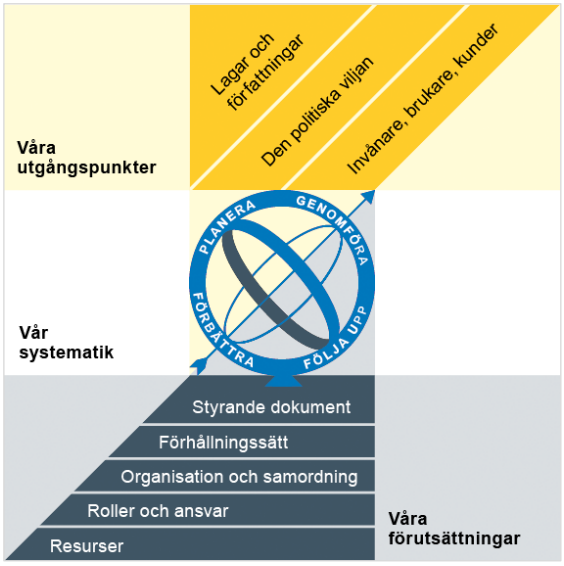
Göteborgs Stad

Försäkrings AB Göta Lejons anvisning för riskhantering

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



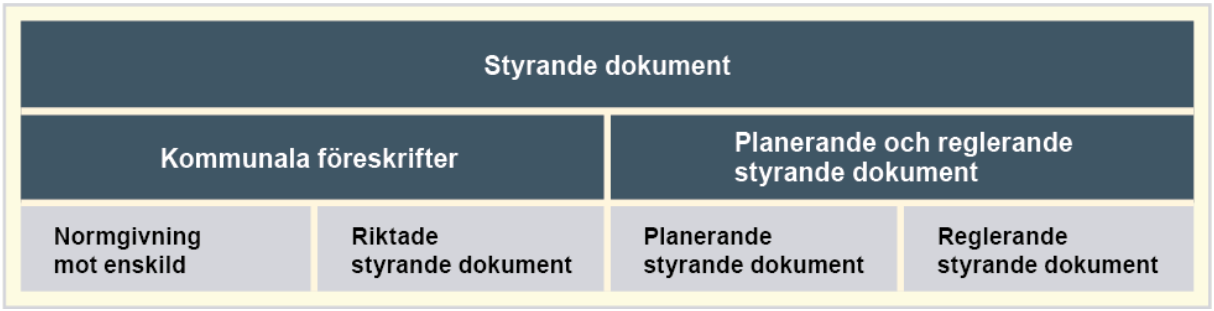
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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:**
VD	Försäkrings AB Göta Lejon		[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Anvisning	Till vidare	2026-01-09	Bolagscontroller

Bilagor:
Bilaga 1: Kompletterande material som stöd vid riskanalys avseende informationssäkerhet
Bilaga 2: Mall för att genomföra riskanalys

Innehåll

Inledning 4
Syftet med denna anvisning 4
Vem omfattas av anvisningen 4
Koppling till andra styrande dokument 4
Stödjande dokument 4
Anvisning 5
Process och hantering 5
Övergripande och lokala riskanalyser 6
Övergripande riskanalys 6
Lokala riskanalyser 6
Bedömningsmetod 7
Skala för konsekvens 8
Skala för riskacceptans 11
Genomföra riskanalys 12
Förberedelser – omfattning och förutsättningar 12
Riskbedömning och riskbehandling 13
Följa upp 14
Förbättra 14
Bilaga 1 15
Kompletterande material som stöd vid riskanalys avseende informationssäkerhet 15
Dokumentation ..... **Fel! Bokmärket är inte definierat.**

Inledning

Syftet med denna anvisning

Syftet med denna anvisning är att tydliggöra hur Göta Lejon arbetar med riskhantering.

Vem omfattas av anvisningen

Denna anvisning gäller för Försäkrings AB Göta Lejon.

Koppling till andra styrande dokument

Denna anvisning har koppling till nedanstående styrande dokument.

