2025.02 - IKT Tredjepartsrisker (DORA)

Från: Internrevisionen, Grant Thornton Sweden AB
Till: Styrelse & VD på S:t Eriks Försäkrings AB

2026-03-04

CONFIDENTIAL/FOR INTERNAL USE ONLY

Inledning och bakgrund

Bakgrund till granskningen

EU:s förordning om digital operativ motståndskraft för finanssektorn (DORA) trädde i kraft i januari 2023 och har som primärt syfte att konsolidera nuvarande reglering och höja kraven inom IKT-riskhantering. Drivande faktorer till regelverket är bland annat ökad digitalisering och sammankoppling, där finansiella aktörer blir alltmer beroende av informations- och kommunikationsteknik (IKT). Detta skapar möjligheter men medför också ökade risker.

S:t Erik Försäkrings AB (”SEF” eller ”Bolaget”) omfattas av DORA och har att säkerställa att Bolaget följer regelverket, vilket började tillämpas i januari 2025. Ett centralt område i DORA är hantering av IKT-tredjepartsrisker.

Internrevisionen har granskat och tagit del av central dokumentation inom DORA:s ramverk avseende IKT-tredjepartsrisker. Detta i form av t.ex. styrdokument kopplade till IKT-tredjepartsrisker och det informationsregister som ska upprätthållas avseende avtal med tredjeparter som tillhandahåller IKT-tjänster. Internrevisionen har även hållit genomgångar med relevant personal på Bolaget för att förstå Bolagets processer och rutiner kopplat till IKT-tredjepartshantering och informationsregistret.

Syfte

Syftet med aktuella granskningen har varit att utvärdera hur Bolaget arbetar med hantering av IKT-tredjepartsrisker utifrån de krav som DORA ställer.

Omfattning

1. Styrdokument
2. Informationsregister
3. Rutiner och processer

Avgränsningar

Granskningen har inte omfattat någon uttömmande bedömning av Bolagets avtal med leverantörer av IKT-tjänster mot DORA:s ramverk. Övriga kapitel i DORA utöver kapitel 5 som rör hantering av IKT-tredjepartsrisker har endast berörts i den mån det har varit relevant och haft en tydlig koppling till IKT-tredjepartsriskhantering.

Regulatorisk kontext

1. Europaparlamentets och Rådets förordning (EU) 2022/2554 (DORA)
2. Kompletterande tekniska standarder till DORA av relevans för IKT-tredjepartsrisker

Sammanfattning av resultat

Internrevisionen har genomfört en granskning av Bolagets ramverk kopplat till IKT-tredjepartshantering. Granskningen visar att Bolaget har etablerat en styrning och intern kontroll i förhållande till IKT-tredjepartshantering som i flera avseenden framstår vara välfungerande. Samtidigt bedömer Internrevisionen att det finns ett visst förbättringsbehov i vissa avseenden. Den sammantagna bedömningen efter granskningen är att det föreligger ett mindre Förbättringsbehov. För att förbättra intern styrning och kontroll inom det granskade området rekommenderas åtgärder i linje med Internrevisionens rekommendationer. Internrevisionen lämnar fyra (4) rekommendationer baserat på iakttagelser som gjorts. En (1) av dessa bedöms vara av medium risk-karaktär och tre (3) av låg risk-karaktär.

#	Fokusområde	Rekommendation	Risknivå
2025.02.1	1. Styrdokument	Bolaget bör säkerställa ett tydligt dokumenterat ansvar för den funktion som inrättats för att övervaka de arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster eller den medlem av den verkställande ledningen som utsetts till ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation	Låg
2025.02.2	1. Styrdokument	Bolaget bör se över sina riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och säkerställa att dessa svarar mot kraven i RTS 2024/1773	Medium
2025.02.3	2. Informationsregister	Bolaget bör förtydliga sina Riktlinjer för Uppdragsavtal vad gäller rutiner och processer kring informationsregistret samt ansvar och roller för informationsregistret och beredning av beslut avseende kritiska och viktiga funktioner	Låg
2025.02.4	3. Rutiner och processer	Bolaget bör säkerställa att det tydligt i Bolagets dokumentation framgår vilka IKT-tillgångar och informationstillgångar som stödjer respektive identifierad affärsfunktion	Låg

