Tjänsteutlåtande
Utfärdat 2026-04-02
Ärendenummer FGL-2026-00102

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

Styrande dokument för årligt beslut i styrelse 2026

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

- Styrelsen antar Försäkrings AB Göta Lejons riktlinje säkerhet
- Styrelsen antar Försäkrings AB Göta Lejons riktlinje för testning av digital operativ motståndskraft

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 säkerhet

2. Försäkrings AB Göta Lejons riktlinje för testning av digital operativ motståndskraft

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 säkerhet** har nedanstående ändringar utförts.

I avsnittet **Lagbestämmelser** samt **Hantering och övervakning, Oberoende funktion för informationssäkerhet** har referens till ej längre gällande kravställning tagits bort.

I avsnittet Riktlinje har formuleringen *Som captivebolag med verksamheten begränsad till koncernens egna risker* förtydligats till *Som captivebolag med verksamheten begränsad till att försäkra Göteborgs stads egna risker*.

I avsnittet **Ansvar och Roller, VD** har det gjorts ett tillägg avseende att tillräckliga resurser och kompetens *inkluderat teknisk utveckling, säkerhet och riskhantering* ska säkerställas.

I avsnittet **Informationssäkerhet** har följande ändringar genomförts:

Avsnittet **Mekanismer för att upptäcka, förebygga och skydda mot IKT-relaterade incidenter** har lagts till. Tillägget har gjorts i enlighet med Dora Art 6.8e som ställer krav på att IKT-riskhanteringsramen ska beskriva vad bolaget gör för att upptäcka IKT-relaterade incidenter, förebygga effekter och ge skydd mot dessa.

I avsnittet **Hantering och övervakning, Oberoende funktion för informationssäkerhet** har justeringar i punktlistan gjorts för att passa nuvarande reglering i Dora.

I avsnittet **Tillämpning** har formuleringen *Regulatoriska minimikrav i Dora-förordningen ska dock alltid uppfyllas* ersatt den tidigare formuleringen*: 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.*

Försäkrings AB Göta Lejons riktlinje för testning av digital operativ motståndskraft är en ny riktlinje. Riktlinjen är framtagen i enlighet med Dora-förordningen där det ställs krav på en heltäckande IKT-riskhanteringsram omfattande en strategi för digital operativ motståndskraft som bland annat inbegriper att genomföra tester av denna (Artikel 6.1 samt 6.8 g).

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

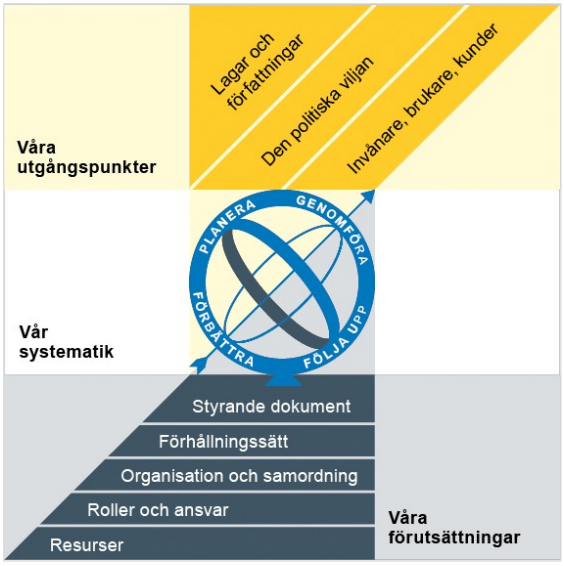
Göteborgs Stad

Försäkrings AB Göta Lejons riktlinje för säkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



