IKT-RIKTLINJER I S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2023-05-26

#2494836

1 Inledning

För att konkretisera strategin för informations- och kommunikationsteknik, nedan IKT, och riktlinjer som är styrande för IKT har S:t Erik Försäkrings AB, nedan Bolaget, antagit dessa riktlinjer.

Riktlinjerna är framtagna i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn, nedan DORA, samt Eiopas riktlinjer (20/600) för säkerhet och företagsstyrning avseende IKT, nedan Eiopas IKT-riktlinjer. Cybersäkerhet inkluderas i IKT och ska därmed hanteras som en del av Bolagets allmänna hantering av IKT-risker och säkerhetsrisker.

Dessa riktlinjer omfattar samtliga anställda samt Bolagets ledning. Riktlinjerna ska kommuniceras med samtliga anställda. När det bedöms relevant ska hela eller delar av dessa riktlinjer kommuniceras till och gälla för Bolagets tjänsteleverantörer.

Bolaget tillämpar, utöver de definitioner som nämns nedan, de definitioner som anges i Eiopas IKT-riktlinjer.

Dessa riktlinjer ska ses över och revideras löpande, minst årligen.

2 Syftet med riktlinjerna

Riktlinjerna syftar till att minska de IKT-risker och säkerhetsrisker som Bolaget är exponerade för samt för att säkerställa god förberedelse för att hantera eventuella IKT- och säkerhetsincidenter.

3 Definitioner

Cyberattack	Alla former av hackande som leder till ett offensivt/skadligt försök att förstöra, exponera, ändra, deaktivera, stjäla eller få obehörig åtkomst till eller på ett obehörigt sätt använda en informationstillgång som riktar sig mot IKT-system.
Cybersäkerhet	Bevarande av konfidentialitet, integritet och tillgänglighet vad gäller information och/eller informationssystem via ett cybermedium.
IKT-tillgång	En programvaru- eller maskinvarutillgång som finns i affärsmiljön.
IKT- och säkerhetsrisk	Som en delkomponent i operativ risk; risk för förlust som beror på brott mot konfidentialiteten, på att integriteten hos system och data inte fungerar, på att system och data är olämpliga eller

	otillgängliga, eller på oförmåga att ändra på IKT:n inom rimlig tid och till rimliga kostnader när miljö eller verksamhetskraven förändras (dvs. flexibilitet). Detta inkluderar cyberrisker och informationssäkerhetsrisker till följd av otillräckliga eller icke-funktionella interna processer eller externa händelser, däribland cyberattacker eller otillräcklig fysisk säkerhet.
Informationssäkerhet	Bevarande av konfidentialitet, integritet och tillgänglighet vad gäller information och/eller informationssystem. Därtill kan även andra egenskaper vara aktuella, såsom autenticitet, ansvar, oavvislighet och tillförlitlighet.
IKT-tjänster	Tjänster som tillhandahålls via IKT-system och tjänsteleverantörer till en eller flera interna eller externa användare.
IKT-system	Uppsättning program, tjänster, it-tillgångar, IKT-tillgångar eller andra komponenter som hanterar information, vilket inkluderar driftsmiljön.
Informationstillgång	En samling uppgifter, antingen materiella eller immateriella, som är värda att skyddas.

4 Riktlinjer som behandlar IKT

Bolaget har en rad interna policyer och riktlinjer som på ett eller annat sätt berör IKT.

Bolaget är anslutet till flera tjänster och IKT-tillgångar som upphandlats genom Stockholms stad. Därvid finns flertalet riktlinjer som behandlar olika typer av frågor rörande IKT och informationssäkerhet som är producerade av Stockholms stad vilka också ska efterlevas av Bolaget. Dessa kan i sin tur ha påverkan på Bolagets arbete kring informationssäkerhet och IKT-strategi.