2025.02.1 Bolaget bör säkerställa ett tydligt dokumenterat ansvar för den funktion som inrättats för att övervaka de arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster eller den medlem av den verkställande ledningen som utsetts till ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation

Låg

1. Styrdokument

Kriterium	**Artikel 5.3 Förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA)** *Andra finansiella entiteter än mikroföretag ska inrätta en funktion för att övervaka de arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster, eller utse en medlem av den verkställande ledningen som ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation.* **Artikel 3.5 Förordning (EU) 2024/1773 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 (DORA RTS 2024/1773)** *I riktlinjerna ska det tydligt anges vilken roll i eller vilken medlem av den högre ledningen som ansvarar för att övervaka de relevanta avtalsarrangemangen. Riktlinjerna ska ange hur den rollen i eller medlemmen av den högre ledningen ska samarbeta med kontrollfunktionerna och fastställas rapporteringsvägar till ledningsorganet, inbegripet vilken typ av information som ska rapporteras och vilka dokument som ska tillhandahållas. Det ska också anges hur ofta sådan rapportering ska ske.*
Observation	Det följer av artikel 5.3 i DORA att Bolaget har att inrätta en funktion för att övervaka de arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster, eller utse en medlem av den verkställande ledningen som ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation. Vid granskning av Bolagets styrdokumentation avseende tredjepartsriskhantering har Internrevisionen noterat att det inte tydligt framgår vilken funktion eller vem i ledningen som fått ansvaret som föreskrivs i artikel 5.3 i DORA samt vad detta ansvar innebär. Baserat på vad som har framgått under genomförda intervjuer uppfattar Internrevisionen dock att Bolagets chefsjurist kan ha fått detta ansvar.
Risk	Vad som nämnts ovan kan vara förknippat med en risk för en otydlig ansvarsfördelning och otydliga roller samt bristande styrning av Bolagets IKT-tredjepartsrisker. Detta kan leda till att uppföljning, rapportering och kontrollaktiviteter inte genomförs konsekvent eller i enlighet med DORA:s krav.
Rekommendation	Internrevisionen rekommenderar att Bolaget ser över styrdokumentation och säkerställer att det finns ett tydligt dokumenterat ansvar för den roll som föreskrivs i artikel 5.3 i DORA. Av styrdokumentation bör framgå: • vilken funktion eller vilken medlem av ledningen som ansvarar för att övervaka relevanta avtalsarrangemang, • hur funktionen i eller medlemmen av ledningen ska samarbeta med kontrollfunktionerna, • rapporteringsvägar från funktionen/medlemmen av ledningen till styrelsen, inbegripet vilken typ av information som ska rapporteras och vilka dokument som ska tillhandahållas, och • hur ofta rapportering ska ske.
Ledningens åtgärdsplan:	En person i ledningen kommer att utses och IKT-riktlinje uppdateras med en ännu tydligare beskrivning av process för uppföljning och rapportering avseende arrangemang ingångna med tredjepartsleverantörer. Processen kommer även innefatta en tydligare beskrivning hur dessa arrangemang övervakas löpande.
Ansvarig och deadline:	Bolagsjurist, Q4 2026.

2025.02.2 Bolaget bör se över sina riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och säkerställa att dessa svarar mot kraven i RTS 2024/1773

