Tjänsteutlåtande
Utfärdat 2025-11-06
Ärendenummer FGL-2025-00123

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

Styrande dokument för årligt beslut i styrelse 2025

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

- Styrelsen antar Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll
- Styrelsen antar Försäkrings AB Göta Lejons riktlinje för säkerhet

Sammanfattning

Bolagets styrelse ska minst årligen anta de styrande dokument och riktlinjer som finns i verksamheten och är kopplade till regelverk som rör försäkringsrörelsen.

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.

Bilagor som ingår i beslutsunderlaget

1. Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll
2. Försäkrings AB Göta Lejons riktlinje för säkerhet

Beskrivning av ärendet

Bolagets styrelse ska minst årligen anta de styrande dokument och riktlinjer som finns i verksamheten och är kopplade till regelverk som rör försäkringsrörelsen.

Solvens II-regelverket och kopplade lagar och förordningar ställer krav på att försäkringsföretag har vissa styrdokument och riktlinjer för att säkerställa att bolaget styrs på ett sunt och ansvarsfullt sätt, att bolaget fortlöpande kan identifiera, värdera, övervaka, hantera och rapportera risker samt kan uppnå god intern styrning och kontroll. Styrelsen har det yttersta ansvaret för att det finns effektiva styrmedel och riktlinjer och ansvarar för att årligen se över och fastställa dessa för att säkerställa att de är i linje med gällande Solvens II-regelverk (försäkringsområdet) och praxis. Vidare ställer EU-förordningen för enhetlig reglering av digital operativ motståndskraft för finansiella entiteter, vanligen benämnd DORA (Digital Operational Resilience Act), krav på företag inom den finansiella sektorn. Bolaget ska ha robusta strategier och åtgärder för att hantera och motverka risker relaterade till digital operativ motståndskraft.

I **Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll** har nedanstående ändringar utförts.

I avsnitten 2.1 och 3.2 har den nedre gränsen för solvenskvoten ändrats från 150 % till 175 % och den övre gränsen från 250 % till 275 %.

I avsnitt 7. Fastställande, utvärdering och efterlevnad har följande tillägg gjorts med anledning av krav i Dora på översyn av IKT-riskhanteringsramen: *Riskhanteringsramen ska fortlöpande förbättras baserat på erfarenheter från genomförande av riskhanteringsarbete och övervakning. Översyn ska ske vid uppkomst av allvarliga IKT-relaterade incidenter, tillsynsinstruktioner eller slutsatser från relevanta testnings- eller revisionsprocesser för digital operativ motståndskraft.*

I **Försäkrings AB Göta Lejons riktlinje för säkerhet** har nedanstående ändringar utförts.

I avsnittet Leverantörer har ett tillägg gjorts så att det framgår att både riktlinje för utlagd verksamhet och rutin för utkontraktering av IKT-tjänster ska följas. Tillägget har gjorts med anledning av krav i Dora. *Vid utkontraktering av IKT-tjänster, upprättande av utlagd verksamhet och/eller uppföljning av någon av dessa tjänster ska bolagets riktlinje för utlagd verksamhet samt rutin för utkontraktering av IKT-tjänster följas.*

I avsnittet Fastställande och efterlevnad har följande tillägg gjorts med anledning av krav i Dora på översyn av IKT-riskhanteringsramen: *Riktlinjen och dess tillämpning ska ses över vid uppkomst av allvarliga IKT-relaterade incidenter, tillsynsinstruktioner eller slutsatser från relevanta testnings- eller revisionsprocesser för digital operativ motståndskraft.*

Bolagets bedömning

Det är bolagets bedömning att de styrande dokumenten överensstämmer med bolagets syn på hur verksamheten ska bedrivas. Styrelsen föreslås anta de styrande dokumenten.

Petra Willquist	Anders Jonasson
Bolagscontroller	VD

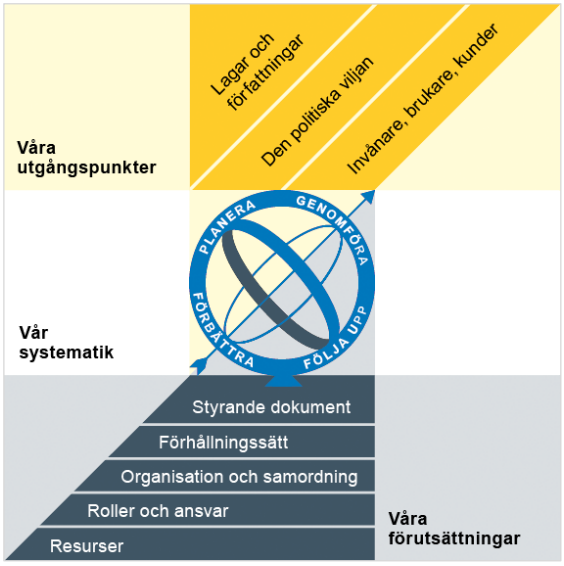
Göteborgs Stad

Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll

Reglerande styrande dokument

- Policy
- ► **Riktlinje**
- Regel
- Anvisning
- Rutin
- Instruktion

Göteborgs Stads styrsystem



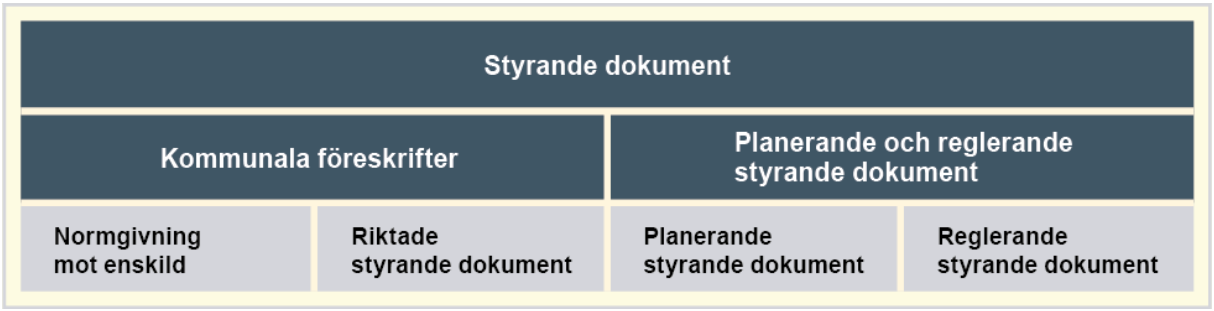
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Styrelse	Försäkrings AB Göta Lejon	FGL-2025-00123	

Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tillsvidare	2025-11-10	Bolagscontroller

Bilagor:

-

Innehåll

Inledning

Syftet med denna riktlinje

Syftet med denna riktlinje är att fastställa Försäkrings AB Göta Lejons avsikt och krav inom risktagande samt beskriva bolagets riskhantering och interna styrning och kontroll.

Vem omfattas av riktlinjen

Denna riktlinje gäller tills vidare för Försäkrings AB Göta Lejon samt för riskhanteringsfunktionen för Försäkrings AB Göta Lejon.

Lagbestämmelser

Denna riktlinje har upprättats i enlighet med:

- Försäkringsrörelselagen 10 kap 2, 6–7 §§
- FFFS 2015:8 9 kap 1§
- EIOPA-BoS-14/253 Riktlinje 17–19.
- Dora-förordningen (EU) 2022/2554

Koppling till andra styrande dokument

Göteborgs Stads riktlinje för finansverksamheten
Göteborgs Stads riktlinje för styrning uppföljning och kontroll
Försäkrings AB Göta Lejons finansiella anvisning
Försäkrings AB Göta Lejons försäkringstekniska riktlinjer
Försäkrings AB Göta Lejons riktlinje för företagsstyrning
Försäkrings AB Göra Lejons riktlinje för hantering av intressekonflikter
Försäkrings AB Göra Lejons riktlinje för lämplighetsprövning
Försäkrings AB Göta Lejons riktlinje för regelefterlevnad
Försäkrings AB Göta Lejons riktlinje för reservsättning
Försäkrings AB Göta Lejons riktlinje för teckningsrisker
Försäkrings AV Göta Lejons riktlinje för utlagd verksamhet
Försäkrings AB Göta Lejons riktlinje för återförsäkring
Försäkrings AB Göta Lejons riktlinje för aktuariefunktionen
Försäkrings AB Göta Lejons riktlinje för regelefterlevnad
Försäkrings AB Göta Lejons riktlinje för egen risk- och solvensanalys
Försäkrings AB Göta Lejons riktlinje för internrevision

Riktlinje

Försäkrings AB Göta Lejons verksamhet är förenad med risktagande vilket medför att bolaget ska arbeta strukturerat med riskhantering och regelefterlevnad. Hanteringen av risk ska vara en naturlig del i den dagliga verksamheten på alla nivåer och underlätta för verksamheten att nå uppsatta mål och leva upp till åtaganden mot försäkringstagarna.

Genom en väl fungerande riskhanteringsprocess och intern kontroll ska bolaget vid varje tillfälle vara i stånd att identifiera, värdera, övervaka, hantera och rapportera de risker som kan hindra bolaget från att uppnå sina verksamhetsmål eller efterleva gällande lagar och regler.