4.1 Bolagets interna riktlinjer

a) Styrelsens arbetsordning
b) Riktlinjer för intern styrning och kontroll
c) Riktlinjer för riskhantering
d) Instruktion för funktionen för riskhantering
e) Riktlinjer för internrevision
f) Riktlinjer för rapportering av händelser av väsentlig betydelse
g) Riktlinjer för hantering av personuppgifter
h) Katastrofplan
i) IT-avbrottsplan med tillhörande bilagor
~~i)~~j) Hanteringsrutin för informationssäkerhetsincidenter

Kommentar [JG1]: Gulmarkerade ses över inom ramen för DORA-projektet. FI har meddelat att det är oklart om riktlinjer av händelse av väsentlig betydelse kommer vara krav i framtiden maa DORA-rapporteringen

4.2 Riktlinjer som delas med Stockholms stad

a) Riktlinjer för incidentrapportering
b) Policy för skyddande av personuppgifter
c) Ramverk vid anskaffning av molntjänster
d) Kryptorekommendationer
e) Handbok för informationsklassning

f) Riktlinjer för infrastruktur
g) E-strategi
h) Riktlinjer för stadens IT-infrastruktur
i) Riktlinje informationssäkerhet
j) Stockholms stads IT-program

5 Roller och ansvarsområden

5.1 Styrelsen

Bolagets styrelse har det övergripande ansvaret att fastställa och godkänna Bolagets skriftliga IKT-strategi som en del av och i överensstämmelse med Bolagets övergripande affärsstrategi. Styrelsen ansvarar också för att Bolaget har ett effektivt system för hantering av IKT-risker och säkerhetsrisker som en del av Bolagets allmänna riskhanteringssystem.

5.2 VD

Bolagets vd ansvarar för att Bolagets kartläggning och identifiering av risker utförs i enlighet med Bolagets riktlinjer för riskhantering samt där relevant, dessa riktlinjer. Vd ansvarar därutöver för den fortsatta processen med att analysera och/eller minimera identifierade IKT-risker. Arbete enligt ovan kan delegeras till annan anställd.

Bolagets vd ska säkerställa att samtliga anställda erhåller relevant information och utbildning om IKT-risker och säkerhetsrisker.

5.3 Anställda

Samtliga anställda ansvarar för att utföra sitt arbete i enlighet med fastställda riktlinjer, instruktioner och befattningsbeskrivningar. Bolagets anställda ansvarar för att rapportera eventuella incidenter i enlighet med Stockholms stads riktlinjer för incidentrapportering.

5.4 Informationssäkerhetssamordnare

Bolaget ska ha en intern informationssäkerhetssamordnare som utgör ett stöd till Bolagets ledning i IKT-relaterade frågor och rapporterar även direkt till Bolagets styrelse och vd.

Samordnaren är ansvarig för vart och ett av Bolagens system. Denne ska löpande se över risken för avbrott eller andra störningar ur IKT-synpunkt och sköter Bolagets kontakt i dessa frågor med Stockholms stad. Rollen som Bolagets informationssäkerhetssamordnare upprätthålls av IT-ansvarig.

Ansvar vid eventuella avbrott framgår av Bolagets IT-avbrottsplan.

5.5 Dataskyddsombud

Bolaget ska ha ett Dataskyddsombud som löpande ska se över potentiella brister i Bolagets informationssäkerhet som kan påverka hanteringen av personuppgifter i verksamheten. Eventuella brister ska rapporteras till Bolagets vd och styrelse.

5.6 Riskhanteringsfunktionen

Bolagets funktion för riskhantering utför bl.a. sådant arbete som faller på funktion för informationssäkerhet i enlighet med DORA och EIOPA:s IKT-riktlinjer. Funktionen för riskhantering ska mot den bakgrunden bl.a.:

- utgöra ett stöd till Bolagets ledning i samband med fastställande och upprätthållande av Bolagets IKT-riktlinjer,

- 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 IKT-riktlinjer, och
- samordna granskningar av operativa incidenter eller säkerhetsincidenter och rapportera granskningar till Bolagets ledning och vd.

Det arbete som utförs inom ramen för funktion för informationssäkerhet rapporteras till Bolagets styrelse och vd.