Medium

1. Styrdokument

Kriterium	**Artikel 28.2 Förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA)** *Som en del av sin IKT-riskhanteringsram ska andra finansiella entiteter än de enheter som avses i artikel 16.1 första stycket och mikroföretag anta och regelbundet se över en strategi för IKT-tredjepartsrisk, med beaktande av den strategi för flera olika leverantörer som avses i artikel 6.9 i tillämpliga fall. Strategin för IKT-tredjepartsrisk ska omfatta riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster och ska tillämpas individuellt och, i förekommande fall, på undergrupps- och gruppnivå. Ledningsorganet ska, baserat på en bedömning av den finansiella entitetens allmänna riskprofil samt omfattningen av och komplexiteten i entitetens affärstjänster, regelbundet se över de risker som har identifierats vad gäller kontraktsmässiga arrangemang för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner.* **Artikel 1-10 Förordning (EU) 2024/1773 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 (DORA RTS 2024/1773)**
Observation	Bolaget har *Riktlinjer för IKT* samt *Riktlinjer för Uppdragsavtal* som tillsammans adresserar vissa krav i DORA och RTS 2024/1773 (kompletterande teknisk standard till DORA) på en övergripande nivå. Internrevisionen har dock vid granskning av riktlinjerna noterat att de inte fullt ut uppfyller kraven på en strategi för IKT-tredjepartsrisk som omfattar riktlinjer för användning av IKT-tjänster som stöder kritiska eller viktiga funktioner enligt artikel 28.2 i DORA och de kompletterande kraven i RTS 2024/1773. Nedan följer icke uttömmande exempel på iakttagna områden där nuvarande styrdokumentation inte bedöms uppfylla gällande krav i DORA och tillhörande teknisk standard: • Bolagets *Riktlinjer för IKT* och *Riktlinjer för Uppdragsavtal* adresserar inte på ett tydligt sätt leverantörers geografiska lokalisering och plats från vilken IKT-tjänster tillhandahållas och uppgifter behandlas (artikel 1 DORA RTS 2024/1773). • Bolagets *Riktlinjer för IKT* och *Riktlinjer för Uppdragsavtal* innehåller vissa övergripande beskrivningar av avslut och uppsägning av uppdrag. I riktlinjerna framgår däremot inte på ett tydligt sätt vilka regler, ansvarsområden och processer som ska gälla för alla faser i livscykeln. Exempelvis anges inte på ett tydligt sätt hur exitplaner ska utformas, såsom kravet på att beakta scenarier som oförutsedda och ihållande driftstopp vid upprättandet (artikel 4 och artikel 10 i DORA RTS 2024/1773). • Det framgår inte tydligt av Bolagets *Riktlinjer för IKT* och *Riktlinjer för Uppdragsavtal* att den riskanalys som ska genomföras och som ligger till grund för styrelsens beslut om ingång av nya uppdragsavtal ska beakta rättsliga risker, anseenderisker, platsrelaterade risker, leverantörens geografiska placering och IKT-koncentrationsrisker (artikel 5 RTS 2024/1773). • Minimikraven som Bolagets *Riktlinjer för IKT* och *Riktlinjer för Uppdragsavtal* uppställer för att en verksamhet ska bedrivas av en extern part genom uppdragsavtal omfattar exempelvis inga krav på att leverantören ska kunna följa teknisk utveckling och implementera ledande IKT-säkerhetsmetoder (artikel 6 RTS 2024/1773). • Bolagets *Riktlinjer för IKT* och *Riktlinjer för Uppdragsavtal* innehåller krav på identifiering och utredning av potentiella intressekonflikter men det framgår inte på ett tydligt sätt hur Bolaget ska hantera IKT-tjänster som stöder kritiska eller viktiga funktioner som tillhandahålls av koncerninterna IKT-tjänsteleverantörer (artikel 7 RTS 2024/1773). • Bolagets *Riktlinjer för IKT* och *Riktlinjer för Uppdragsavtal* anger inte uttryckligen krav på rätt till information, inspektioner, revisioner eller IKT-tester i avtal (artikel 8.2 DORA RTS 2024/1773) och saknar information om att Bolaget inte får förlita sig enbart på tredjepartscertifieringar eller externa revisionsrapporter (artikel 8.3 RTS 2024/1773).
Risk	Vad som nämnts ovan kan vara förknippat med risk för bristande regelefterlevnad av DORA och tillhörande tekniska standarder. Det finns en risk att Bolagets dokumenterade ramverk beträffande IKT-tredjepartsriskhantering inte är tillräckligt tydligt i vissa avseenden.
Rekommendation	Internrevisionen rekommenderar att Bolaget ser över de styrdokument som svarar mot Bolagets riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och säkerställer att dessa innehåller alla delar som RTS 2024/1773 föreskriver ska inkluderas i riktlinjerna.

