från vanliga skador när antalet skador rapportera bör finnas.		*Björn Wennerström*	En aktuarierapport finns nu på plats.

1.4 2021 Rapport kvartal 1, Internrevisionen

Rekommendationer	Status	Ansvarig	Kommentar
Rapport internrevisionen kvartal 1 2021 Process för hantering av kontinuitetsplan - Vi rekommenderar Bolaget att årligen granska och uppdatera kontinuitetsplanen genom att uppdateringen diskuteras och behandlas i ledningen/Business Continuity Management Team istället för att utkastet förbereds av bolagsjuristen.		*Björn Wennerström*	Uppdatering pågår. Ska vara klart före sommaren.
Rapport internrevisionen kvartal 1 2021 Testning av kontinuitetsplan - Vi rekommenderar Bolaget att årligen testa kontinuitetsplanen genom att till exempel riskkontrollfunktionen eller annan på Bolaget sätter upp ett scenario som gör att kontinuitetsplanen måste användas.		*Björn Wennerström*	På gång. Testning av bortfall av Insman gjordes i dec 2021. Ny testning av ett annat område kommer att göras under året.

Rekommendationer	Status	Ansvarig	Kommentar
Rapport internrevisionen kvartal 1 2021 Utbildning för anställda om kontinuitetsplanen - Vi rekommenderar Bolaget att årligen ha en kortare genomgång av kontinuitetsplanen för de anställda.		*Björn Wennerström*	Bolaget ska utbildas i kontinuitetsplan och krisplan under 2022.

1.5 2021 Rapport kvartal 1, Auktoriserade revisorer (EY)

Rekommendationer	Status	Ansvarig	Kommentar
Rapport EY kvartal 1 2021 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		*Hanna Svantesson*	Arbetet fortgår som en del av det större informationssäkerhetsarbetet. Kartläggning av processer är klar, genomgång av styrdokument och riktlinjer för processerna pågår.
Rapport EY kvartal 1 2021 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.		*Hanna Svantesson*	Egenkontrollplan finns. Efter genomgång av IT-processer skall egenkontrollplan ses över och eventuellt utvecklas med fler kontroller. Kopplar till observation #1. Vi kan börja med processer, identifiera viktiga kontroller/uppföljningar etc som behöver göras. Specificera ansvar (initiering, utförande, åtgärd) , frekvens, dokumentation.
Rapport EY kvartal 1 2021 Formalisera och dokumentera en process för tillägg av ny behörighet i Insman. Processen bör behandla centrala områden som: spårbarhet i beställning, godkännande av behörighet och analys av "giftiga kombinationer av behörigheter.		*Hanna Svantesson*	Rutin för beställning och registrering av behörighet dokumenterad och finns sparad i verksamhetshandboken. Klar.
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*	220118: Arbete pågår med att ta fram tabell över behörighetsgrupper, vem som får beställa samt godkänna respektive grupp. Bedömning över vad som anses vara "hög behörighet" ska göras. Instruktioner ska skrivas över hur beställning/godkännande görs. 220530: Kontroll av behörigheter genomförd av ansvarig för respektive behörighetsgrupp. Högre behörigheter granskas också av VD. Rutin ska dokumenteras och sparas i verksamhetshandboken.