5.7 Katastrofgrupp IT

Bolaget ska ha en katastrofgrupp med i förväg utsedda medlemmar och ersättare. De personer som ska vara med och ta beslut om alternativa rutiner, återgång till normalläge och eventuella korrigerande åtgärder ska finnas med i gruppen. Katastrofgruppens medlemmar och ansvar vid avbrott framgår i Bolagets IT-avbrottsplan.

Bolaget har även en krisledningsorganisation som består av en krisledning- och kommunikationsansvarig, administrativ funktion, samverkansfunktion samt analysfunktion. Dessa funktioners ansvar finns beskrivna i Bolagets katastrofplan.

5.8 Övriga nyckelfunktioner

I Bolagets organisation utgör vd, samtliga anställda samt vissa outsourcade verksamheter nyckelfunktioner. Bolaget har två kundansvariga, en riskhanteringsansvarig, en skadeansvarig, en bolagsjurist, en IA ansvarig och en ekonomiansvarig. Dessa samt deras ersättare anges närmare i Bolagets katastrofplan. För de aktuella tjänsterna gäller att ersättaren kanske inte fullt ut kan ta över samtliga arbetsuppgifter. Emellertid finns kompetens hos konsulter, närstående bolag och förvaltningar i staden som kan utnyttjas.

Roller och ansvarsområden inom Stockholms stad finns angivna i Stockholms stads riktlinjer för informationssäkerhet. Till stöd för stadens säkerhetsarbete och för kommunfullmäktiges mål om en trygg och säker stad finns ett strategiskt riskhanteringsråd, som bland annat hanterar frågor som rör informationssäkerhet. Informationssäkerhetschefen, som är placerad på stadsledningskontoret, samordnar aktiviteter inom informationssäkerhet över hela staden och är rådgivare för förvaltningar och bolag.

Utöver ovan har Bolaget centrala funktioner som bevakar IKT-risker ur olika perspektiv. Respektive funktions uppdrag och ansvar finns beskrivna i separat riktlinjer och varje funktion rapporterar direkt till Bolagets styrelse och vd.

6 IKT-strategi

Bolaget ska regelbundet analysera arbetet för att upprätthålla god informationssäkerhet samt ha en IKT-strategi. Strategi och analys finns dokumenterat i bilaga 1.

7 Utkontraktering m.m.

7.1 Upphandling och utkontraktering

Bolaget ska inför nya upphandlingar och utläggning av verksamhet ta eventuella IKT-risker i beaktande. Bolaget ska identifiera och ställa de krav som Bolaget anser nödvändiga för att Bolagets information ska hanteras säkert hos den externa leverantören.

Bolagets styrelse har antagit separata riktlinjer för dels upphandling, dels utlagd verksamhet. 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, Finansinspektionens rätt till insyn etc.

Respektive leverantör följs därtill upp mer formaliserat och minst årligen enligt separat checklista för uppdragstagare.

7.2 Beroende gentemot tjänsteleverantörer

När IKT-tjänster och IKT-system utkontrakteras ska Bolaget se till att relevanta krav för sådana tjänster och system uppfylls, utan att det påverkar tillämpningen av dessa interna IKT-riktlinjer samt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer.

I de fall kritiska eller viktiga funktioner utkontrakteras ska Bolaget se till att tjänste-leverantörens avtalsförpliktelser omfattar krav på innehåll i sådana avtal enligt EIOPA:s IKT-riktlinjer samt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer.

Vid hantering av tredjepartsleverantörer ska Bolaget även beakta Stockholms stads riktlinjer för informationssäkerhet.

Vid utkontraktering till en molntjänstleverantör ska Bolaget även beakta Stockholms stads ramverk vid anskaffning av molntjänster.

8 Riskhanteringsprocess

Bolaget ska regelbundet genomföra en kartläggning över Bolagets affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar). Syftet med kartläggningen är att identifiera deras betydelse och ömsesidiga beroendeförhållanden beträffande IKT-risker och säkerhetsrisker.