Med intern kontroll avses den struktur av riktlinjer, processer, rutiner och organisation som utformats för att bidra till en ändamålsenlig och effektiv verksamhet, tillförlitlig finansiell rapportering samt efterlevnad av tillämpliga lagar och förordningar.

Riskhantering är en central del av den interna kontrollen.

Med riskhantering avses de samordnande aktiviteter som genomförs för identifiering, analys, utvärdering, behandling, övervakning och granskning av risker.

1. Ansvar

Styrelsen ska fastställa avsikt och krav inom risktagande. Risknivån bestäms årligen av styrelsen och uttrycks genom att ange ett intervall för bolagets risktolerans.

För att säkerställa ändamålsenlig riskhantering och intern kontroll är ansvarsfördelningen mellan olika typer funktioner baserat på principen om tre försvarslinjer. Modellen skiljer mellan den operativa verksamheten (första linjen), funktioner för övervakning och kontroll (andra linjen) och funktioner för oberoende granskning (tredje linjen).

Bolaget ska upprätthålla följande fyra centrala funktioner. Ansvar och befogenhet för respektive funktion ska fastslås i särskild riktlinje.

- Aktuarie
- Internrevision
- Riskhantering
- Regelefterlevnad

Alla medarbetare och outsourcade funktioner ansvarar för att denna riktlinje följs. Chefer i organisationen säkerställer att riktlinje efterlevs och att kunskap om innehållet finns inom avdelningen. Ansvarig för att granska verksamhetens efterlevnad är funktionen för regelefterlevnad.

Styrelsen har den centrala rollen för företagsstyrningssystemet och är ytterst ansvarig för bolaget och hur verksamheten bedrivs. Till sin hjälp har styrelsen särskilt utsett en riskhanteringsfunktion inkluderande en oberoende riskkontrollfunktion. Detaljerad information finns i bolagets interna riktlinjer.

2. Riskhanteringsstrategi

Risktagande är nödvändigt för att uppnå verksamhetens mål och ska ske utifrån medvetna beslut. Bolaget ska arbeta strukturerat och disciplinerat med riskhantering för att skapa möjlighet till medvetna beslut, understödja strategiska mål samt undvika förluster. I alla beslut ska hänsyn tas till risk, säkerhet och regelefterlevnad. Bolaget är verksamt på en reglerad marknad varvid regelöverträdelser inte är acceptabla. Regelefterlevnadsrisker är inte föremål för medvetet risktagande.

Målet med Göta Lejons riskhanteringsstrategi är att öka sannolikheten för att bolaget ska uppnå de strategiska (verksamhetsnära) målen. Effekter av oönskade och oväntade händelser ska minimeras. Detta innebär att bolagets riskhantering ska:

- definiera en acceptabel risknivå och eventuell risktolerans för bolaget
- identifiera risker som utgör ett hot mot att bolagets strategiska mål uppnås
- beakta långsiktiga hållbarhetsmål och principer, så att bolaget säkerställer att en ansvarsfull och hållbar affärspraxis upprätthålls
- se till att resultaten för riskhanteringen implementeras i den dagliga verksamheten
- kontrollera, definiera och vidta lämpliga åtgärder för att kontrollera bolagets riskexponering.
- identifiera, definiera och regelbundet utvärdera metoder för att mäta risk så att risker kan bevakas effektivt.
- kontinuerligt revidera och utvärdera bolagets riskregister
- ta fram egen risk- och solvensrapport (ERSA-rapport)

2.1 Övergripande risktolerans och kapitalmål

Bolagets risknivå bestäms årligen av styrelsen och uttrycks genom att ange ett intervall för bolagets risktolerans. Risktoleransen i sin tur uttrycks som funktion av bolagets solvenskvot beräknad enligt standardformeln för Solvens 2.

Risktoleransens nedre gräns satts till 175 % och den övre gränsen till 275 % av solvenskvoten. Om solvenskvoten befinner sig inom målintervallet ska bolaget agera för att bibehålla kvoten därinom. Om bolagets solvenskvot däremot skulle avvika från målnivån, skall åtgärder utformas och implementeras. På en övergripande nivå skall följande två alternativ övervägas:

1. Förändra storleken på och/eller sammansättningen av bolagets kapitalbas så att denna uppfyller bolagets kapitalbehov
2. Förändra bolagets risktagande och därmed även dess kapitalbehov.

3. Risker i verksamheten

Göta Lejon har identifierat risker i riskkategorier kopplat till bolagets verksamhet enligt nedanstående sammanställning. Till dessa riskkategorier finns specifika rutiner för kontroll och övervakning. Till denna riktlinje finns därför underliggande riktlinjer som mera detaljerat beskriver vad som ska göras för att de övergripande avsikterna i detta dokument ska uppnås.

- Försäkringsrisker i form av underwritingrisk (premierisk)- och reservsättningsrisker
- Återförsäkringsrisker och andra riskreducerande metoder
- Investeringsrisker (marknadsrisker)
- Likviditets- och koncentrationsrisker
- Matchningsrisker
- Operationella risker såsom säkerhetsrisker (t ex informationssäkerhetsrisker och informations- och kommunikationstekniska (IKT)-risker) samt regelefterlevnadsrisker (inkl förekomst av oegentligheter)
- Strategiska risker

3.1 Risknivå och toleranser

Risknivån är ett mått på den risk som bolaget är berett att acceptera för att uppnå de strategiska målen. Risknivån ska:

- beakta både kvalitativa och kvantitativa aspekter
- vara en länk mellan bolagets strategiska mål och bolagets riskhantering
- vara tydligt uttryckt och kunna integreras till vardagliga affärsbeslut och processer

För att definiera risknivån används följande process med fem steg.

Steg 1: Övergripande risknivå – solvenskvot.
En angiven högsta risknivå som bolaget är villigt att acceptera för att uppnå sina strategiska mål.

Steg 2 Risknivå per riskkategori
Ett uttryck för den accepterade risknivå som bolaget är villigt att acceptera för varje enskild riskkategori. Respektive risknivå ska ligga i linje med den risknivå som definierats i steg 1.

Steg 3 Nyckelvariabler
En lista med nyckelvariabler som används för att bevaka varje risknivå enligt definitionen i steg 2.

Steg 4 Gränser
De definierade och exakta gränser, kontroller och/eller tidiga varningssignaler som gäller för varje nyckelvariabel, så att den dagliga affärsverksamheten kan bedrivas enligt den fastställda risknivån för varje riskkategori.

Steg 5 Tolerans för varje gräns
Beslut om högsta acceptabla avvikelse för varje gräns för varje enskild nyckelvariabel.

3.2 Sammanställning risknivåer

I nedanstående sammanställning redovisas högsta risknivå samt risknivåer per riskkategori tillsammans med tillhörande nyckelvariabler, gränser och eventuella toleranser.

Försäkrings AB Göta Lejon			
Alltid ha en solvenskvot mellan 175 % och 275%.			
Riskkategori: Försäkringsrisker (Underwriting/premiesättning och reservsättning)			
Risknivå	Nyckelvariabler	Operationella gränser	Tolerans
Säkerställa kapitalet i kapitalbasen	Maximalt självbehåll per försäkringsklass	Fakultativ återförsäkring av egendomsförsäkringarna skall tecknas så att de begränsar Göta Lejons åtagande till 20 Mkr per skada och 85 Mkr per år. Fakultativ återförsäkring av ansvarsförsäkringarna skall tecknas så att de begränsar Göta Lejons åtagande till 10 Mkr per skada och 30 Mkr per år för allmänt ansvar, 10 Mkr per skada och 15 Mkr per år för järnvägsansvar och 10 Mkr per skada och 15 Mkr per år för trafikansvar. Fakultativ återförsäkring av förmögenhetsbrottsförsäkringen skall tecknas så att de begränsar Göta Lejons åtagande till 10 Mkr per skada. Fakultativ återförsäkring av kaskoförsäkringarna skall tecknas så att de begränsar Göta Lejons åtagande till 10 Mkr.	Styrelsen kan besluta om en högre riskexponering om bolagets solvenskvot så tillåter.
	Kapitalbasen	Bolagets kapitalbas får utgöras av eget kapital, aktieägartillskott, balanserad vinst samt säkerhetsreserv.	Om en kapitalbaspost behöver bytas ut på grund av ändringar i bolagets verksamhet eller ändringar i regelverket skall detta ske på ett kontrollerat sätt och efter beslut av styrelsen.
	Försäkringstekniska avsättningar	Principer avseende försäkringstekniska avsättningar beskrivs utförligt enligt Försäkringstekniska riktlinjer. Avsättningar för oreglerade skador görs av professionella skadereglerare. Avsättning för skaderegleringskostnader görs av professionella skadereglerare. Avsättning för ej intjänade premier sker pro rata temporis Beräkning av den bästa skattningen (best estimate) sker i enlighet med gällande försäkringstekniska riktlinje.	Ingen avvikelse
Riskkategori: Återförsäkringsrisker och andra riskreducerande tekniker			
Risknivå	Mätvariabler	Operationella gränser	Tolerans
Återförsäkring ska bidra i bolagets leverans på uppdrag	Rating	Göta Lejon skall endast köpa extern återförsäkring från återförsäkrare som enligt Standard and Poor's (eller annan likvärdig bedömare) har ansetts ha en kreditvärdighet motsvarande A- eller bättre eller motsvarande ekonomisk ställning	Återförsäkring får placeras hos försäkringsgivare med lägre rating endast efter godkännande av styrelsen.

