Rapport om översyn av IKT-riskhanteringsram

DORA artikel 6.5

Finansiell entitet	Försäkrings AB Göta Lejon
Organisationsnummer	516401-8185
Koncern	Del av Göteborgs Stadshus AB, org.nr 556537- 0888
Översynsperiod (start–slut)	[ÅÅÅÅ-MM-DD] – [ÅÅÅÅ-MM-DD]
Rapportdatum	[ÅÅÅÅ-MM-DD]
Klassificering	Sekretess enligt OSL 18:13

Godkännande

Godkänd av	
Godkännandedatum	[ÅÅÅÅ-MM-DD]
Giltighet	[Gäller till nästa översyn/annan regel]

Versionshantering

Datum	Version	Beskrivning av ändring	Ändrat av

Innehåll

1 Inledning och sammanfattning 3

1.1 Ledningssammanfattning 3

1.2 Verksamhets- och kontextbeskrivning 3

2 Översynens bakgrund, skäl och metod 4

2.1 Skäl till översyn 4

2.2 Tidsperiod och omfattning 5

2.3 Ansvarig funktion och deltagare 5

2.4 Källor som använts vid utarbetande av rapporten 5

3 Förändringar i IKT-riskhanteringsramen sedan föregående översyn 6

4 Resultat: brister, svagheter och gap-analys 6

4.1 Sammanfattning av fynd 7

4.2 Bedömning av kontrollernas effektivitet 7

5 IKT-incidenter 7

6 Åtgärdsplan 8

6.1 Åtgärder som inte genomförs (residualrisk) 10

7 Planerade vidareutvecklingar 10

8 Slutsatser 10

9 Historik och uppföljning av tidigare översyner 11

1 Inledning och sammanfattning

Syftet med denna rapport är att dokumentera översynen av organisationens IKT-riskhanteringsram och att kunna överlämna rapporten till behörig myndighet på begäran enligt DORA artikel 6.5. Rapporten ska vara sökbar i elektroniskt format och stödjas av spårbar evidens.

Rapporten är utformad i enlighet med RTS 2024/1774 artikel 27.

Rapporten ska godkännas av vd. Rapporten diarieförs i samband med godkännande.

1.1 Ledningssammanfattning

> I ledningssammanfattningen ska det finnas en sammanfattning av de åtgärder som vidtagits för att avhjälpa identifierade svagheter, brister och luckor (punkt 5 nedan)

- Övergripande bedömning av IKT-riskprofil, nuläge och kommande: [Fyll i]
- Hotbild: [Fyll i]
- Kontrollernas effektivitet: [Fyll i]
- Säkerhetsstatus: [Fyll i]
- Största identifierade risker och prioriterade åtgärder: [Fyll i]
- Slutsats: [Fyll i]

1.2 Verksamhets- och kontextbeskrivning

xxx

> Beskriv organisationens verksamhet (art, omfattning, komplexitet), organisation och viktiga beroenden. Inkludera kritiska/”viktiga” funktioner samt konsekvenser vid total/försvårad förlust av IKT-tjänster. Beskriv även beroenden kopplade till utlagd verksamhet och tredjepartsleverantörer.
>
> Det ska finnas ett avsnitt som ”beskriver bakgrunden till rapporten med avseende på karaktären på, omfattningen av och komplexiteten i den finansiella entitetens tjänster, verksamhet och insatser, den finansiella entitetens organisation, identifierade kritiska funktioner, strategi, större pågående projekt eller aktiviteter, relationer och beroende av interna och utkontrakterade IKT-tjänster och IKT-system eller de konsekvenser som en total förlust eller allvarlig försämring av sådana system skulle få med avseende

på kritiska eller viktiga funktioner och marknadseffektivitet”

- Uppdrag, strategi och tjänster: [Fyll i]
- Kritiska funktioner (lista): [Fyll i]
- Viktiga IKT-tillgångar/tjänster och beroenden (inkl. tredjepartsleverantörer): [Fyll i]
- Större förändringar i riskhanteringsramen sedan föregående rapport: [Fyll i]

2 Översynens bakgrund, skäl och metod

2.1 Skäl till översyn

☐ Årlig översyn

☐ Efter större förändring

☐ Efter IKT-incident(er)

☐ Efter internrevision/extern revision

☐ Efter testning av operativ digital motståndskraft

☐ På grund av tillsynsinstruktion

Beskrivning: [Fyll i]

OBS!