Hantering av IKT-risker och säkerhetsrisker ska vara en del av Bolagets allmänna riskhanteringssystem och riskhanteringsprocess som finns beskrivet i Bolagets interna riktlinjer för riskhantering. Detta inbegriper att, i enlighet med Bolagets riskstrategi, fastställa risktolerans för IKT-risker och säkerhetsrisker. IKT-risker ska inkluderas i Bolagets riskregister som tas fram Bolaget tillsammans med funktionen för riskhantering.

9 Logisk säkerhet

9.1 Behörighetstilldelning och åtkomsträttigheter

Bolaget ska hantera åtkomsträttigheter, däribland fjärråtkomst till informationstillgångar och deras stödsystem utifrån behovsenlig behörighet. Bolaget tillämpar principen om begränsad behörighet innebärande att anställda och tredjepartsleverantörer endast beviljas de åtkomsträttigheter som är nödvändiga för att utföra arbetsuppgifterna.

Ansvar för behörighetstilldelning och åtkomsträttigheter ligger på Bolagets vd eller den person vd valt att delegera ansvar till. Beviljad behörighet och åtkomsträttigheter ska dokumenteras. Behörighet och åtkomsträttigheter bör ses över regelbundet för att säkerställa att anställda och tredjepartsleverantörer inte har för omfattande rättigheter och att åtkomsträttigheter upphävs/tas bort om de inte längre behövs.

9.2 Fjärråtkomst och autentiseringsmetoder

Fjärradministratörsåtkomst till kritiska IKT-system ska endast beviljas utifrån behovsenlig behörighet och förutsatt att starka autentiseringslösningar används. Bolaget tillämpar för närvarande dubbel autentiseringslösning genom att fjärråtkomst endast ges genom användande av säkerhetskort i kombination med en lösenordskod eller annan motsvarande säkerhetslösning.

9.3 Loggning

Möjlighet för Bolaget att logga all användaraktivitet kravställs inför att Bolaget tar in nya system. I dagsläget tillämpas rutiner för loggning av användaraktivitet i samtliga av Bolagets system.

9.4 Programvara

Endast av Bolaget godkänd programvara får användas i IT-miljön. Programvara får inte installeras eller på annat sätt exekveras utan tillstånd från Bolagets vd. Otillåten användning kan utsätta IT-miljön och den information som hanteras för en säkerhetsrisk. Detta gäller all typ av programvara, även s.k. tilläggsmoduler till webbläsare.

10 Fysisk säkerhet

Bolaget ska skydda lokaler, IT-utrustning och känsliga områden från obehörigt tillträde och från miljöfaror. För detta ändamål har Bolaget vidtagit säkerhetsåtgärder i form av skalskydd, branschnormer för stöldskydd och brand, lås och larm, lösenordsskydd och tillträdeskontroll. Utrustning, särskilt stöldbegärlig, ska vara märkt så att den kan identifieras.

Stöldskyddsmärkningen ska utformas så att den är svår att avlägsna. Vidare ställer Bolaget fysiska säkerhetskrav vid upphandlingar. Fysisk och miljörelaterad säkerhet återges i sin helhet i Stockholms stads riktlinjer för informationssäkerhet.

Fysisk åtkomst till IKT-system ska endast beviljas behöriga personer i enlighet med avsnitt 9.1 ovan. Behörighet ska tilldelas i enlighet med personens uppgifter och ansvarsområden och begränsas till personer som har lämplig utbildning och som övervakas på ett lämpligt sätt.

Fysisk åtkomst bör ses över regelbundet för att säkerställa att onödiga åtkomsträttigheter snabbt tas bort om de inte längre behövs.

11 IKT-säkerhet

Genom vad som nämns ovan i dessa riktlinjer samt genom redan befintliga riktlinjer nämnda i avsnitt 4 har Bolaget infört rutiner för att säkerställa konfidentialitet, integritet och tillgänglighet.

Bolaget har därtill processer för att förhindra säkerhetsincidenter i IKT-system och IKT-tjänster, samt att om de inträffar minimera effekten på IKT-leveransen.

Då hela Bolagets IT-infrastruktur är placerad i Stadens struktur, är det stadens riktlinjer och åtgärder som gäller för Bolaget.