Riskkategori: Investeringsrisker			
Risknivå	Mätvariabler	Operationella gränser	Tolerans
Minimera risken för värdeminskning på tillgångar	Typ av investering och allokering	Försäkrings AB Göta Lejon ska placera alla likvida tillgångar hos koncernbanken i Göteborgs Stad.	Ingen avvikelse
Riskkategori: Likviditets- och koncentrationsrisker			
Risknivå	Mätvariabler	Operationella gränser	Tolerans
Minimera förluster pga. dålig likviditet	Likviditet	Det skall alltid finnas likvida tillgångar för att täcka kostnader som bolaget har för att driva verksamheten kommande 2 månader vilket motsvarar 20 Mkr.	Enligt reverstid. Kommunkonto: ingen avvikelse
	Placeringstyp	Tillgångarna som används för skuldtäckning skall investeras i revers. Övriga medel skall som regel placeras på kommunkonto.	Skuldtäckning 125% eller enligt styrelsebeslut.
Riskkategori: Matchningsrisker			
Risknivå	Mätvariabler	Operationella gränser	Tolerans
Minimera förluster på grund av bristfällig matchning mellan tillgångar och skulder	Löptid på tillgångar	Löptiden på tillgångar ska vara kortare än löptiden av försäkringstekniska avsättningar.	Ingen avvikelse.
Riskkategori: Operationella risker			
Risknivå	Mätvariabler	Operationella gränser	Tolerans
Minimera förluster pga. otillräcklig intern styrning och kontroll Minimera förluster pga. operationella risker	Ledningsprövning	Ledningsprövning skall göras i linje med Finansinspektionens instruktioner	Ingen avvikelse
	Avbrott i dagliga verksamheten	Enligt kontinuitetsplanen	Ingen avvikelse
	Förekomst av oegentligheter eller bedrägerier/ Penningtvätt	Ingen förekomst tolereras	Ingen avvikelse
	Sanktioner från Finansinspektioner	Bolaget ska uppfylla samtliga minimikrav. Myndighetssanktioner accepteras ej	Mindre sanktioner orsakade av den mänskliga faktorn kan tolereras. Skall alltid leda till översyn av befintliga rutiner och processer för att förhindra framtida sanktioner
	Säkerhetsrisker	Enligt strategi i kontinuitetsplan Enligt strategi digital operativ motståndskraft i kontinuitetsplan Bolaget ska uppfylla samtliga efterlevnadskrav. Myndighetssanktioner accepteras ej	Mindre sanktioner orsakade av den mänskliga faktorn kan tolereras men ska alltid leda till översyn av befintliga rutiner och processer för att förhindra framtida sanktioner
Riskkategori: Strategiska risker			
Risknivå	Mätvariabler	Operationella gränser	Tolerans
Minimera risk för att bolaget inte arbetar i enlighet med strategiska mål	KPIer enligt strategikarta	Enligt KPI i strategikarta	Enligt KPI i strategikarta

3.3 Beskrivning av riskkategorier

I följande tabeller ges en beskrivning av samtliga riskkategorier tillsammans med nyckelvariabler, kontroller, beskrivning av riskreducering samt hur risken regleras.

<table>
<tr><th>Riskkategori</th><th colspan="2">Försäkringsrisker</th></tr>
<tr><td>Underkategori</td><td colspan="2">Underwritingrisk (premierisk)</td></tr>
<tr><td colspan="3">Beskrivning</td></tr>
<tr><td colspan="3">Risken att skadekostnaderna blir högre än förväntat. Göta Lejons huvudsakliga risker återfinns inom frekvensskador eller enskilda stora skador; alltså kan försäkringsrisken delas upp i risken att antalet skador blir större än förväntat eller att skadebeloppen för enskilda skador blir högre än beräknat.</td></tr>
<tr><td>Kvantifierbar risk?</td><td>Nyckelvariabler</td><td>Kontroller</td></tr>
<tr><td>Ja</td><td>• Maximalt självbehåll per försäkringsklass
• Försäkringstekniska avsättningar</td><td>• Kontroll av maximalt självbehåll per försäkringsprodukt.
• Bedömd maximal skada
• Bedömning av likviditetens och återförsäkringskapacitetens tillräcklighet och risknivå</td></tr>
<tr><td>Riskreducering vidtas om:</td><td colspan="2">• de toleransnivåer som definierats i den acceptabla risknivån har överskridits
• solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen
• en händelse inträffar som ger avsevärda konsekvenser för den risk som bolaget kan exponeras för</td></tr>
<tr><td>Riskreducering</td><td colspan="2">Identifieras i:

• Riskregister
• Rapport från centrala funktioner
• ERSA

Motåtgärder för att reducera risken ska definieras så långt som möjligt.</td></tr>
<tr><td>Risken regleras i:</td><td colspan="2">• Försäkrings AB Göta Lejons försäkringstekniska riktlinjer
• Försäkrings AB Göta Lejons riktlinje för återförsäkring
• Försäkrings AB Göta Lejons riktlinje för teckningsrisker
• Bolagsordning

Försäkringsengagemang där återförsäkring krävs får inte slutgiltigt accepteras förrän återförsäkringsavtäckning kan anses vara säkerställd.</td></tr>
</table>

Riskkategori	**Försäkringsrisker**	
Underkategori	Reservsättningsrisk	
Beskrivning		
Risker för att Göta Lejons ansvar undervärderas genom att inte tillräcklig höjd tas för inträffade skador.		
Kvantifierbar risk?	Nyckelvariabler	Kontroller
Ja	• Tydliga principer för försäkringstekniska avsättningar, som återfinns i riktlinje för reservsättning.	• Skadechef genomför kvartalsvisa genomgångar med samtliga skaderegleringsbolag • Aktuarien beräknar avsättning för okända skador (IBNR) • Kontroll av IBNR sker årligen av auktoriserade revisorer
Riskreducering vidtas om:	• de toleransnivåer som definierats i den acceptabla risknivån har överskridits • solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen • en händelse inträffar som ger avsevärda konsekvenser för den risk som bolaget kan exponeras för	
Riskreducering	Identifieras i: • Riskregister • Rapport från centrala funktioner • ERSA Motåtgärder för att reducera risken ska definieras så långt som möjligt	
Risken regleras i:	• Försäkrings AB Göta Lejons riktlinje för reservsättning • Beslutsordning och befogenheter	

Riskkategori	**Återförsäkring och andra riskreducerande metoder**
Beskrivning	
Oförutsedda återförsäkringsrisker kan uppstå om omfattningen av Göta Lejon återförsäkringsprogram inte är heltäckande eller om återförsäkringsprogrammet inte omfattar alla risker eller om återförsäkringsbolagen inte kan uppfylla sina åtaganden gentemot bolaget.	

Kvantifierbar risk?	Nyckelvariabler	Kontroller
Ja	• Rating av Göta Lejons återförsäkringsbolag • Självbehållsnivåer beslutade av styrelsen	• Följa upp Göta Lejon återförsäkringsbolag regelbundet avseende rating. • Se till att bolaget håller sig till de självbehållsnivåer som är bestämda av styrelsen • Följa utvecklingen på försäkringsmarknaden avseende premierater och aktuell tillgång av återförsäkringskapacitet. • Följa Göta Lejon återförsäkringsstrategi som framgår av bolagets försäkringstekniska riktlinjer och/eller Teckningsinstruktioner.
Riskreducering vidtas om:	• de toleransnivåer som definierats i den acceptabla risknivån har överskridits • solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen • en händelse inträffar som ger avsevärda konsekvenser för den risk som bolaget kan exponeras för.	
Riskreducering	Lämpliga motåtgärder för att reducera risken så att den faller inom gränser för vad bolaget kan acceptera ska definieras så långt som möjligt. På styrelsemöte i januari presenteras ett återförsäkringsprogram av vd som antas av styrelsen. Kontroll av kreditvärdigheten ska ske löpande under avtalsperioden, dock åtminstone en gång per kalenderkvartal. Om återförsäkrare under avtalstiden hamnar under accepterad kreditvärdighet görs omedelbart en riskanalys och åtgärder vidtas	
Risken regleras i:	• Försäkringstekniska riktlinjer • Riktlinje för återförsäkring • Riktlinje för teckningsrisker • Riskregister • ERSA-rapport	

<table>
<tr><th>Riskkategori</th><th colspan="2">Investeringsrisk</th></tr>
<tr><td colspan="3">Beskrivning</td></tr>
<tr><td colspan="3">Investeringsrisken är den risk för förlust som uppstår genom negativa förändringar och svängningar i marknadspriser på investeringar och tillgångar. Denna risk är mycket begränsad då bolaget placerar sitt kapital på bankkonto tillhörande Göteborgs kommun samt reverser utställda mot Göteborgs kommun. Risken omfattar

• Ränterisk: förluster som uppstår på grund av negativa ränteförändringar.
• Kreditrisk: förluster på grund av att en låntagare går i konkurs.</td></tr>
<tr><td>Kvantifierbar risk?</td><td>Nyckelvariabler</td><td>Kontroller</td></tr>
<tr><td>Ja</td><td>• Tillåtna investeringar och riskspridning, enligt bolagets finansiella anvisning.</td><td>• De försäkringstekniska avsättningarna (FTA) registerförs och kontroller görs att de medel som används för täckande av FTA är registrerade i Göta Lejons namn och följer bolagets rutin för förmånsrättsregister.
• De tillgångar som inte används för att täcka FTA placeras på kommunkontot.