2025.02.2 Bolaget bör se över sina riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och säkerställa att dessa svarar mot kraven i RTS 2024/1773

Medium

1. Styrdokument

Ledningens åtgärdsplan:	• Bolagets riktlinjer och avtal ska vid behov ses över och justeras för att bättre återspegla hur Bolaget säkerställer geografisk lokalisering varifrån IKT-tjänster levereras. • Bolagets allmänt hållna exitstrategier kommer att förtydligas. • Bolagets beskrivning av riskanalys kommer att förtydligas. • Bolaget ska se över detta och komplettera riktlinjer och vid behov leverantörsavtal, med information om det som omnämns i rekommendationen. Observera att Bolaget kommer att följa upp detta mot bakgrund av proportionalitet, innebärande att kraven kommer ställas gentemot leverantörerna i förhållande till hur viktig den levererade tjänsten är för Bolagets verksamhet. • Bolaget ser det inte som att det uppstår specifika intressekonflikter enkom för att andra bolag i koncernen upphandlar tjänster som Bolaget därefter nyttjar. Bolaget ska dock se över interna riktlinjer avseende såväl de områden som ovan nämns, som interna riktlinjer för intressekonflikter för att se om detta behöver förtydligas eller utredas vidare. • Samtliga områden som nämns under denna punkt finns med i de leverantörsavtal som Bolaget ingått med leverantörer avseende IKT-tjänster. Bolaget avser dock följa upp om detta kan förtydligas än mer i Bolagets interna riktlinjer.
Ansvarig och deadline:	Bolagsjurist, Q4.

2025.02.3 Bolaget bör förtydliga sina Riktlinjer för Uppdragsavtal vad gäller rutiner och processer kring informationsregistret samt ansvar och roller för informationsregistret och beredning av beslut avseende kritiska och viktiga funktioner

Låg

2. Informationsregistret

Kriterium	**Artikel 28.3 Förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA)** *Som en del av sin IKT-riskhanteringsram ska finansiella entiteter upprätthålla och uppdatera ett register med information på entitetsnivå, undergrupps- och gruppnivå om alla kontraktsmässiga arrangemang som rör användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster.* *De kontraktsmässiga arrangemang som avses i första stycket ska dokumenteras på lämpligt sätt, varvid åtskillnad ska göras mellan de kontraktsmässiga arrangemang som omfattar kritiska eller viktiga funktioner och de som inte gör det.* *Finansiella entiteter ska minst en gång per år rapportera till de behöriga myndigheterna om antalet nya arrangemang för användningen av IKT-tjänster, kategorierna av tredjepartsleverantörer av IKT-tjänster, typen av kontraktsmässigt arrangemang och de IKT-tjänster och funktioner som tillhandahålls. […]* *Finansiella entiteter ska i god tid informera den behöriga myndigheten om eventuella planerade kontraktsmässiga arrangemang för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner samt när en funktion har blivit kritisk eller viktig.* **Artikel 4(e) Förordning (EU) 2024/1773 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 (DORA RTS 2024/1773)** *Riktlinjerna ska specificera kraven, inklusive reglerna, ansvarsområdena och processerna, för varje huvudfas i livscykeln för det kontraktsmässiga arrangemanget, som omfattar minst följande:* *e) Dokumentation och registerhållning, med beaktande av de krav avseende informationsregistret som fastställs i artikel 28.3 i förordning (EU) 2022/2554.*
Observation	Internrevisionen har granskat Bolagets styrdokumentation, inklusive *Riktlinjer för Uppdragsavtal* med särskilt fokus på den beskrivna processen för dokumentation av Bolagets IKT-register och rapportering av leverantörsavtal och uppdragsavtal avseende IKT-tjänster till Finansinspektionen och noterat följande: • *Riktlinjerna för Uppdragsavtal* anger att för det fall Bolaget ingår avtal avseende en ny IKT-tjänst ska detta dokumenteras i Bolagets IKT-register och rapporteras till Finansinspektionen med beaktande av artikel 28-32 i DORA (*Riktlinjer för Uppdragsavtal*, s. 9). De anger vidare att styrelsen ska besluta om vilka funktioner som är kritiska eller viktiga. Riktlinjerna är dock övergripande och innehåller inte information om att rapporteringen av informationsregistret ska göras minst årligen och omfatta antalet nya arrangemang för användningen av IKT-tjänster, kategorierna av tredjepartsleverantörer av IKT-tjänster, typen av kontraktsmässigt arrangemang och de IKT-tjänster och funktioner som tillhandahålls. Riktlinjerna innehåller vidare inte information om vem som ska rapportera in informationsregistret till Finansinspektionen. • Bolagets *Riktlinjer för Uppdragsavtal* anger att VD eller delegerad ska rapportera ”verksamhet som avser operativ verksamhet eller funktioner av väsentlig betydelse” till Finansinspektionen innan ett avtal träder i kraft (*Riktlinjer för Uppdragsavtal* sidan 9). Riktlinjerna och övrig granskad relevant styrdokumentation innehåller dock inte några krav på att informera Finansinspektionen om avtal avseende IKT-tjänster som stödjer kritiska eller viktiga funktioner.
Risk	Vad som nämnts ovan kan vara förknippat med en risk att dokumentationen av IKT-arrangemang inte blir fullständig eller tillräckligt strukturerad, vilket i sin tur kan påverka Bolagets förmåga att säkerställa att all information rapporteras korrekt och i enlighet med gällande krav. Vidare kan det finnas risk för otydligheter i ramverket kopplat till rapportering av informationsregistret.
Rekommendation	Internrevisionen rekommenderar att Bolaget i *Riktlinjer för Uppdragsavtal*: • Tydliggör att Bolaget minst årligen ska rapporterar antalet nya arrangemang för användningen av IKT-tjänster, kategorierna av tredjepartsleverantörer av IKT-tjänster, typen av kontraktsmässigt arrangemang och de IKT-tjänster och funktioner som tillhandahålls till Finansinspektionen. Bolaget rekommenderas även tydligare dokumentera vem som ska rapportera in informationsregistret. • Tydliggör att Bolaget ska informera Finansinspektionen om nya avtal för användning IKT-tjänster som stöder kritiska eller viktiga funktioner samt ev. befintliga avtal när en funktion har blivit kritisk eller viktig.
Ledningens åtgärdsplan:	Bolaget kommer att förtydliga vem som ska rapportera. Vad avser innehållet och när/hur rapportering sker finns i Riktlinje för uppdragsavtal en hänvisning till DORA. Bolaget ser inte behovet med att återge förordningstexten i riktlinjen och kommer låta hänvisningen till DORA stå kvar. Den som ansvarar för att rapportera kommer att vara väl insatt i reglerna så att förordningen uppfylls.
Ansvarig och deadline:	Bolagsjurist, Q4 2026.