Mot bakgrund av att Bolaget är en del av Stockholms stad ingår Bolaget i Stockholms stads avtal med Leverantör avseende systemdrift och systemförvaltning av stadens centrala verksamhetssystem. Genom detta avtal tillgodoses för verksamhetssystemen hög grad av tillgänglighet, driftssäkerhet, tillförlitlighet och säkerhet. Inom ramen för detta avtal finns specifika och omfattande riktlinjer för informationssäkerhet som Leverantören är bunden av. Till avtalet hör också beskrivning av säkerhetskrav och därav ingående aktiviteter i IT-säkerhetsarbetet, hur sekretessbelagda handlingar ska hanteras samt krav på kommunikationslösningar och krisberedskap. Verksamheten kontrolleras regelbundet av Bolaget i enlighet med avsnitt 7 ovan.

Avseende Bolagets verksamhetssystem ansvarar upphandlad leverantör för att uppdatera systemets tekniska och säkerhetsmässiga plattform, och genomföra nödvändiga uppgraderingar. När det emellertid gäller uppgradering av servrar där Bolagets övriga system huserar, är det stadens ansvar att implementera relevanta säkerhetsuppdateringar och tillse att nödvändiga uppgraderingar sker. Bolaget ska regelbundet säkerställa att sådana uppdateringar utförs på ett korrekt sätt.

Gällande informationsklassning tillämpar Bolaget stadens handbok för informationsklassning. Bolaget tillämpar därtill rutinen att informationsklassningen utförs åtminstone årligen för de IKT-tillgångar som anges i bilaga 2.

12 Granskning, bedömning och testning

Bolagets centrala funktioner ska regelbundet och ur olika synvinklar granska och bedöma Bolagets arbete med IKT. Vid behov ska Bolaget utföra stresstester som validerar tillförlitligheten och effektiviteten hos Bolagets informationssäkerhetsåtgärder och säkerställer att Bolaget tar hänsyn till de hot och sårbarheter som har identifierats genom hotövervakning samt riskbedömningsprocessen för IKT-risker och säkerhetsrisker. Testerna ska vidare identifiera eventuella svagheter, överträdelser och incidenter vad gäller säkerheten. Sådana tester ska utföras av oberoende personer med ändamålsenlig kunskap och kompetens.

System tillhandahållna genom Stockholms stad testas regelbundet i ~~egen~~ Stockholms stads regi. Bolaget avser att regelbundet kontrollera att sådana tester utförs samt efterfråga information om incidenter, skador eller annat som kan påverka Bolagets informationssäkerhetsarbete.

13 Revision

Bolagets styrning, system och processer för IKT-risker och säkerhetsrisker ska vid behov genomgå revision. Är systemet kritiskt ska revision utföras minst årligen. Sådan revision ska utföras av revisorer eller motsvarande med tillräcklig kunskap, kompetens och expertis inom IKT-risker och säkerhetsrisker för att kunna lämna en oberoende försäkran om deras effektivitet till Bolagets styrelse och vd.

Bolaget ska vidare säkerställa löpande att nödvändig revision av system tillhandahållna genom Stockholms stad utförs.

14 Hantering av incidenter och IT-avbrott

Bolaget har i befintliga interna riktlinjer samt genom Stockholms stads riktlinjer, rutiner för bl.a. spårning, loggning, klassificering och analys av incidenter och IT-avbrott.

15 Utbildning

Bolaget ska regelbundet utbilda all personal och ledning om informationssäkerhet och IKT-risker. Bolaget ska eftersträva en hög medvetenhet kring informationssäkerhet, IKT-risker och säkerhetsrisker i syfte att minska antalet fel som beror på den mänskliga faktorn, stölder, bedrägerier, felaktig användning och förluster.

Bilaga 1

1 Informations- och kommunikationsstrategi

Informations- och kommunikationsteknologi, nedan IKT, är en viktig och integrerad del av S:t Erik Försäkrings AB:s, nedan Bolaget, verksamhet. Informations- och kommunikationsflödet inom Bolaget sker övervägande digitalt och är ständigt accelererande. Med detta ökar komplexiteten inom IKT och det följer större krav på att säkerställa ändamålsenlig säkerhet och företagsstyrning avseende IKT.