Ekonomichef ansvarar för skuldtäckning av FTA samt förmånsrättsregistret.</td></tr>
<tr><td>Riskreducering vidtas om:</td><td colspan="2">• de toleransnivåer som definierats i den acceptabla risknivån har överskridits.
• en händelse inträffar som ger avsevärda konsekvenser för den risk som bolaget kan exponeras för.</td></tr>
<tr><td>Riskreducering</td><td colspan="2">Motåtgärder för att reducera risken ska definieras så långt som möjligt</td></tr>
<tr><td>Risken regleras i:</td><td colspan="2">• Finansiell anvisning
• Rutin för förmånsrättsregister
• Göteborgs stads riktlinje för finansverksamheten
• Riktlinje för värdering avsolvensbalansräkning samt bolagets kapitalbasmedel</td></tr>
</table>

Riskkategori	Likviditets- och koncentrationsrisker	
Beskrivning		
Likviditetsrisk är risken att Göta Lejon, även vid solvens, inte kan realisera placeringar och/eller få fram tillräckliga medel för att uppfylla sina finansiella åtaganden när de förfaller. Koncentrationsrisk omfattar risken för ytterligare förluster för bolaget på grund av antingen bristande spridning i tillgångsportföljen (till exempel koncentration av placeringar i ett geografiskt område eller inom en bransch) eller stor risk för problem hos en ensam värdepappersemittenteller grupp av emittenter. Placeringsportföljen ska hela tiden ha tillräcklig likviditet för att uppfylla alla rimligen förutsebara verksamhetskrav. Detta ska möjliggöras genom att portföljen struktureras på ett sådant sätt att investeringar uppfyller förutsedda kontantbehov.		
Kvantifierbar risk?	Nyckelvariabler	Kontroller
Ja	• Tillräcklig mängd likvida tillgångar ska finnas för Göta Lejon d v s minst 15 mkr • Placeringstyp	• Bedömning av det framtida kapitalbehovet vid omplacering av revers. Görs av ekonomichef.
Riskreducering vidtas om:	• de toleransnivåer som definierats i den acceptabla risknivån har överskridits • solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen • en händelse inträffar som ger avsevärda konsekvenser för den risk som bolagetkan exponeras för.	
Riskreducering	Lämpliga motåtgärder för att reducera risken så att den faller inom gränser för vad Göta Lejon kan acceptera ska definieras så långt som möjligt. Om riskreducering krävs minskar ekonomichef revers hos koncernbanken.	
Risken regleras i:	• Finansiell anvisning	

Riskkategori	Matchningsrisker
Beskrivning	
Hantering av matchningsrisk är en del av bolagets Asset-Liability Management (ALM). Tillgångar som innehas för att täcka försäkringstekniska avsättningar ska investeras på ett sätt som är lämplig med hänsyn till försäkrings- och återförsäkringsskuldernas art och duration. Bristfällig matchning kan innebära att tillgångar behöver inlösas under ofördelaktiga förhållanden samt kan leda till	

ofördelaktig exponering för ränte-, valuta- och kursrisker. Denna risk är mycket begränsad då bolaget placerar sitt kapital på bankkonto tillhörande Göteborgs kommun samt korta reverser utställda mot Göteborgs kommun.		
Kvantifierbar risk?	Nyckelvariabler	Kontroller
Ja	• Löptid (duration) totala tillgångar jämfört med totala skulder.	• Kontroll ska finnas att det vid alla tillfällen skall finnas tillräckligt med likvidamedel för att täcka de skulder som förfaller. • Ekonomichefen följer löpande upp placeringar och löptid.
Riskreducering vidtas om:	• de toleransnivåer som definierats i den acceptabla risknivån har överskridits. • solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen • en händelse inträffar som ger avsevärda konsekvenser för den risk som bolaget kan exponeras för.	
Riskreducering	Motåtgärder för att reducera risken ska definieras så långt som möjligt Vid avvikelse föreslårekonomichef lämpliga åtgärder.	
Risken regleras i:	• Finansiell anvisning	

Riskkategori	**Operationella risker**	
Beskrivning		
Med operationella risker avses risken för förluster till följd av felaktiga eller misslyckade interna processer och rutiner, mänskliga fel, avbrott och störning i verksamhet och system, externa händelser, interna och externa bedrägerier och legala risker. Operativa risker är de som är relaterade till verksamheten och som inte regleras inom någon av ovanstående riskklasser. Med operativa risken regelefterlevnadsrisk menas risken för att verksamheten inte följer lagar och regler.		
Kvantifierbar risk?	Nyckelvariabler	Kontroller
Ja (kvantifieras via schablon i standardformeln)	• Genomförd ledningsprövning/ fit & proper • Göta Lejon drabbas av avbrott i dagliga verksamheten	• Nya styrelseledamöter, vd och dess ställföreträdare ledningsprövas av Finansinspektionen innan personen tillträder sin tjänst.

	• Göta Lejon utsätts för bedrägerier/ penningtvätt • Göta Lejon påförs sanktioner från Finansinspektionen	• En kontroll sker att bolagets nyckelpersoner uppfyller de internt ställda kraven på ”fit & proper” när en nyckelperson tillträder sin tjänst. • Det finns en kontinuitetsplan för hur avbrott i verksamheten ska hanteras. • Göta Lejon uppfyller eventuella krav för att förhindra bedrägerier och/ellerpenningtvätt. • Göta Lejon har rutiner för att hantera bolagets risker och att det finns processer för hur och när rapportering till myndigheter ska genomföras. • Operativa risker tas upp årligen i bolagets övergripande riskanalys
Riskreducering vidtas om:	• de toleransnivåer som definierats i den acceptabla risknivån har överskridits • solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen • en händelse inträffar som ger avsevärda konsekvenser för den risk som Göta Lejon kan exponeras för.	
Riskreducering	Lämpliga motåtgärder för att reducera risken så att den faller inom gränser för vad bolaget kan acceptera ska definieras så långt som möjligt. Riskanalysen tillsammans med riskregister, ERSA rapport och riktlinje för intern styrning och kontroll ger stöd till styrelsen i ansvaret för arbetet med nämnda motåtgärder.	
Risken regleras i:	Operationella risker identifieras, analyseras, planeras för, genomförs samt följs upp och återfinns i Göta Lejons riskregister och ERSA-rapport. • Riktlinje för riskhantering samt intern styrning och kontroll • Försäkrings AB Göta Lejons riktlinje för regelefterlevnad • Försäkrings AB Göta Lejons riktlinje för hantering av intressekonflikter.	

<table>
<tr><th>Riskkategori</th><th colspan="2">Operationella risker</th></tr>
<tr><td>Underkategori</td><td colspan="2">Säkerhetsrisker</td></tr>
<tr><td colspan="3">Beskrivning</td></tr>
<tr><td colspan="3">Med säkerhetsrisker avses hot och sårbarheter som kan leda till skador eller förluster om de utnyttjas eller inträffar, särskilt inom områden som information, teknik, personal eller fysisk säkerhet. Kategorin inkluderar informationssäkerhets- och IKT-risker men även fysisk säkerhet, personalsäkerhet och avbrottsrisker. Med informationssäkerhets- och IKT-risker avses risker som kan äventyra informationens konfidentialitet, riktighet, tillgänglighet eller äkthet. I kategorin ingår även dataskydd.