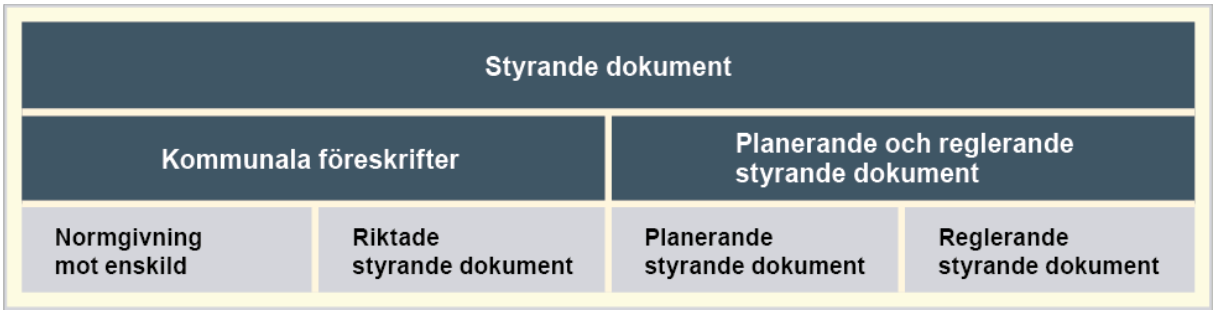
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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-2026-00102	

Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	2026-04-01	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

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 att försäkra Göteborgs stads 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