Informationssäkerhet handlar om styrning av skydd till lämplig nivå för varje informationsmängd, inklusive styrning av utformningen av fysiskt skydd. Bolaget eftersträvar ett systematiskt IKT- och informationssäkerhetsarbete som bygger på att säkerhetsåtgärder ska vidtas utifrån de risker verksamhetens IKT- och informationshantering är utsatta för. Bolagets fysiska skydd motsvarar därmed de krav som kommer fram i Bolagets riskanalys och informationsklassningar. Sammanfattningsvis är det Bolagets behov som ska styra skyddsnivån.

Mot bakgrund av ovan och som en del i Bolagets IKT-strategi har Bolagets styrelse antagit interna riktlinjer för IKT. I dessa riktlinjer finns bl.a. beskrivet hur Bolaget är organiserat, vilka IKT-system Bolaget använder och hur nyckelberoenden gentemot Bolagets tjänsteleverantörer ska hanteras. Bolagets interna riktlinjer kopplade till IKT ska alltid innehålla krav på starka lösenord, begränsad behörighet, säkerhetskopiering och dataskydd, inklusive personuppgifter.

Som en del i IKT-strategin avser Bolaget att kontinuerligt utbilda Bolagets anställda och ledning i IKT-relaterade frågor och att upprätthålla en god medvetenhet kring IKT-risker. Bolaget har även upprättat särskild förteckning över personer med nyckelroller och ansvar kopplade till IKT-relaterade frågor, vilket närmare framgår i Bolagets kontinuitetsplan. Detta syftar till att minimera risken för att potentiella incidenter, cyberattacker och intrång inträffar samt för att minimera eventuella skador.

-Bolagets vd ska omedelbart informera styrelsen vid allvarliga säkerhetsincidenter. Det ska finnas en incidenthanteringsplan som beskriver hur kommunikationen ska ske internt, externt och vilka roller som ska finnas med i en intern incidenthanteringsgrupp. Det är viktigt att på ett tidigt stadie ge information till kunder, leverantörer, samarbetspartners och andra eventuella intressenter.

Bolaget ska i möjligaste mån vara öppet och transparent vid kommunikation med media samt i andra öppna kanaler såsom webbsida och sociala media.

Utöver ovan är en viktig del i Bolagets IKT-strategi är att kartlägga och identifiera IKT-risker inom ramen för riskhanteringsprocessen i syfte att kunna möta riskerna med ändamålsenligt skydd och förhindra att incidenter inträffar. Inom ramen för riskhanteringsprocessen ska Bolaget regelbundet analysera IKT- och säkerhetsrisker samt de åtgärder Bolaget vidtar för att säkerställa god hantering av IKT. Sådana analys ses över löpande och följer nedan.

2 Analys

Bolaget ska minst årligen genomföra och uppdatera verksamhetsanalys, omvärldsanalys och riskanalys hänförlig till informationssäkerhet och där tillhörande risker.

2.1 Verksamhetsanalys

Bolaget har den ~~1 oktober 2021~~22 november 2024 hållit en workshop för att närmare analysera verksamheten ur informationssäkerhetssynpunkt och därvid kartlagt Bolagets och andra intressenters behov, förväntningar och förutsättningar vilka behöver beaktas vid utformning av informations-säkerhetsarbetet och dess styrning. Bolaget har utarbetat såväl kontinuitets- som beredskaps-planer för att i största möjliga mån säkerställa driften av viktiga system i verksamheten. Det kan dock konstateras att verksamheten utan större problem skulle kunna fungera trots att vitala system under viss tid ligger nere, såsom exempelvis skadereglering kan dokumenteras manuellt och en okulär besiktning kräver inte nödvändigtvis digitala hjälpmedel. Sådant arbete fordrar emellertid visst efterarbete i form av att registrera dokumentation i Bolagets olika system.
Vidare utvisar verksamhetsanalysen att Bolaget är beroende av andra verksamhetsutövare i form av såväl tjänsteleverantörer som leverantörer av utkontrakterade tjänster. Mot bakgrund av att Bolaget är tillståndspliktigt ställs redan en mängd krav på Bolaget avseende uppföljning av utlagd verksamhet. Således gör Bolaget bedömningen att uppföljningsarbetet inte nämnvärt kommer förändras eller behöva förstärkas, dock avser Bolaget att utöka kravställandet i så måtto att Bolaget även fångar upp leverantörers hantering och beredskap rörande frågor om informationssäkerhet.