Dessa risker hanteras genom Göta Lejons riskhanteringssystem regleras ytterligare i övriga säkerhetsrelaterade styrande dokument. Mätning görs via bolagets övergripande riskanalys med uppföljning av centrala funktioner.</td></tr>
<tr><td>Kvantifierbar risk?</td><td>Nyckelvariabler</td><td>Kontroller</td></tr>
<tr><td>Nej</td><td>Företagets strategiska mål definierade i affärsplanen.
Säkerhetsrisker upptagna i riskregistret
Göta Lejon påförs sanktioner från tillsynsmyndighet</td><td>Göta Lejons riskregister ska uppdateras regelbundet för att säkerställa att accepteradrisknivå inte avviker.
Riskanalys vid utlagd verksamhet dvs bedömning om tjänsten avser en kritisk eller viktig funktioneller verksamhet och identifiera och bedöma relevanta risker med överenskommelsen om uppdragsavtal.</td></tr>
<tr><td>Riskreducering vidtas om:</td><td colspan="2">de toleransnivåer som definierats i den acceptabla risknivån har överskridits
solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen
en händelse inträffar som ger avsevärda konsekvenser för den risk sombolaget kan exponeras för.</td></tr>
<tr><td>Riskreducering</td><td colspan="2">Lämpliga motåtgärder för att reducera risken så att den faller inom gränser för vad bolagetkan acceptera ska definieras så långt som möjligt.
Riskanalys, riskregistret och ERSA rapporten ger stöd till styrelsen i ansvaret för arbetetmed nämnda motåtgärder.</td></tr>
<tr><td>Risken regleras i:</td><td colspan="2">Göteborgs Stads riktlinje för informationssäkerhet
Riktlinje för uppdragsavtal och utlagd verksamhet
Kontinuitetsplan
Riktlinje för säkerhet</td></tr>
</table>

Riskkategori	**Strategiska risker**	
Beskrivning		
Strategisk risk definieras som följden av ett eller flera felaktiga affärsbeslut och/eller genomförande av beslut som kommer att påverka Göta Lejons nuvarande resultat eller kapital alternativt Göta Lejons framtida resultat eller kapital i förhållande till Göta Lejons strategiska mål.		
Kvantifierbar risk?	Nyckelvariabler	Kontroller
Nej	• Företagets strategiska mål definierade i affärsplanen.	• En årlig översyn av bolagets strategiska mål ska genomföras tillsammans med bolagets mest väsentliga risker i samband med framtagande av affärsplan. • Göta Lejons riskregister ska uppdateras regelbundet för att säkerställa att accepterad risknivå inte avviker. • Uppföljning av mål
Riskreducering vidtas om:	• de toleransnivåer som definierats i den acceptabla risknivån har överskridits • solvenskvoten i utfall eller prognos bedöms riskera att underskrida den miniminivå som fastställts av styrelsen • en händelse inträffar som ger avsevärda konsekvenser för den risk sombolaget kan exponeras för.	
Riskreducering	Lämpliga motåtgärder för att reducera risken så att den faller inom gränser för vad bolagetkan acceptera ska definieras så långt som möjligt. Riskanalys, riskregistret och ERSA rapporten ger stöd till styrelsen i ansvaret för arbetetmed nämnda motåtgärder.	
Risken regleras i:	• Årlig övergripande riskanalys	

4. Årlig övergripande riskanalys och centralt riskregister

Göta Lejons årliga *övergripande riskanalys* är en organisationsövergripande riskanalys som syftar till att identifiera och bedöma bolagets centrala riskområden på en övergripande nivå. I denna analys ska alla risker som kan hindra Göta Lejon att uppnå de strategiska målen identifieras och dokumenteras. Lokala *riskanalyser* utförs för avgränsade delar inom en organisation, såsom avdelningar, enheter, informationssystem eller processer.

De övergripande riskerna dokumenteras i bolagets centrala riskregister Riskhanteringsfunktionen upprättar och reviderar riskregistret minst en gång per år. Riskregistret åskådliggör bolagets riskprofil och utgör underlag till bolagets ERSA-rapport samt är utgångpunkt för bolagets lokala riskanalyser.

4.1 Tillvägagångssätt

Riskhanteringsprocessen beskrivs kortfattat nedan och är uppdelat i fem delsteg:

1. Identifiera analysens omfattning, avgränsningar och händelser som ska bedömas
2. Analysera hot och sårbarheter, orsaker och konsekvenser
3. Värdera riskerna, bedöm sannolikhet och konsekvens samt skapa riskprofil
4. Hantera riskerna, ta fram och implementera handlingsplaner och åtgärdsprogram
5. Följa upp, granska och utvärdera årligen

Riskregistret utgörs av risker som består av:

- Orsaker och konsekvenser
- Bedömning av sannolikhet och påverkan
- Handlingsplan med riskreducerande åtgärd
- Ansvarig
- Tidplan

För utvärderingen av risker används de sannolikhets- och påverkansklassificeringar som anges i nedan tabeller. Påverkansklassificering är kopplat till ett finansiellt värde.

Påverkan/konsekvensmatris

Nivå	1.Lindrig/Ringa	2. Betydande	3. Allvarlig	4. Mycket allvarlig
Finansiell påverkan (MKR)	0-2.5	2.5-5	5-10	>10
Operationell påverkan *(processer, IT-system, operativdrift)*	Mindre fel i processer system, Ringa förseningar. Mindre avbrott i processer eller system. Ringa på externa relationer	En eller flera huvudansvarskrav uppfylls inte. Större förseningar. Obekvämt men äventyrar inte kunder och leverantörer	Affärsrelationer påverkas allvarligt men bara på kort sikt. Höga kostnader uppstår. Driftstopp	Affärskritiska system eller processer påverkas allvarligt. Affärsverksamheten och kundrelationer påverkas långvarigt. Driftstopp

Sannolikhetstabell

Nivå	Sannolikhet	Kvantitativ bedömning
5	Mycket hög sannolikhet	Inträffar en gång per vecka
4	Hög sannolikhet	Inträffar en gång per månad
3	Medel sannolikhet	Inträffar en gång per år
2	Låg sannolikhet	Inträffar mellan 1 gång per 1-10 år
1	Mycket låg sannolikhet	Inträffar mer sällan än vart 10e år

Riskmatris

Sannolikhet	Mycket hög sannolikhet	5	Medel nivå	Hög nivå	Oacceptabel nivå	Oacceptabel nivå
	Hög sannolikhet	4	Medel nivå	Hög nivå	Oacceptabel nivå	Oacceptabel nivå
	Medel sannolikhet	3	Acceptabel nivå	Medel nivå	Hög nivå	Hög nivå
	Låg sannolikhet	2	Acceptabel nivå	Medel nivå	Medel nivå	Hög nivå
	Mycket låg sannolikhet	1	Acceptabel nivå	Acceptabel nivå	Medel nivå	Hög nivå
			1	2	3	4
			Lindrig/Ringa	Betydande	Allvarlig	Mycket allvarlig
	Konsekvens					

När riskvärdering har genomförts så ska nedanstående skala användas för att bedöma om risk ska hanteras, hur risken får accepteras och vilka som ska informeras om risken.

Tabell för riskvärdering/riskacceptans

Risknivå	Bedömning	Risk får accepteras av	Krav på information
Oacceptabel nivå	Allvarliga risker som behöver åtgärdas snarast. Riskerna har värderats med hög sannolikhet eller hög konsekvens. Dessa risker kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.	Ledning	Ledning, styrelse och bolagscontroller
Hög nivå	Höga risker som behöver åtgärdas. Dessa risker kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.	Ledning	Ledning
Medel nivå	Risker som behöver analyseras djupare. Riskerna ska bevakas i syfte att snabbt kunna sätta in åtgärd om händelsen inträffar.	Riskägare	Ansvarig chef
Acceptabel nivå	Risker som inte kräver någon åtgärd alternativt bedömts som låga. Risken har värderats lågt och det har bedömts att den inte medför störningar i organisationen. Risk som kan accepteras men som ska bevakas. Dessa risker kan hanteras i den löpande verksamheten.	Riskägare	Inga krav

5. Egen risk- och solvensanalys (ERSA)

Den egna risk- och solvensanalysen (ERSA) skall säkerställa att bolagets kapital är, och förblir, tillräckligt för att bära de risker som följer av bolagets affärsplan. Analysen ska därför ta utgångspunkt i arbetet med affärsplanen och inkludera ogynnsamma men realistiska scenarier, stresstester och omvända stresstester.

Resultaten av analysen ska få leda till modifieringar av affärsplanen om så krävs för att en acceptabel risknivå ska kunna upprätthållas. Tillvägagångssätt och resultat ska rapporteras till Finansinspektionen.

Inom ramen för ERSA:n skall även en utvärdering av riskhanteringssystemet genomföras i vilken lämpligheten och effektiviteten hos de processer, system, organisationer och kontroller som finns på plats för att hantera och kontrollera risk granskas.

Styrelsen för bolaget är ytterst ansvarig för ERSA:n. Ekonomichef och Riskhanteringsfunktionen ansvarar dock för det operativa arbetet och rapporteringen. ERSA-processen och hur scenarier och stresstester utförs beskrivs i Riktlinje för ERSA.

5.1 Stresstester och scenarioanalyser

Bolaget ska minst en gång per år genomföra stresstester och scenarioanalyser kopplat till de risker som bolaget är exponerad mot.

6. Kontroll och uppföljning av risker i verksamheten

Enligt trelinjesmodellen ansvarar den första försvarslinjen inklusive vd för att i sitt dagliga arbete löpande kontrollera att den definierade riskaptiten i respektive riskkategori inte överskrids. Första förvarslinjen ansvarar även för att de kontroller som definieras i bolagets egenkontrollplan utförs.

Om riskaptiten överskrids så ska vd omgående informeras. Vd ska därefter fastställa lämpliga åtgärder för att minska risken inom de gränser som har godkänts av styrelsen.

Riskreducerande åtgärder vidtas om:

- den definierade riskaptiten som återfinns i bolagets interna riktlinjer överskridits,
- en händelse inträffar som potentiellt kan ge stora negativa konsekvenser för riskkategorin.

Den andra försvarslinjen kontrollerar vid sina granskningar bland annat att den definierade riskaptiten i riskkategorierna inte har överskridits medan den tredje bland annat undersöker och utvärderar efterlevnad av interna strategier, styrande dokument, processer och rapporteringsrutiner.