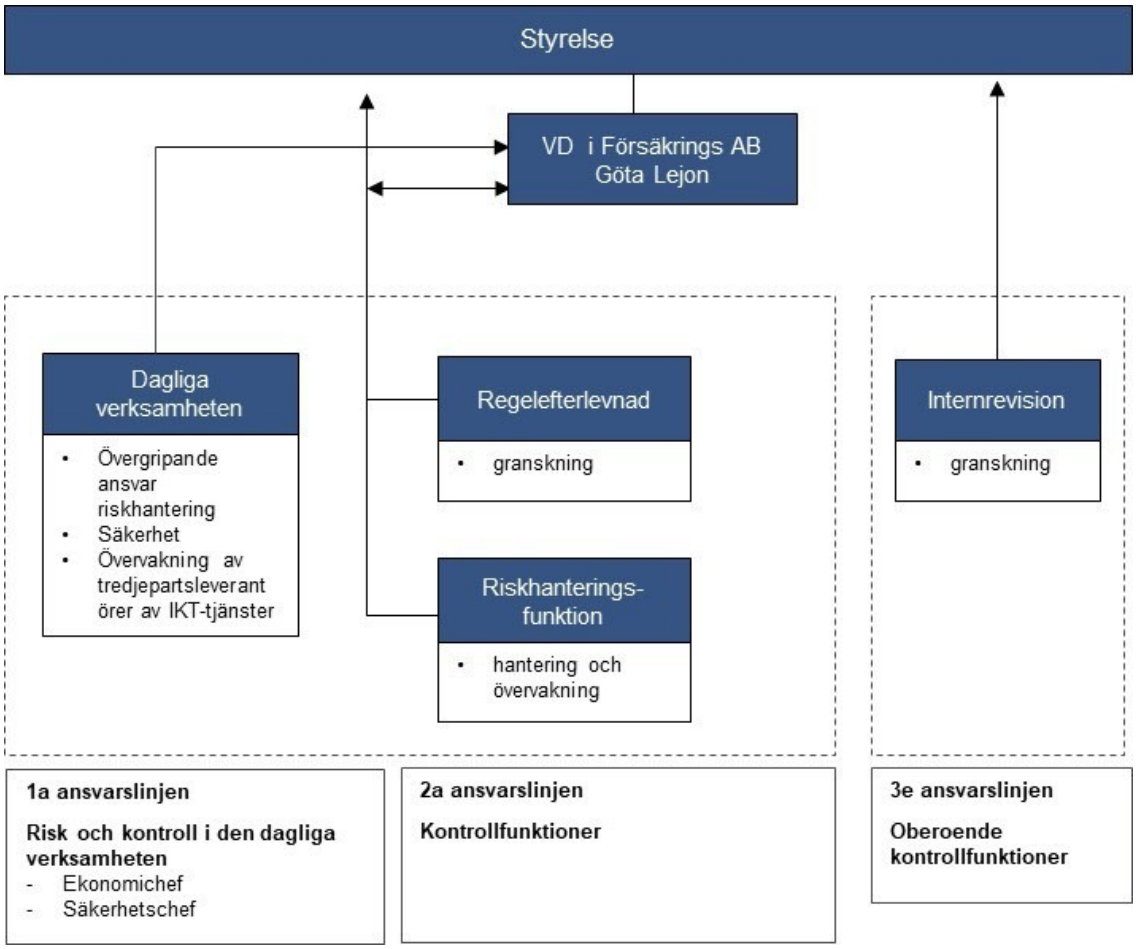
Ansvar och roller

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, inkluderat teknisk utveckling, säkerhet och riskhantering, 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.

Ansvarsfördelning informationssäkerhet

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
- fastställa krav och följa upp att IT-drift och systemansvariga tillämpar mekanismer för upptäckt, förebyggande och skydd samt att brister hanteras inom fastställda tidsramar.

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 form eller miljö den förekommer i.

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.

Mekanismer för att upptäcka, förebygga och skydda mot IKT-relaterade incidenter

Bolaget ska ha dokumenterade och införda mekanismer för att upptäcka, förebygga och skydda mot IKT-relaterade incidenter och avvikande aktiviteter. Mekanismerna ska vara riskbaserade, spårbara och omfatta system och tjänster med högre kritikalitet i första hand.

Bolaget ska:

- Tillämpa **loggning, övervakning och larm** med tydliga eskaleringsvägar och ansvar samt tidsramar för åtgärd.
- Fastställa och tillämpa **minimikrav för skydd** utifrån risk och klassning.
- Säkerställa att **sårbarheter identifieras, prioriteras och åtgärdas** inom fastställda tidsramar.
- Säkerställa etablerad **incidenthantering** (registrering, klassificering, eskalering och analys).
- Säkerställa att **behörigheter** kontrolleras och granskas regelbundet för system som är nödvändiga för att upprätthålla kritiska funktioner.

Uppföljning och underlag för aktuell nivå av digital operativ motståndskraft

Bolaget ska löpande kunna redovisa ett spårbart underlag som visar aktuell nivå och utveckling av bolagets digitala operativa motståndskraft, baserat på incident utfall och effektivitet i förebyggande åtgärder. Underlaget ska användas för styrning, prioritering och intern kontroll.

Bolaget ska:

- Föra ett **incidentregister** som möjliggör trendanalys (t.ex. frekvens, typ, rotorsak, påverkan, åtgärder och återställning).
- Definiera och följa upp relevanta **indikatorer/KPI/KRI** för motståndskraft och förebyggande förmåga.
- Dokumentera **brister och avvikelser med ansvar och tidsfrist** samt verifiera genomförda förbättringar.
- Genomföra **analys** och dokumentera **lärdomar** efter allvarliga incidenter och verifiera att beslutade förbättringar fått avsedd effekt.
- Säkerställa att uppföljningsunderlag används i **riskregister**, internkontroll och ledningens uppföljning.

Göta Lejon ska verifiera sin förmåga till digital operativ motståndskraft genom planerade tester och övningar. Detta ska omfatta såväl förebyggande kontroller som återställnings- och kontinuitetsförmåga. Resultat från tester och övningar ska användas vid översyn av bolagets IKT-riskhantering.

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 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:

- löpande övervaka och kontrollera IKT-risker som en del av bolagets övergripande riskhanteringssystem
- oberoende följa upp första linjens arbete
- rapportera till vd och styrelse
- utgöra ett stöd till bolaget i samband med översyn av IKT-riskhanteringsramen i enlighet med Dora
- följa upp incidenter, tredjepartsrisker och kontinuitetsförmåga
- löpande ge rådgivning till ledning och verksamhet i IKT-relaterade frågor

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. Regulatoriska minimikrav i Dora-förordningen ska dock alltid uppfyllas.

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.

