Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2026-09-07
Ärendenummer FGL-2026-00004

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

Internrevisionsfunktionens granskningsrapport 1 2026

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar granskningsrapport 1 från internrevisionen 2026.

Sammanfattning

Internrevisionen har under årets första granskning granskat bolagets ramverk för IKT-riskhantering med utgångs punkt i DORA-kraven avseende policys, roller och ansvar samt processer för identifiering, bedömning, hantering och rapportering av IKT-risker, inklusive styrning och integrering i den övergripande riskhanteringen.

Internrevisionen rekommenderar bolaget att säkerställa att etablerade KRI:er följs upp löpande samt att en strukturerad och formell rapporteringsprocess för IKT-risker implementeras.

Bedömning ur ekonomisk dimension

Internrevisionens granskning viktig ur ett ekonomiskt perspektiv då den syftar till att säkerställa långsiktig ekonomisk hållbarhet i bolaget, vilket i sin tur syftar till att ge Göteborgs stad en långsiktigt hållbar kostnadseffektiv riskhantering.

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

Internrevisionsrapport 2026:1 – Granskning av DORA

Beskrivning av ärendet

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

För att ta del av internrevisionens rapport hänvisas till bilaga 1.

Enligt Försäkringsrörelselagen 10 kap, 4§ ska försäkringsföretag ha fyra centrala funktioner. Dessa utgörs av regelefterlevnadsfunktionen, riskhanteringsfunktionen, aktuariefunktionen och internrevisionsfunktionen. Dessa kontrollfunktioner ska utvärdera systemet för internrevision, regelefterlevnad och riskhantering. Funktionerna ska även utvärdera andra delar av företagsstyrningssystemet och rapportera resultatet och lämna rekommendationer efter utvärdering till företagets styrelse.

Internrevisionen har under årets första granskning granskat bolagets ramverk för IKT-riskhantering med utgångs punkt i DORA-kraven avseende policys, roller och ansvar samt processer för identifiering, bedömning, hantering och rapportering av IKT-risker, inklusive styrning och integrering i den övergripande riskhanteringen.

Internrevisionens sammanfattande bedömning är att förbättringar rekommenderas. De har identifierat en lågprioriterad iakttagelse avseende den praktiska implementeringen av ramverket, vilken avser att någon löpande uppföljning av fastställda KRI:er ännu inte implementerats samt att det saknas en strukturerad och formell rapportering av IKT-risker i enlighet med riktlinjen för säkerhet.

Internrevisionsfunktionen lämnar följande rekommendation till bolaget utifrån granskningen:

- Bolaget rekommenderas att säkerställa att etablerade KRI:er följs upp löpande samt att en strukturerad och formell rapporteringsprocess för IKT-risker implementeras, där uppföljning och rapportering sker regelbundet till vd och styrelse i enlighet med riktlinjen för säkerhet.

Enligt bolagets riktlinje för internrevisionsfunktionen ska resultat och eventuella rekommendationer rapporteras till styrelsen.

Bolagets bedömning

Det är bolagets bedömning att rapporten är relevant för bolaget och att lämnade iakttagelser ytterligare kan förbättra bolagets arbete kring DORA-förordningen.

Petra Willquist Rönnäng	Anders Jonasson
Bolagscontroller	VD

Granskning av DORA

Internrevisionsrapport 2026:1

Försäkrings AB Göta Lejon

KPMG AB

21 augusti 2026

Till styrelse

1. Sammanfattande bedömning

Vi har genomfört en granskning av bolagets ramverk för IKT-riskhantering med utgångspunkt i DORA-kraven avseende policys, roller och ansvar samt processer för identifiering, bedömning, hantering och rapportering av IKT-risker, inklusive styrning och integrering i den övergripande riskhanteringen.

Vår sammanfattande bedömning är att förbättringar rekommenderas. Vi har identifierat en lågprioriterad iakttagelse avseende den praktiska implementeringen av ramverket, vilken avser att någon löpande uppföljning av fastställda KRI:er ännu inte implementerats samt att det saknas en strukturerad och formell rapportering av IKT-risker i enlighet med riktlinjen för säkerhet. Bolaget har uppgett att båda delar kommer att etableras framgent.