6.1 Riskhanteringsfunktion

Göta Lejon har en riskhanteringsfunktion som är objektiv och oberoende från operativa funktioner. Denna funktion är utlagd på extern tredje part. Funktionen regleras i Riktlinje för riskhanteringsfunktionen.

I riskhanteringsfunktionens uppdrag ingår att:

- Ta fram riskhanteringsrapport varje kvartal
- Gå igenom och vid behov uppdatera riktlinjen för företagsstyrning samt riktlinjen för riskhantering och intern styrning och kontroll
- Gå igenom och eventuellt uppdatera riskregistret
- Förbereda för framtagande av ERSA-rapport.

Vid behov ska riskhanteringsfunktionens arbete även presenteras för styrelse.

6.2 Incidentrapportering

Bolaget ska upprätthålla ett detaljerat register över alla väsentliga händelser och incidenter som kan påverka bolagets riskprofil eller finansiella ställning. Detta register ska regelbundet, minst kvartalsvis, granskas och uppdateras. Riskhanteringsfunktionen har ansvar för att kontinuerligt analysera detta register för att identifiera trender, möjliga riskområden, och att bedöma effekterna av dessa händelser på bolaget. Processen för incidenthantering ska innefatta följande steg:

- **Insamling av data:** Alla medarbetare inom bolaget är ansvariga för att rapportera incidenter till riskkommittén. Rapporteringen ska ske omedelbart efter det att en

incident har identifierats. Riskkommittén underrättar riskhanteringsfunktionen löpande om inträffade incidenter.

- **Analys och utvärdering**: Inträffade incidenter analyseras och utvärderas av bolagets riskkommitté som även tillser att omedelbara åtgärder vidtas. Inträffade incidenter behandlas även i bolagets gruppering för intern styrning och kontroll (ISK). Vidare analyserar och utvärderar även riskhanteringsfunktionen alla rapporterade incidenter för att fastställa deras inverkan och underliggande orsaker. Denna analys hjälper till att förstå riskexponering och behovet av ytterligare åtgärder.
- **Sammanställning av rapporter**: Bolaget tar löpande fram en rapport innehållande inträffade incidenter och vidtagna åtgärder. Riskhanteringsfunktionen sammanställer en detaljerad rapport baserad på analysen av incidenterna. Denna rapport inkluderar rekommendationer för åtgärder och förbättringar.
- **Kommunikation till styrelsen**: De sammanställda rapporterna presenteras för styrelsen som en del av deras regelbundna möten. Detta möjliggör för styrelsen att göra välgrundade beslut baserade på aktuell och relevant riskinformation.

7. Fastställande, utvärdering och efterlevnad

Denna riktlinje fastställs av styrelsen och träder i kraft dagen för beslut.

Riktlinjen ska utvärderas och ses över minst en gång per år. Riskhanteringsramen ska fortlöpande förbättras baserat på erfarenheter från genomförande av riskhanteringsarbete och övervakning. Översyn ska ske vid uppkomst av allvarliga IKT-relaterade incidenter, tillsynsinstruktioner eller slutsatser från relevanta testnings- eller revisionsprocesser för digital operativ motståndskraft.

Riktlinjen ska årligen fastställas av styrelsen även om inga ändringar beslutas. Ansvarig för uppdatering av riktlinjen är vd.

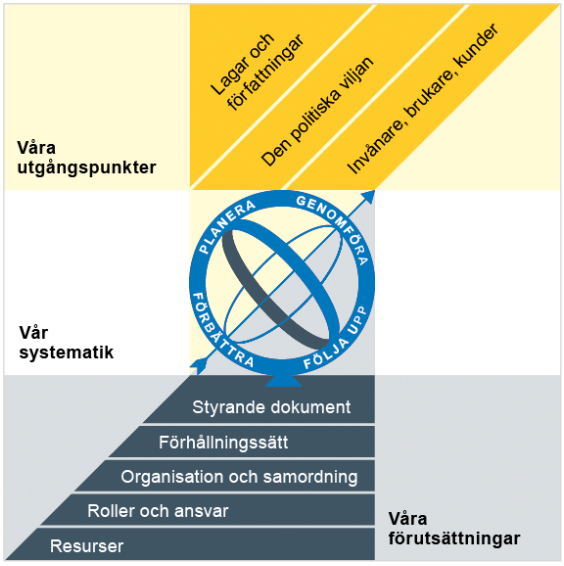
Göteborgs Stad

Försäkrings AB Göta Lejons riktlinje för säkerhet

Reglerande styrande dokument

- Policy
- ► **Riktlinje**
- Regel
- Anvisning
- Rutin
- Instruktion

Göteborgs Stads styrsystem



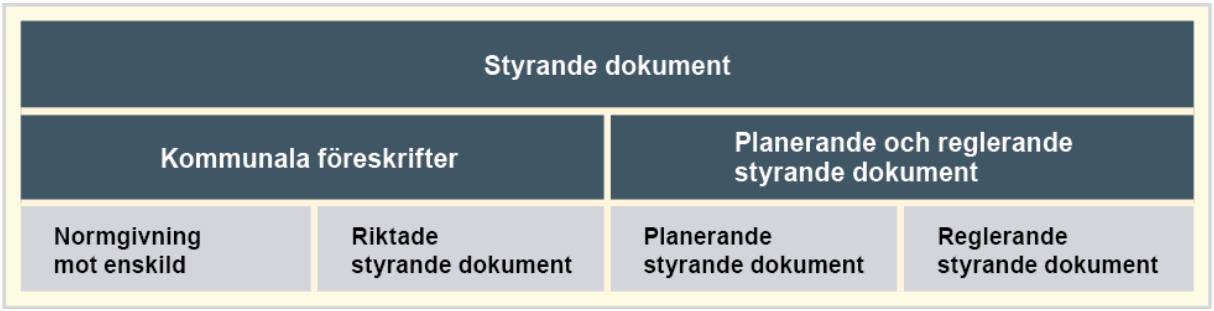
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Styrelse	Försäkrings AB Göta Lejon	FGL-2025-00123	§ 107 2025-06-12
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	2025-06-02	Säkerhetschef

Bilagor:

Innehåll

Inledning

Syftet med denna riktlinje

Syftet med denna riktlinje är att ange bolagets strategi, principer och ansvar avseende Göta Lejons systematiska säkerhetsarbete för att främja en effektiv riskhantering och säkerställa erforderligt skydd rörande bolagets information. Särskild hänsyn är tagen för att säkerställa uppfyllnad av krav utifrån DORA förordningen.

Riktlinjen utgör Försäkrings AB Göta Lejons strategi för säkerhet.

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för hela bolaget samt utlagd verksamhet och verksamhet som utför arbete genom uppdragsavtal.

Lagbestämmelser

Denna riktlinje har upprättats i enlighet med:

- Dora-förordningen (EU) 2022/2554
- EIOPA-BoS – 20/600: Riktlinjer för säkerhet och företagsstyrning avseende informations och kommunikationsteknik

Koppling till andra styrande dokument

Styrande dokument
Göteborgs stads säkerhetspolicy
Göteborgs stads riktlinje för informationssäkerhet
Göteborgs stads regel för IT användare
Göteborgs stads regler för användande av e-post
Försäkrings AB Göta Lejons riktlinje för företagsstyrning
Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll
Försäkrings AB Göta Lejons riktlinje för uppdragsavtal och utlagd verksamhet
Försäkrings AB Göta Lejons riktlinje för hantering och rapportering av händelser av väsentlig betydelse
Försäkrings AB Göta Lejons riktlinje för datakvalité
Försäkrings AB Göta Lejons riktlinje för internrevisionsfunktionen

Försäkrings AB Göta Lejons riktlinje för integritet och dataskydd
Försäkrings AB Göta Lejons kontinuitetsplan
Försäkrings AB Göta Lejons krisledningsplan

Riktlinje

Göta Lejons företagsstyrning och system för riskhantering och intern kontroll ska utformas så att säkerhetsrisker, med särskild vikt på informations- och kommunikationstekniska risker samt informationssäkerhetsrisker, hanteras på lämpligt sätt.

Som captivebolag med verksamheten begränsad till koncernens egna risker tillämpar bolaget regelverket för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik (IKT) på ett sätt som står i proportion till arten, omfattningen och komplexiteten av bolagets inneboende risker.

Denna riktlinje fastställs av styrelsen och träder i kraft dagen för beslut. Riktlinjen ska årligen fastställas av styrelsen även om inga ändringar beslutas. Ansvarig för uppdatering av riktlinjen är vd.

Alla medarbetare ansvarar för att denna riktlinje följs. Chefer i organisationen säkerställer att riktlinjen efterlevs och att kunskap om innehållet finns inom gruppen.

Göta Lejon integrerar informationssäkerhetsarbetet i IKT. I detta ingår även dataskydd.

Säkerhetsstrategi

Bolagets strategi för säkerhet grundar sig på den befintliga riskstrategin inom bolagets riskhanteringssystem, dvs att öka sannolikheten för att bolaget ska uppnå de strategiska (verksamhetsnära) målen. Säkerhetsstrategin fastställer en strukturerad och långsiktig inriktning för hur organisationen ska skydda sina tillgångar, säkerställa verksamhetens kontinuitet och bygga en motståndskraftig säkerhetskultur. Effekter av oönskade och oväntade händelser ska minimeras. Säkerhetsstrategin utgör även bolagets IKT-strategi.