2025.02.4 Bolaget bör säkerställa att det tydligt i Bolagets dokumentation framgår vilka IKT-tillgångar och informationstillgångar som stödjer respektive identifierad affärsfunktion

Låg

3. Rutiner och processer

Kriterium	**Artikel 8.1 Förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA)** *Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter identifiera, klassificera och på lämpligt sätt dokumentera alla IKT-stödda affärsfunktioner, roller och ansvarsområden, de informationstillgångar och IKT-tillgångar som stöder dessa funktioner och deras roller och beroenden i förhållande till IKT-risk. Finansiella entiteter ska vid behov, och minst en gång per år, granska lämpligheten i denna klassificering och i all relevant dokumentation.*
Observation	Bolaget har identifierat affärsfunktioner och dokumenterat dessa tillsammans med de avtal som är kopplade till respektive funktion. Bolaget har även tagit fram systemkartor som visar Bolagets IKT-tillgångar och informationstillgångar. Vidare har Bolaget upprättat avbrottsplaner, vilka i vissa fall indirekt visar vilka IKT-tillgångar och informationstillgångar som stödjer olika affärsfunktioner. Internrevisionen har dock noterat att det av Bolagets dokumentation inte på ett tydligt och direkt sätt framgår vilka specifika IKT-tillgångar och informationstillgångar som stödjer respektive identifierad affärsfunktion, i enlighet med kravet i artikel 8.1 DORA.
Risk	Vad som nämnts ovan kan vara förknippat med en risk att Bolagets dokumentation av IKT- och informationstillgångar samt affärsfunktioner är otydlig vilket kan medföra en risk för att samband och beroenden mellan funktioner och de tillgångar som stödjer dem inte fullt ut förstås eller är korrekt kartlagda. Detta kan i sin tur innebära en risk för att Bolagets förmåga att upprätthålla affärskontinuitet vid incidenter eller avbrott påverkas negativt.
Rekommendation	Internrevisionen rekommenderar att Bolaget förtydligar dokumentationen så att det tydligt kan utläsas vilka IKT-tillgångar och informationstillgångar som stödjer respektive identifierad affärsfunktion.
Ledningens åtgärdsplan:	Bolaget kommer att förtydliga detta i IKT-riktlinjen så det blir mer överskådligt.
Ansvarig och deadline:	Bolagsjurist, Q4 2026.