Göteborgs Stad

Försäkrings AB Göta Lejons riktlinje för testning av Digital Operativ Motståndskraft

Reglerande styrande dokument

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

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Styrelse	Försäkrings AB Göta Lejon	FGL-2026-00102	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	2026-04-01	Säkerhetschef

Bilagor:
Begrepp och definitioner

Innehåll

Inledning

Syftet med denna riktlinje

Syftet med denna riktlinje är att ange ramarna för testning av bolagets digitala operativa motståndskraft. Ramarna ska säkerställa att bolaget upprätthåller ett sunt och heltäckande program för testning genom att

- riskbaserat testa kontroller, tekniska och organisatoriska skydd, återställningsförmåga och krisledningsförmåga
- identifiera svagheter, ta fram åtgärder och förnyad testning
- uppdatera riskregister, riskaptit och kontinuitetsförmåga

Programmet ska vara revisionsbart med spårbarhet mellan kritisk/viktig funktion, beroenden, testobjekt, test, resultat, fynd, åtgärd, godkännande och eventuella förnyade tester.

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för Försäkrings AB Göta Lejon.

Lagbestämmelser

Denna riktlinje har upprättats i enlighet med:

- Dora-förordningen (EU) 2022/2554

Koppling till andra styrande dokument

- Riktlinje för riskhantering och intern styrning och kontroll
- Riktlinje för säkerhet
- Riktlinje för kontinuitet
- Anvisning för riskhantering
- Anvisning för incidenthantering

Stödjande dokument

- Leverantörsregister
- Processbeskrivningar

Riktlinje

Enligt Dora, artikel 24 ska bolaget inrätta, upprätthålla och se över ett sunt och heltäckande program för testning av digital operativ motståndskraft. Genom programmet ska bolaget kunna bedöma beredskapen för hantering av IKT-relaterade incidenter, identifiera svagheter, brister och luckor i den digitala operativa motståndskraften och snabbt genomföra korrigerande åtgärder.

Göta Lejons testprogram är en del av bolagets IKT-riskhanteringsram. Det består av den riktlinjen för testning samt obligatoriska dokument och register (testkatalog, kalender, resultat, historik, beslutslogg, tredjepartsevidens). Tillsammans säkerställer detta spårbarhet, uppföljning och revisionsbarhet.

Ansvar

Ansvaret för testning fördelas i enlighet med tre ansvarslinjer bolagets riktlinje för företagsstyrning. Det innebär att:

- första linjen äger testobjekt, säkerställer åtgärder och genomför tester enligt plan
- andra linje granskar testprogram, kvalitetssäkrar koppling mellan risk och test, godkänner kontrolltester och följer upp eskalering
- interrevision utför oberoende granskning av testprogrammet och dess effektivitet

En årsplan för tester tas fram i samband med fastställande av bolagets årsplan för informations- och IKT-säkerhet.

Resultatet från tester rapporteras i bolagets forum för intern styrning och kontroll (ISK). En sammanlagd rapportering sker varje kvartal i bolagets verksamhetsrapport.

Testbas

Göta Lejons testprogram ska utgå från följande parametrar:

- Register över kritiska funktioner och identifierade återställningstider i bolagets BIA (Business Interruption Analysis)
- Riskregister – identifierade risker med risknivå som överstiger acceptabel nivå
- Riskaptit och Key Risk Indicators (KRIer)
- Återställningsscenarion i kontinuitetsplan

Testobjekt

Bolaget ska ha en förteckning över testobjekt som specificerar

- objektstyp (process, system, kontroll, leverantör, återställningskedja)
- koppling till kritisk/viktig funktion
- kritikalitet
- risknivå
- prioritering och rekommenderad testtyp(er)

- utlagd verksamhet (ja/nej)

Prioriteringen ska baseras på den sammanlagda bedömningen av kritikalitet och risknivå så att testobjekt med hög kritikalitet och hög risknivå testas oftare och med mer rigorösa metoder än ett med låg kritikalitet och obetydlig risknivå.