Denna strategi gäller all verksamhet bolaget bedriver, oavsett om den utförs internt eller av extern part. Strategin ska alltid beaktas, oavsett om det gäller verksamhetsplanering, organisations- och verksamhetsutveckling, dagligt arbete eller system och tjänster.

Målet med strategin är att:

- Säkerställa att bolaget efterlever lagar och förordningar samt övergripande krav utifrån tillsynsmyndigheter och Göteborgs Stad.
- Skydda information utifrån konfidentialitet, integritet, tillgänglighet och äkthet
- Förebygga samt ha kapacitet att upptäcka och hantera säkerhetsincidenter
- Etablera en god säkerhetskultur samt stärka medarbetares säkerhetsmedvetenhet och förståelse för individens ansvar

Riskhantering

Hantering av säkerhetsrisker ska vara en del av bolagets allmänna riskhanteringssystem och riskhanteringsprocess som finns beskrivet i bolagets riktlinje för riskhantering och intern styrning och kontroll. I enlighet med bolagets riskhanteringssystem gäller följande avseende säkerhetsrisker:

- Identifierade säkerhetsrisker ska tas dokumenteras i bolagets riskregister
- Hantering av säkerhetsrisker ska analyseras, planeras för, följas upp och hanteras i enlighet med bolagets styrande dokument för risk och säkerhet
- Kvarstående säkerhetsrisker ska hanteras i bolagets kontinuitetsplan

- Myndighetssanktioner till följd av otillräcklig intern styrning och kontroll accepteras ej

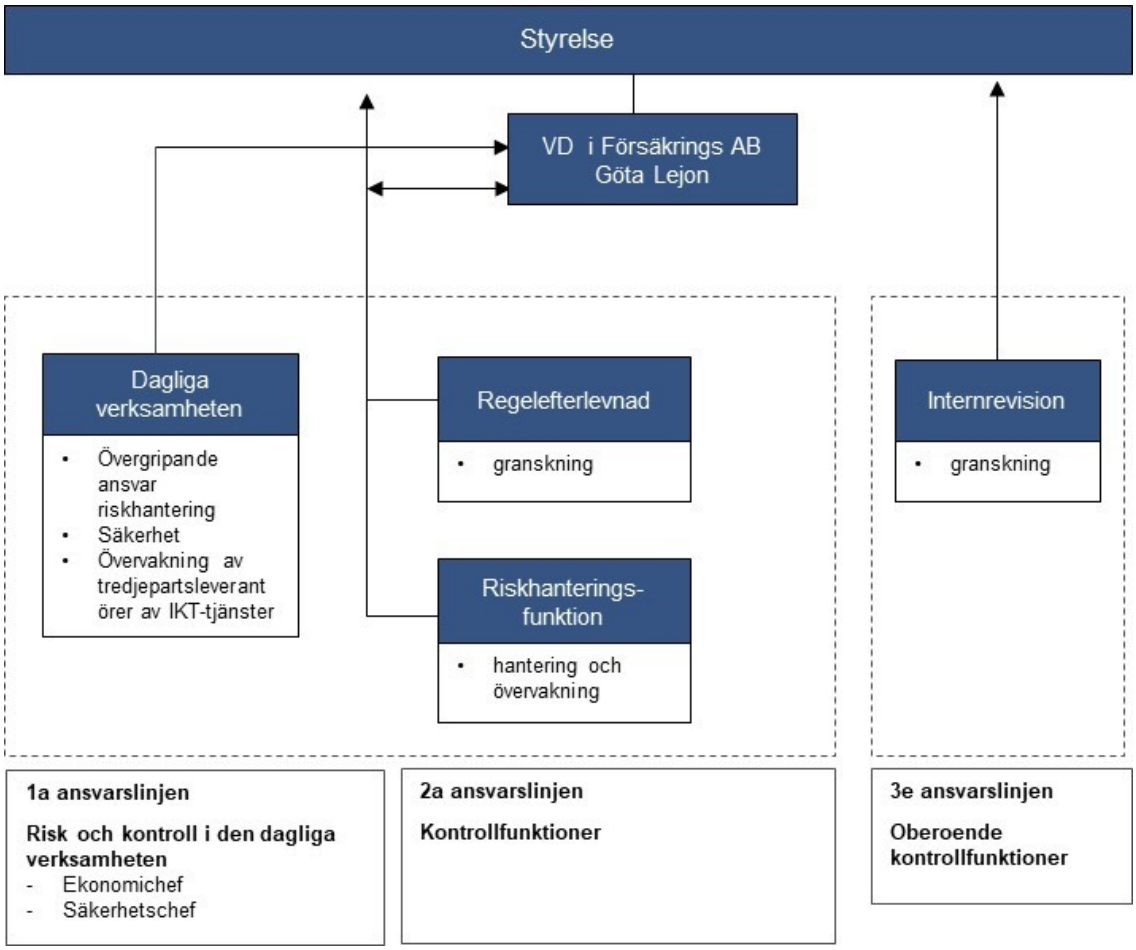
Ansvar och roller

Roller och ansvarsfördelning för säkerhetsarbetet beskrivs i Tabell 1.

Tabell 1: Roller och ansvarsfördelning för säkerhetsarbetet.

Område	Ansvar	Utförare/deltagare
Övergripande ansvar hela riskhanteringsområdet	Ekonomichef	
Riskkommitté	Ekonomichef	Säkerhetschef
Intern riskhantering, inkl. kontinuitetshantering och övervakning av IKT-tredjepartsleverantörer	Ekonomichef	
Intern säkerhet	Säkerhetschef	
Personsäkerhet	Säkerhetschef	Administratör
Fysisk säkerhet	Säkerhetschef	Administratör
Informationssäkerhet, inkl. säkerhetsskydd	Säkerhetschef	Processägare IT
Krisberedskap	Säkerhetschef	

Roller och ansvar avseende IKT och respektive försvarslinje beskrivs i Figur 1. Respektive roll förtydligas ytterligare i avsnitten om Hantering och övervakning, oberoende funktion för informationssäkerhet och internrevision.



Figur 1: Roller och ansvar avseende IKT relaterat till trelinjesmodellen.

Styrelsen

Styrelsen ska se till att bolagets hantering och kontroll av risker är tillfredsställande och har det yttersta ansvaret för bolagets säkerhetsarbete. Detta ansvar inkluderar att tillse att bolaget har en tillräcklig hantering av säkerhet. Styrelsen ansvarar för att sätta riktning, fatta beslut, tilldela resurser och följa upp säkerhetsarbetet samt även upprätta och fastställa bolagets styrande dokument som en del av bolagets affärsstrategi.

Inom säkerhetsområdet omfattar styrelsens ansvar specifikt att:

- Bedöma och förstå säkerhetsrisker på verksamhetsnivå
- Godkänna årliga riskanalyser och riskbedömningar
- Fatta beslut om riskaptit och toleransnivå
- Prioritera och resurssätta säkerhetsinsatser utifrån risk
- Ta del av årliga rapporter om säkerhetsarbetet
- Säkerställa att revisioner och tester genomförs
- Följa upp åtgärder efter incidenter eller avvikelser
- Fastställa relevanta riktlinjer
- Fastställa bolagets IKT-strategi, dvs säkerhetsstrategin

VD

Vd ansvarar för att de grundläggande inriktningarna som framgår av denna riktlinje tillämpas i den dagliga verksamheten och att de efterlevs. Vidare ska vd säkerställa att det finns tillräckliga resurser och erforderlig kompetens för att efterleva vad som anges i denna riktlinje och övriga tillämpliga interna regler avseende säkerhet. Vd ska även tillse att berörda parter/medarbetare har nödvändig kunskap genom lämplig utbildning inom säkerhetsområdena.

Processägare

Ansvarar för att:

- identifiera kritiska processer och risker inom sitt ansvarsområde
- säkerställa att informationsbärare och information är identifierad och att informationen är klassad utifrån bolagets anvisning för informationsklassning
- personal, inhyrda konsulter och kontrakterad tredje part är informerade om relevanta krav på säkerhet samt får tillgång till erforderlig utbildning

Medarbetare

Ansvarar för att:

- säkerställa efterlevnad i det dagliga arbetet och att aktivt ta del av de regler och krav som ställs på individen
- delta i de aktiviteter som beslutas av bolagets säkerhetsansvarig
- delta i hantering av inträffade säkerhetsincidenter
- genomföra obligatoriska utbildningar och säkerhetskampanjer anvisade av Göteborg Stad eller bolaget.

Kontinuitetshantering

Kontinuitetshantering avser den planering som behövs för att hantera och minimera negativa konsekvenser då avbrott sker i den dagliga verksamheten. Syftet är att säkerställa tillgång till kritiska resurser och funktioner för att upprätthålla prioriterad verksamhet vid störningar och kriser. Planerna ska regelbundet testas och uppdateras. Ekonomichef ansvarar för att kontinuitetsplaner är framtagna för bolagets kritiska processer och att beroenden är utredda och har nödvändiga åtgärder planerade.