Appendix A - Granskningens tillvägagångssätt och metodik

Intervjuer

Internrevisionen har inom ramen för granskningen utfört intervju med Johan Grenefalk, regelefterlevnadsfunktionen och Johan Gagner, IT-ansvarig.

Dokumentgranskning

Internrevisionen har med ett riskbaserat selektivt tillvägagångsätt granskat ändamålsenlighet och efterlevnad av styrdokument, rutinbeskrivningar och andra relevanta interna dokument. Se 'Appendix C – Mottagna dokument' för information om erhållna dokument.

Avgränsningar

Granskningen har genomförts med ett riskbaserat tillvägagångssätt, vilket innebär att ingen uttömmande granskning har gjorts av alla aspekter som rör de områden som omfattas. De resultat som presenteras är vägledande och en fördjupad granskning kan vara nödvändig för att närmare kunna bedöma risker och konsekvenser.

Bedömningskriterier

Alla utfärdade observationer klassificeras i enlighet med följande bedömningsskala Låg, Medium, Hög, Mycket hög.

En sammanfattande bedömning av det granskade området görs i enlighet med skalan Tillfredsställande, Förbättringsbehov, Väsentliga förbättringsbehov och Otillfredsställande.

Se Appendix B för ytterligare beskrivning av 'Gradering av observationer och rapporter'.

Appendix B – Gradering av observationer och rapporter

Granskningsrapport

Internrevisionen bedömer intern kontroll och styrning inom det granskade området som “Tillfredställande”, “Förbättringsbehov”, ”Väsentliga förbättringsbehov”, eller “Otillfredsställande” utifrån följande:

Otillfredsställande

Väsentliga förbättringsbehov

Förbättringsbehov

Tillfredsställande

Varje observation tilldelas en av följande risknivåer; låg, medium, hög eller mycket hög risknivå:

Observationer

Risknivå	Kriterium
Mycket hög	Implicerar kritisk brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en mycket hög residual risk, eftersom bristen kan leda till kritisk ekonomisk förlust, ineffektivitet och / eller offentlig eller juridisk inverkan. Ledningen bör adressera bristen genom att vidta åtgärder omedelbart och adressera den bakomliggande orsaken till bristen.
Hög	Implicerar väsentlig brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en hög residual risk, eftersom bristen kan leda till väsentlig ekonomisk förlust, ineffektivitet och / eller offentlig eller rättslig inverkan. Ledningen bör adressera bristen genom att snarast vidta åtgärder.
Medium	Implicerar ett utvecklingsområde / betydande brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad som indikerar en medium residual risk som ensam, eller i kombination med andra brister, kan påverka funktionaliteten / integriteten hos system, processer och / eller kontroller, leda till anmärkningar från tillsynsmyndigheter alternativt indikera betydande potential för effektivisering. Ledningen bör adressera bristen genom att vidta åtgärder inom en rimlig tidsram.
Låg	Implicerar ett mindre utvecklingsområde / mindre brist inom styrning, intern kontroll, riskhantering eller regelefterlevnad och som har en låg residual risk av kritisk påverkan på system, processer eller kontroller, men indikerar potentiell förbättring för effektiviteten i processer och / eller kontroller. Ledningen bör adressera bristen inom ramen för den dagliga verksamheten.

Appendix C – Mottagna Dokument

- Avtal i registret
- FUNKTIOER
- IKT-riktlinje 250312
- Insman 2022
- IT Avbrottsplan 250226
- IT Avbrottsplan Bilagor
- Riktlinje för uppdragsavtal 250523
- FUNKTIONER m process
- iFACTS subcontractors
- Instruktion för riskbaserad kontraktsuppföljning 251219
- riktlinje-for-informationssakerhet
- tillampningsanvisning-informationssakerhet-v-1-3
- 2025-YEAR-DORA-IND-22067

Om du har några frågor om denna rapport eller dess innehåll, vänligen kontakta:

Louise Wennström

Senior Manager Advisory
T +46 (0) 73 82 32 494

E louise.wennstrom@se.gt.com

Grant Thornton