Om översynen initierades till följd av
- tillsynsinstruktioner
- slutsatser från testning av digital operativ motståndskraft
- revisionsprocesser

så ska rapporten innehålla uttryckliga hänvisningar till sådana instruktioner eller slutsatser, vilket gör det möjligt att identifiera skälet till att översynen initierades.

Om översynen initierades med anledning av IKT-relaterade incidenter ska rapporten innehålla en

förteckning över alla IKT-relaterade incidenter med en analys av grundorsaken till respektive incident.

2.2 Tidsperiod och omfattning

- Översynens period (start–slut): [Fyll i]
- Omfattning (processer, system, enheter, leverantörer, utlagd verksamhet): [Fyll i]
- Avgränsningar och motivering: [Fyll i]

2.3 Ansvarig funktion och deltagare

[Redigera förteckning nedan]

Funktion/Roll	Namn	Ansvar i översynen
Säkerhetschef	[Fyll i]	Övergripande ansvarig
IT-strateg	[Fyll i]	Underlag, åtgärder
Riskansvarig	[Fyll i]	Bedömning
Regelefterlevnad	[Fyll i]	[Granskning]
Internrevision	[Fyll i]	[Input]
Riskhantering	[Fyll i]	[Input]
Övriga	[Fyll i]	[Fyll i]

2.4 Källor som använts vid utarbetande av rapporten

Lista de viktigaste källorna:

- resultat från internrevision
- resultat av bedömning av efterlevnad
- resultat av testning av digital operativ motståndskraft, och i tillämpliga fall resultaten av avancerad testning, baserad på hotbildsstyrd penetrationstestning, av IKT-verktyg, IKT-system och IKT-processer
- externa källor

- [Fyll i källa 1]
- [Fyll i källa 2]
- [Fyll i källa 3]

3 Förändringar i IKT-riskhanteringsramen sedan föregående översyn

I detta avsnitt beskrivs de större förändringar och förbättringar som gjorts avseende IKT-riskhanteringsramen sedan föregående översyn.

> I tabellen nedan: beskriv vilken inverkan förändringarna har på bolagets strategi för operativ motståndskraft, på vår interna IKT-kontrollram samt på styrningen av IKT-riskhantering.

[Kopiera nedanstående tabell för samtliga förändringar.]

ID	[ÄND-001]
Ändring	
Motiv	
Påverkan	
Implementerad (ja/Nej/Delvis)	

4 Resultat: brister, svagheter och gap-analys

I nedanstående avsnitt ges en sammanfattning av resultaten av översynen och en analys och bedömning av hur allvarliga svagheterna, bristerna och luckorna i IKT-riskhanteringsramen har varit under översynsperioden. Allvarlighetsgraden bedöms i fyra steg: kritisk/hög/medel/låg. Innebörden av dessa fyra steg förtydligas i Tabell 1.

Tabell 1: Kriterier vid bedömning av allvarlighet avseende svagheter och brister.

Kritisk	Allvarlig svaghet eller brist som behöver åtgärdas snarast. Bristen kan med **hög** sannolikhet leda till en allvarlig eller mycket allvarlig konsekvens.
Hög nivå	Brist eller svaghet med hög allvarlighetsgrad. Bristen/svagheten kan leda till mycket allvarlig konsekvens eller med **hög** sannolikhet ha en kännbar eller betydande konsekvens.
Medel nivå	Brist eller svaghet som behöver analyseras djupare. Det är låg sannolikhet att bristen/svagheten leder till allvarlig konsekvens. Bristen ska bevakas i syfte att snabbt kunna sätta in åtgärd om omständigheterna förändras.
Acceptabel nivå	Brister eller svagheter som inte kräver någon åtgärd. Bristen/svagheten bedöms ha mycket låg sannolikhet att leda till en kännbar konsekvens. Bristen kan accepteras men bevakas..