Bedömning av kritikalitet utgår från i vilken utsträckning testobjektet stödjer en kritisk/viktig funktion eller inte och graderas i

- Hög (stödjer kritisk/viktig funktion)
- Medel (väsentlig men stödjer ej kritisk/viktig funktion)
- Låg (stödfunktion)

Risknivå utgår från bedömd risk i riskregistret och graderas i fyra steg i enlighet med bolagets anvisning för riskhantering

- Obetydlig/lindrig
- Kännbar/betydande
- Allvarlig
- Mycket allvarlig

Testtyper

Varje test ska motiveras av ett verifieringsbehov. Baserat på detta delas tester in i följande testtyper.

- **Kontrolltest/Egenkontroll**. Verifiering av att kontroller fungerar i normalläge. Används för att bekräfta att en definierad kontrollpunkt faktiskt utförs och ger avsett resultat. Källa är egenkontrollplanen, utförs i första linjen och granskas av andra linjen. I testtypen ingår även funktionstest i samband med återstart efter planerade händelser, eller vid större versionsförändringar i programvara.
- **Sårbarhetsscanning**. Verifiering av att kända sårbarheter identifieras och åtgärdas. Används löpande för att fånga tekniska svagheter innan de utnyttjas. Frekvensen styrs av hur snabbt hotbilden förändras och hur kritiska systemen är.
- **Penetrationstest**. Verifiering av att systemen tål ett aktivt angrepp. Används för att testa om en angripare faktiskt kan ta sig in, inte bara om kända sårbarheter finns. Kräver mer resurser och genomförs mer sällan — men är obligatoriskt för system som stödjer kritiska eller viktiga funktioner.
- **Återställningstest**. Verifiering av att bolaget kan återställa efter ett avbrott inom RTO/RPO. Direkt kopplat till kontinuitetsplanen och definierade återställningsmål. Testet är godkänt om och bara om återställning sker inom RTO och utan att förlora mer data än RPO tillåter.
- **Kontinuitetsövning**. Verifiering av att organisationen fungerar vid en kris. Testar inte system utan roller och kommunikation. Visar om kontinuitetsplanen är känd, om rollerna är tydliga och om beslutsvägarna fungerar under press.
- **Leverantörsuppföljning och leverantörsrevision (inkl granskning av leverantörers testresultat).** Verifiering av att leverantörers säkerhetsnivå håller.

Tredjepartstester för kritiska/viktiga funktioner ska innehålla följande:

- Resultat från test av återställning och kontinuitetsövning som berör den levererade tjänsten
- Sammanfattning av penetrationstester och hantering av kritiska fynd
- Öppna kritiska fynd som påverkar tjänsten
- Incidenthistorik
- Översikt av omfattning av testad beredskap för utträde och data-portabilitet

Testfrekvens

Testfrekvens ska styras av följande tre faktorer.

- **Risknivå**: Högriskfunktioner testas oftare. En kritisk eller viktig funktion med Oacceptabel risknivå i riskregistret ska testas med högre frekvens än en funktion som inte är kritisk eller viktig med Acceptabel risk.
- **KRI-status**: Om en KRI som relaterar till ett testobjekt tenderar att vara gul — dvs. nära gränsen för toleransen — är det en signal om att testfrekvensen bör öka.
- **Förändringstakt**: System och processer som förändras ofta (nya versioner, ny konfiguration, ny leverantör) behöver testas oftare än stabila miljöer. Varje väsentlig förändring är ett implicit testbehov.

Resultatet från tester rapporteras i bolagets forum för intern styrning och kontroll (ISK). En sammanlagd rapportering sker varje kvartal i bolagets verksamhetsrapport.