Kontinuitetsplaneringen ska utgå från risk och konsekvensanalys där identifierade processer, system och resurser bedöms utifrån tidskritiska återställningskrav samt interna och externa beroenden. Det ska finnas upprättade kontinuitetsplaner för prioriterade funktioner samt återställningsplaner för kritiska och viktiga IT-system. Nödvändiga rutiner för kommunikation och kriskommunikation ska upprättas, både internt och externt. Planer ska testas årligen och lärdomar ska återföras genom uppdaterade planer.

Fysisk säkerhet

Med fysisk säkerhet avses skydd för verksamhetens personal, lokaler, informationstillgångar och utrustning från skadegörelse, brand, stöld, obehörig åtkomst samt andra fysiska hot. Säkerhetsåtgärder ska definieras oavsett om det gäller bolagets egna lokaler eller tjänsteleverantörer. Åtgärder ska

dokumenteras och genomföras för att skydda lokaler, datacenter och känsliga områden från obehörigt tillträde med hjälp av passerkort, nycklar eller kodlås. Tillträde ska endast beviljas till behörig personal och besökare ska registreras i reception, bära besöksbricka och ha en följeslagare i skyddade områden.

Åtkomst ges efter principen minsta möjliga behörighet och bör granskas regelbundet. Skyddade områden som kan vara känsliga är ex. serverrum, nätverksskåp eller teknikrum och dessa bör skyddas med ex. larm, kameraövervakning eller brandklassade dörrar. Alla lokaler ska ha brandskydd enligt gällande lagar och förordningar.

Incidenthantering

Bolaget ska säkerställa att säkerhetsincidenter hanteras snabbt, korrekt och spårbart för att minimera skador på verksamheten, information och infrastruktur. Alla incidenter ska rapporteras omgående och dessa ska bedömas utifrån allvarlighet, påverkan (verksamhet, information, system) samt om incidenten rör utpekad kritiskt/viktigt system eller personuppgifter. Säkerhetsincidenter ska hanteras enligt bolagets styrande dokument avseende incidenthantering.

Informationssäkerhet

Informationssäkerhetsarbetet omfattar alla typer av informationstillgångar och informationsbehandlande resurser som bolaget hanterar, oavsett om de behandlas manuellt eller digitalt och oberoende av vilken i form eller miljö den förekommer.

Göta Lejon ska skydda informationstillgångar avseende:

- Konfidentialitet, att information inte tillgängliggörs eller avslöjas för obehöriga.
- Riktighet, att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd. Detta inkluderar även äkthet, i form av säkerställande av sändare och mottagare.
- Tillgänglighet, att information är tillgänglig och användbar när den behövs.

Göta Lejon följer Göteborgs stads metod för säker informationshantering. Arbetet ska bedrivas systematiskt och långsiktigt och innehålla följande delar:

- Informationsklassificering
- Riskanalys
- Vidtagande av säkerhetsåtgärder
- Uppföljning

Bolaget ska tillse att det finns en uppdaterad förteckning över informationstillgångar enligt Göteborgs stads riktlinje för informationssäkerhet.

Bolaget ska ha uppdaterade processbeskrivningar som tillsammans med förteckningen över informationstillgångar utgör ett underlag för att kunna bedöma informationssäkerhetsrisker och hur informationssäkerhetsarbetet bedrivs på ett lämpligt sätt.

Informationssäkerhetsrisker ska inkluderas i bolagets riskregister som tas fram av bolaget tillsammans med funktionen för riskhantering.

Bolagets ekonomichef har övergripande ansvar för hela riskhanteringsområdet. Informationssäkerhet är ett åtgärdsområde inom riskhanteringen. För planering, genomförande och uppföljning av informationssäkerhet ansvarar bolagets säkerhetschef.

Detta inbegriper att:

- utveckla och förvalta ledningssystem för informationssäkerhet
- utveckla interna regler och säkerhetsåtgärder
- förvalta bolagets register över informationstillgångar
- genomföra riskbedömningar och hotbildsanalyser
- medverka i riskanalyser som berör informationssäkerhet samt uppdatering av riskregister
- uppföljning av informationssäkerhetsarbetet
- utvärdera bolagets informationssäkerhetsarbete

IT-drift

Bolagets IT-drift utförs av Intraservice som därför ansvarar för att Göta Lejons IT har de säkerhetsåtgärder, rutiner och funktioner som krävs för att säkerställa en tillräckligt hög säkerhetsnivå i enlighet med externa och interna krav. Verksamheten bedrivs på uppdragsavtal och följs upp av Göta Lejon i enlighet med riktlinje för utlagd verksamhet.

Hantering och övervakning, Oberoende funktion för informationssäkerhet

I enlighet med Dora-förordningen, Artikel 6:4 samt EIOPA-BoS – 20/600 ska bolaget ska ha en oberoende funktion eller person för hantering och övervakning av informationssäkerhet. Riskhanteringsfunktionen ansvarar för att identifiera och bedöma risker kopplade till informationssäkerhet, och ska därvid även vara oberoende gentemot utvecklings- och driftprocessen inom informationssäkerhet. Särskilt när det kommer till informationssäkerhet samt IKT-risker ska riskhanteringsfunktionen:

- utgöra ett stöd till bolagets ledning i samband med fastställande och upprätthållande av bolagets informationssäkerhetsarbete
- regelbundet rapportera och ge vägledning om informationssäkerhetens status och utveckling
- övervaka och granska genomförandet av informationssäkerhetsåtgärder
- följa upp hur informationssäkerhetskrav följs upp av tjänsteleverantörer
- följa upp anställda och ledningens kunskap och kännedom om bolagets informationssäkerhetsriktlinjer
- samordna granskningar av operativa incidenter eller säkerhetsincidenter och rapportera granskningar till bolagets ledning och vd.

De närmare reglerna för funktionen finns i riktlinjer för riskhanteringsfunktionen.

Internrevision

I enlighet med Dora-förordningen Artikel 6:6 ska området för IKT och informationssäkerhet ingå som i internrevisionens granskningsplan med lämplig frekvens, (se också riktlinje för internrevision).

Leverantörer

Bolaget ska tillse att relevanta krav för tjänster och system uppfylls även när dessa utförs av extern part. Säkerhetskraven ska beaktas i leverantörsrelationer och införande av nya system. Detta gäller även idrifttagande av nya moduler inom befintliga system eller då större förändring sker exempelvis genom uppdatering till nya versioner.

Verksamhet som inte utförs på uppdragsavtal ska kravställas och följas upp utifrån det Göta Lejon anser nödvändigt för att bolagets information ska hanteras säkert. Samtliga arrangemang med tredjepartsleverantörer av IKT-tjänster ska årligen sammanställas och övervakas avseende riskexponering och relevant dokumentation. Ansvarig för detta är ekonomichef.

Vid kravställande ska bolaget beakta vilken möjlighet som ges till olika former av granskningar av leverantörens säkerhetskrav. Detta kan avse exempelvis rätten till revision, krav på åtkomst till resultat av leverantörens egenkontroller eller externa granskningar initierade av leverantören själv, stöd från leverantören vid granskningar och Finansinspektionens rätt till insyn. Det ska även säkerställas att Göta Lejon har möjlighet att rapportera nödvändig information som ska levereras till Finansinspektionens informationsregister.

Ovanstående krav gäller även vid hantering av tredjepartsleverantörer.

Vid utkontraktering av IKT-tjänster, upprättande av utlagd verksamhet och/eller uppföljning av någon av dessa tjänster ska bolagets riktlinje för utlagd verksamhet samt rutin för utkontraktering av IKT-tjänster följas.

Tillämpning

Denna riktlinje reglerar all informationsbehandling oavsett driftsmiljö och gäller oavsett om behandlingen sker internt eller hos en tjänsteleverantör av outsourcad verksamhet.

Riktlinjen ska göras tillgänglig för och tillämpas av bolagets styrelseledamöter, vd, medarbetare och konsulter. I förekommande fall måste instruktionerna också meddelas och tillämpas av företagets tjänsteleverantörer av utlagd verksamhet.

Vid eventuell diskrepans mellan Göteborgs Stads regler och denna riktlinje, ska stadens riktlinjer och strategi i första hand äga företräde. Bolaget ska dock alltid hålla sig inom ramarna för vad som krävs och är tillåtet för bolaget tillämpliga regelverk varpå det i vissa situationer är Göta Lejons riktlinjer som har företräde.

Fastställande och efterlevnad

Denna riktlinje fastställs av styrelsen och träder i kraft dagen för beslut. Riktlinjen ska årligen fastställas av styrelsen även om inga ändringar beslutas. Ansvarig för uppdatering av riktlinjen är vd.

Riktlinjen och dess tillämpning ska ses över vid uppkomst av allvarliga IKT-relaterade incidenter, tillsynsinstruktioner eller slutsatser från relevanta testnings- eller revisionsprocesser för digital operativ motståndskraft.

Alla medarbetare ansvarar för att denna riktlinje följs. Chefer i organisationen säkerställer att riktlinjen efterlevs och att kunskap om innehållet finns inom gruppen.