Rekommendationer	Status	Ansvarig	Kommentar
Rapport EY kvartal 1 2021 Göta Lejon implementerar en formaliserad process för periodisk genomgång samt dokumenterar hur kontrollen ska genomföras. Processen bör genomgå samtliga behörigheter och ta hänsyn till både access och organisationsnivå, dvs. inte endast verifiera om personer fortfarande har en giltig mailadress hos försäkringstagaren. Periodisk genomgång av alla användarbehörigheter bör genomföras minst årligen. Genomgången bör utgå ifrån en system-genererad lista av användare. Listan bör granskas av relevanta chefer eller ansvariga inom organisationen, alternativt genom utdrag från HR/ekonomi på anställda tillsammans med grupptillhörighet. Genomgången bör dokumenteras och godkännas av utförarna samt arkiveras för att säkerställa spårbarhet.		*Hanna Svantesson*	220118: Arbete pågår med att ta fram tabell över behörighetsgrupper, vem som får beställa samt godkänna respektive grupp. Bedömning över vad som anses vara "hög behörighet" ska göras. Instruktioner ska skrivas över hur beställning/godkännande görs. 220530: Kontroll av behörigheter genomförd av ansvarig för respektive behörighetsgrupp. Högre behörigheter granskas också av VD. Rutin ska dokumenteras och sparas i verksamhetshandboken.
Rapport EY kvartal 1 2021 Göta Lejon implementerar en formaliserad gemensam kontroll för att kontinuerligt följa upp på IT intern kontroll hos leverantörer av utlagd IT-verksamhet. Vid eventuella brister bör dessa följas upp och säkerställas att de hanteras på ett tillfredställande sätt hos leverantören		*Hanna Svantesson*	220118: Påbörjat en översyn av vilka leverantörer som bör följas upp samt vilka områden uppföljning bör omfatta. Till grund för detta ligger GAP-analys IKT samt informationssäkerhetsarbetet generellt. 220530: Genomgång enligt checklista för IKT har genomförts med de två leverantörer som ansågs vara av vikt. Klar.

1.6 2021 Rapport kvartal 2, Regelefterlevnad

Rekommendationer	Status	Ansvarig	Kommentar
Rapport regelefterlevnad kvartal 2 2021 Rekommendation att hålla minst årliga avstämningar med samtliga tjänsteleverantörer samt dokumentera dessa avstämningar.		*Katrin Gundersen, Hanna Svantesson, Björn Wennerström, Cecilia Jansson*	Redovisning kommer att ske på styrelsemötet i september 2022
Rapport regeleftrlevnad kvartal 2 2021 Vidare rekommenderas att det minst årligen genomförs en övergripande analys av den utlagda verksamheten i syfte att kunna bedöma behovet av utlagd verksamhet och fånga upp eventuella brister hos tjänsteleverantörer. Detta bedöms nödvändigt för att bibehålla en god intern styrning och kontroll.		*Katrin Gundersen, Hanna Svantesson, Björn Wennerström, Cecilia Jansson*	Kommer att göras under året.
Rapport regelefterlevnad kvartal 2 2021 Rekommendation att Bolaget ser över Bolagets kontinuitetsplan under året för att säkerställa att där anges uppdaterade och relevanta uppgifter och kontaktuppgifter.petr		*Björn Wennerström*	Uppdatering pågår. Ska vara klart före sommaren.
Rapport regelefterlevnad kvartal 2 2021 Bolaget har ett pågående hållbarhetsarbete och tillsammans med riskfunktionen ska Bolaget fastställa strategi för hållbarhetsmål. Funktionen för regelefterlevnad avser att följa upp detta under nästkommande kvartal.		*Björn Wennerström*	Aktiviteten har inte startat ännu.

1.7 2021 Rapport regelefterlevnad kvartal 3

Rekommendationer	Status	Ansvarig	Kommentar
Rapport regelefterlevnad kvartal 3 2021 De interna riktlinjerna bedöms hålla en god miniminivå, dock behöver deninterna riktlinjen ses över mot bakgrund av den GAP-analys som genomförts av Transcendent Group där en rad brister identifierats.		*Petra Willquist*	Löpande arbete med informationssäkerhet pågår. Brister identifierade i GAP-analyser behandlas efter prio och i takt med att informationssäkerhetsarbetet utvecklas.
Rapport regelefterlevnad kvartal 3 2021 Rekommendation att Bolaget ser över Bolagets kontinuitetsplan för att säkerställa att där anges uppdaterade och relevanta uppgifter och kontaktuppgifter.Utöver ovan har KPMG i sin internrevisionsrapport 2021:1 rekommenderat att Bolaget förtydligar vem som har ansvar för att granska, uppdatera och testa kontinuitetsplanen.		*Björn Wennerström*	Översyn av kontinuitetsplanen pågår. Ska vara klart före sommaren. Bolagets ekonomichef har ansvar för uppdatering samt testning av denna.