4.1 Sammanfattning av fynd

[Kopiera nedanstående tabell för samtliga fynd.]

ID	[FND-001]
Område	
Beskrivning	[Beskriv brist/gap]
Orsak	[Rotorsak]
Risk/konsekvens	
Allvarlighet	
Regel/kravkoppling	
Status	

4.2 Bedömning av kontrollernas effektivitet

- Nyckelkontroller: [Fyll i]
- Resultat från kontrolltest: [Fyll i]
- Identifierade förbättringsområden: [Fyll i]

5 IKT-incidenter

Om översynen initierats av IKT-incidenter: lista incidenter och inkludera rotorsaksanalys samt koppling till åtgärder.

Om översynen inte initierats av IKT-incidenter tas avsnittet bort.

Följande incidenter har relevans till översynen av IKT-riskhanteringsramen.

Incident-ID	Datum	Typ	Påverkan	Huvudorsak	Lärdom/återkoppling
[INC-001]					[Referens till FND-xxx fynd i avsnitt 4.1 eller åtgärd [ÅTG-xxx] i avsnitt 6.]

6 Åtgärdsplan

I nedanstående avsnitt beskrivs åtgärderna för att hantera identifierade svagheter, brister och luckor.

Avsnittet fortsätter på nästa sida.

Åtgärd-ID	Kopplat fynd	Åtgärdsbeskrivning	Ansvarig	Intern/extern	Måldatum	Uppföljningsdatum	Status	Risk för försening	Resurs/budgetpåverkan	Myndighets-information (vid behov)
[ÅTG-001]	[Ref till fynd i 4.1]	[Beskrivning, inkludera verktyg/metod]	[Namn/Roll]	[Ange om verktyg och funktioner är interna eller externa]			[Öppen/Pågår/Stängd]	[Låg/Medel/Hög]	[Beskriv om åtgärden påverkar budget, personal, materiella resurser, inkludera resurser som avsatts för genomförandet av korrigerande åtgärder]	[information om processen för att informera den behöriga myndigheten, i relevanta fall]

6.1 Åtgärder som inte genomförs (residualrisk)

I nedanstående avsnitt redogörs för de svagheter, brister och luckor som inte är föremål för korrigerande åtgärder.

> I motiveringen ska det finnas en detaljerad beskrivning av de kriterier som används för att analysera effekterna av dessa svagheter, brister eller luckor, för att utvärdera den relaterade kvarstående IKT-risken och för att acceptera den relaterade kvarstående risken.

Beslut -ID	Fynt/åtgärd	Motivering	Bedömning av residualrisk	Riskägare	Godkänd (datum/beslut)
[ACC-001]	[FND/ÅTG]	[Fyll i]	[Fyll i]	[Fyll i]	[ÅÅÅÅ-MM-DD]

7 Planerade vidareutvecklingar

- Initiativ 1
- Initiativ 2
- Tidslinje, ev beroenden

8 Slutsatser

- Slutsatser
- Rekommendationer till ledning

9 Historik och uppföljning av tidigare översyner

I åtgärdsstatus ska det framgå en lägesrapport om genomförandet av de korrigerande åtgärder som identifierades i den senaste rapporten. I lärdomar ska det framgå om de föreslagna korrigerande åtgärderna i tidigare översyner har visat sig vara ineffektiva eller har inneburit oväntade utmaningar, en beskrivning av hur dessa korrigerande åtgärder skulle kunna förbättras eller av dessa oväntade utmaningar.

Rapportdatum	Period	Huvudfynd	Åtgärdsstatus	Lärdomar	Referens
[ÅÅÅÅ-MM-DD]	[ÅÅÅÅ-MM-DD – [ÅÅÅÅ-MM-DD]]	[Fyll i]	[Fyll i]	[Fyll i]	[Dnr]