Bolaget har etablerat ett i huvudsak ändamålsenligt ramverk för styrning och hantering av IKT-risker, med roller och ansvar samt relevanta styrande dokument. Vidare ser vi positivt på att bolaget genomför en årlig översyn av IKT-riskhanteringsramverket.

Rapporten och dess iakttagelser har klassificerats i enlighet med kriterierna i Bilaga 1.

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

© 2026 KPMG AB. All rights reserved.
Document classification: KPMG Confidential

2. Inledning

2.1 Syfte

Syftet med granskningen har varit att granska bolagets ramverk för IKT-riskhantering med utgångspunkt i DORA-kraven avseende policys, roller och ansvar samt processer för identifiering, bedömning, hantering och rapportering av IKT-risker, inklusive styrning och integrering i den övergripande riskhanteringen.

Granskningen har genomförts i enlighet med fastställd internrevisionsplan för 2026.

2.2 Genomförande

Under granskningen har vi tagit del av relevanta underlag, och de dokumenten som behandlats i granskningen framgår av Bilaga 2.

Vi har genomfört en intervju via Microsoft Teams med bolagets Säkerhetschef och Ekonomichef den 10 juni.

Granskning har genomförts av Matilda Lindqvist och Johannes Johansson under juni 2026. Rapporten har kvalitetssäkrats av My Backman.

© 2026 KPMG AB. All rights reserved.
Document classification: KPMG Confidential

3. Iakttagelser

3.1 Återstående implementering av IKT-riskhanteringsramverket

Låg

Bolaget har ett etablerat ramverk för IKT-riskhantering, men har inte fullt ut implementerat samtliga delar av ramverket i linje med fastställda styrande dokument.

- Bolaget har definierat KRI:er för IKT- och informationssäkerhetsrisker i syfte att möjliggöra löpande och spårbar uppföljning av den digitala operativa motståndskraften, i enlighet med riktlinjen för säkerhet. Någon etablerad och dokumenterad uppföljning av dessa har dock inte implementerats i praktiken. Bolaget har uppgett att kvartalsvis uppföljning planeras införas under hösten.

- Det saknas en strukturerad och formaliserad rapportering av IKT-risker. I riktlinjen för säkerhet anges att Riskhanteringsfunktionen ska övervaka IKT-risker löpande samt rapportera dessa till VD och styrelse. Denna rapportering har ännu inte etablerats. Bolaget har uppgett att sådan rapportering kommer att etableras framgent.

Risk

Risk för att IKT-risker inte identifieras, övervakas och eskaleras i tid, vilket kan försämra bolaget digitala motståndskraft samt begränsa ledningens och styrelsens möjlighet att vidta effektiva och välgrundade åtgärder i tid.

Rekommendation

Vi rekommenderar att bolaget säkerställer att etablerade KRI:er följs upp löpande samt att en strukturerad och formell rapporteringsprocess för IKT-risker implementeras, där uppföljning och rapportering sker regelbundet till vd och styrelse i enlighet med riktlinjen för säkerhet.

Verksamhetens svar

Beslutade åtgärder: Bolaget avser att genomföra åtgärden

Ansvarig: Petra Willquist

Deadline: 2026-12-31

KPMG AB

Matilda Lindqvist	Johannes Johansson
Internrevisor	Internrevisor

© 2026 KPMG AB, a Swedish limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Bilaga 1 Kriterier för utvärdering

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

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

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

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

© 2026 KPMG AB. All rights reserved.
Document classification: KPMG Confidential

Bilaga 2 Dokument som ingått i granskningen

Dokument

Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll (2025-11-10)

Försäkrings AB Göta Lejons riktlinje för riskhanteringsfunktionen (2025-05-27)

Försäkrings AB Göta Lejons riktlinje för säkerhet (2026-04-01)

Försäkrings AB Göta Lejons anvisning för riskhantering (2026-01-09)

Försäkrings AB Göta Lejons rutin för specifik riskbedömning av äldre IKT-system (2026-01-08)

Rapport IKT-riskhantering

Riskaptit informationssäkerhet

Riskaptit och KRI-register GL (260522)

Riskbedömning infosäk (Gota Lejon)

© 2026 KPMG AB. All rights reserved.
Document classification: KPMG Confidential