Bolagets styrelse har konstaterat att ett avbrott i något av Bolagets kritiska system, inte får föreligga i mer än maximalt en vecka. För mer information om hanteringen vid eventuella avbrott, se Bolagets kontinuitetsplan.

Samtliga Bolagets identifierade IKT-tillgångar och system återfinns i bilaga 2.

2.2 Omvärldsanalys

Vid workshopen identifierade vidare Bolaget vilka rättsliga krav som stipuleras för verksamheten och hur dessa påverkar Bolagets informationssäkerhetsarbete. Vid tillfället för analysen kunde det konstateras att Bolaget, utöver Dataskyddsförordningen, träffas av en mängd näringsrättsliga regler såsom försäkringsrörelselagen och lagen om försäkrings-distribution. Därtill ska i sammanhanget särskilt nämnas DORA, EIOPA:s riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik samt EIOPA:s riktlinjer för uppdragsavtal med molntjänstleverantörer.

Bolaget kunde vid omvärldsanalysen konstatera att det finns mycket god beredskap för att hantera de rättsliga krav som ställs och kommer att ställas även i framtiden. I denna del har Bolaget stöd av Bolagets funktion för regelefterlevnad som utför löpande omvärldsbevakning och rapporterar direkt till Bolagets styrelse och vd om relevanta regelverk.

De rättsliga kraven omfattar vidare uppföljning av IKT-leverantörer, tjänsteleverantörer och leverantörer av utlagd verksamhet, vilket omnämns under avsnitt 2.1 ovan.

Kommentar [JG2]: Överväg att tydligare beskriva testning och SLA, framgår primärt av riktlinjer för outsourcing samt respektive leverantörsavtal

2.3 Riskanalys

Riskanalysen ska löpande identifiera IKT-risker och utförs verksamhetsövergripande.

Riskerna avseende informationssäkerheten tas fram genom en systematisk och kreativ process, där riskerna och potentiella händelser som kan leda till negativa konsekvenser ska beskrivs. Dessa bedöms sedan med avseende på sannolikheten att de inträffar samt konsekvensens allvar ifall de skulle inträffa. Riskhanteringsprocessen beskrivs närmare i Bolagets riktlinje för riskhantering. Bolaget har i denna del stöd av Bolagets funktion för riskhantering som rapporterar direkt till Bolagets styrelse och vd.

Närmare information för hur ovan nämnda risker hanteras samt Bolagets riskaptit för IKT-risker, återfinns i Bolagets riktlinje för riskhantering.

Bilaga 2

IKT-tillgångar

Med IKT-tillgångar avses en programvaru- eller maskinvarutillgång som finns i Bolagets affärsmiljö. De verksamhetssystem som Bolaget använder är:

a) IA (incidentrapporteringssystem)
b) INSMAN (försäkringssystem)
c) Outlook (E-post)
d) Microsoft Office (kontorssystem)
e) Telefoni (telefonväxel)
f) Agresso (ekonomisystem)
g) VISMA Agda (lönesystem)
h) www.sterikforsakring.se
i) Tietoevry (datorer, hårdvara, mobil m.m. gruppdiskar, integrationsplattform)
j) Kommers (Primona, upphandlingssystem)
k) eDok (diarieföringssystem)
l) Solvency tools (finansrapportering)
m) Zoom X (Stadens version av Zoom)

Affärsprocesser

- Försäkringsprocess
- Skadehanteringsprocess
- Återförsäkringsprocess
- Kapitalförvaltningsprocess

Affärsverksamhet

- Försäkring