Godkännandekriterier

Godkännandekriterier ska alltid vara definierade innan test genomförs. Det innebär att följande alltid ska vara definierat innan test genomförs:

- **Vad testas**: Exakt vilket system, process eller kontroll.
- **Testad egenskap**: Tillgänglighet, konfidentialitet, riktighet, återställningsförmåga eller kontrolleffektivitet.
- **Godkännandekriterium**: Det mätbara resultatet som krävs för godkänt.
    - För återställningstest - återställningstider (RTO och RPO), “Systemet är återställt inom [X] timmar och dataförlusten överstiger inte [Y] timmar.”
    - För kontrolltest/egenkontroll - om riskreducerande kontroller har avsedd effekt
    - Om störningar leder till att riskaptiten överskrids eller inte
    - Om återställningsscenarion fungerar
- **Källa**: Var godkännandekriteriet kommer från — RTO/RPO från BIA, överskridna toleranser från riskaptit, kontrollkrav från egenkontrollplanen.

Dokumentation

Bolagets testprogram ska innehålla följande:

En **testkatalog** med alla planerade tester, deras frekvens, ansvarig, godkännandekriterium och källdokument (riskregister-ID, Kritisk/viktig funktion-ID, KRI-ID).

En **testkalender** med planerade datum för innevarande år.

En **findings-logg** där alla avvikelser och fynd från tester registreras med klassning (Kritisk/Hög/Medel), åtgärdsplan, ansvarig och status. Fynd i loggen ska hanteras som risk i bolagets riskregister.

En **testhistorik** med resultaten från genomförda tester.

En **beslutslogg** med beslutade frekvensändringar, acceptansbeslut och godkända avvikelser.

Dokumentation över **tredjepartstester**.

Rapportering och återkoppling

Testresultaten ska uppdatera den riskbild som motiverade testprogrammet från början.

Ett fynd som bekräftar en känd risk ska resultera i att risknivån i riskregistret uppgraderas om kontrollen visade sig vara ineffektiv — och att riskacceptansen omprövas.

Ett fynd som avslöjar en okänd risk ska resultera i att en ny risk läggs till i riskregistret och att testprogrammet utvidgas om det finns fler okända risker i samma område.

Ett test som ger godkänt resultat är inte ett skäl att sluta testa — men det är ett underlag för att motivera att frekvensen behålls eller minskas om riskbilden förändrats i positiv riktning.

En förändring i riskbilden — t.ex. en ny leverantör, ett nytt system eller en ny incident — ska trigga en genomgång av testprogrammet för att säkerställa att omfattningen av testprogrammet fortfarande är korrekt.

Överskriden riskaptit som är beslutad av styrelse ska rapporteras vid kommande styrelsemöte.

Oberoende

För att säkerställa oberoende avseende testning ska bolaget undvika att den som utför testet också är den som:

- Designat eller ansvarar för det som testas
- Har ett särskilt intresse av att testresultatet blir bra
- Saknar förmåga att bedöma om resultatet är tillräckligt

Begrepp	Definition (förenklad)	Källor
Konfidentialitet	Egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer	Termbanken, MCF
Riktighet (integritet hos information)	Egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring	Termbanken, MCF
Tillgänglighet	Egenskap hos informationstillgång som innebär att den är åtkomlig och användbar inom förväntad tid och omfattning	Termbanken, MCF
IKT	Informations- och kommunikationsteknik/-teknologi	Termbanken, MCF
BIA	Business Impacts Analysis. Strukturerad analys som identifierar kritiska processer och bedömer konsekvenserna av avbrott över tid. Utgör grunden för kontinuitetsplanering	ISO 22317
RTO	Recovery Time Objective. Den maximalt accepabla tid inom vilken en process eller tjänst måste vara återställd efter ett avbrott, för att undvika oaccetabla konsekvenser.	ISO 22301
RPO	Recovery Point Objective. Den maximalt acceptabla mängd data som får gå förlorad vid ett avbrott, uttryckt som en tidpunkt bakåt från avbrottet - dvs hur gammal en återställd datamängd får vara.	ISO 22301
KRI	Key Risk Indicator. Mätbart värde som ger tidig signal om ökad riskexponering innan en händelse inträffar. Används för löpande riskövervakning mot fastställda tröskelvärden.	ISO 31000