Styrande dokument	Koppling till denna anvisning
Försäkrings AB Göta Lejons riktlinje för intern styrning och kontroll	Fastställer avsikt och krav inom risktagande och beskriver bolagets riskhantering och interna styrning och kontroll
Försäkrings AB Göta Lejons riktlinje för säkerhet	Anger strategi, principer och ansvar för systematiskt säkerhetsarbete. Utgör bolagets strategi för säkerhet
Göteborg stads riktlinje för styrning, uppföljning och kontroll	Styrande dokument från Göteborgs stad

Stödjande dokument

Styrande dokument	Koppling till denna anvisning
Göteborgs stads vägledning för styrning, uppföljning och kontroll - risk	Konkretiserar stadens riktlinje för styrning, uppföljning och kontroll
Försäkrings AB Göta Lejons handbok för informationssäkerhet	Förtydligar hur arbetet med informationssäkerhet bedrivs i bolagets styrning, inklusive årshjul för informationssäkerhetsarbetet.

Anvisning

Med riskhantering avses de samordnade aktiviteter som genomförs för att identifiera, analysera, värdera och hantera de risker som kan komma att negativt påverka Göta Lejons verksamhet och bolagets förmåga att uppfylla sina mål. Riskarbete är grundläggande för att uppnå ständiga förbättringar och en central del av den interna kontrollen.

Göta Lejons riktlinje för riskhantering och intern styrning och kontroll beskriver bolagets riskhanteringsstrategi, ansvar, risknivåer och riskkategorier. Bolagets riktlinje för säkerhet beskriver särskilt strategi, principer och ansvar för det systematiska säkerhetsarbetet.

Denna anvisning tydliggör ovanstående riktlinjer genom att den beskriver hur bolagets riskhanteringsarbete ska utföras. Riskhanteringsarbete kan bedrivas på flera nivåer inom bolaget och med olika syften. Genom att följa denna anvisning möjliggörs samordning av riskhanteringsarbetet inom bolaget.

Process och hantering

Riskhantering ska alltid genomföras inför en ny situation eller en förändring, men också regelbundet, minst en gång per år även om det verkar som att ingen förändring har skett. Riskhantering ska vara en del av beslutsunderlag inför beslut om förändringar.

Figur 1: Schematisk bild över riskhanteringsprocessen.

Riskhanteringsprocess är de samordnade aktiviteterna för att identifiera, analysera, värdera, hantera risker och följa upp riskbehandlingen, se Figur 1.

Exempel på tillfällen när processen för riskhantering alltid ska genomföras:

- vid anskaffning, upphandling eller avveckling av IS/IT-tjänster/drift,
- i samband med systemuppgraderingar, tekniska förändringar i nätverk, infrastruktur eller programvaror,
- förändringar i omvärlden (tex förändrad hotbild, nyupptäckta sårbarheter),
- organisations-/processförändringar som kan påverka informationsbehandlingen eller
- när särskild lagstiftning ställer krav på att riskanalys och riskbedömning ska ligga till grund för beslut av hantering och åtgärder (till exempel PDL, NIS, GDPR)

Övergripande och lokala riskanalyser

Risker kan uppstå och förekomma inom olika riskområden. Väsentliga risker ska inkluderas i bolagets övergripande riskanalys[1]. Väsentliga risker kan vara risker som är gemensamma för alla delar av verksamheten, risker som har stora konsekvenser, rör långsiktiga mål, efterlevnad av legala krav med mera. För att kunna arbeta med riskhantering behöver bolaget genomföra både övergripande och lokala riskanalyser.

De lokala och den övergripande riskanalysen samverkar med varandra. Den övergripande riskanalysen utgör en grund för lokala riskanalyser. De risker som identifieras i lokala analyser kan bidra till att påverka den övergripande riskbedömningen i det övergripande riskregistret. Detta samband säkerställer att de lokala riskanalyserna kontinuerligt påverkar och förbättrar organisationens totala riskbild, vilket är avgörande då lokala analyser kan identifiera risker som annars skulle förbises i central riskhantering.

Övergripande riskanalys

Göta Lejons årliga övergripande riskanalys är en organisationsövergripande riskanalys som syftar till att identifiera och bedöma bolagets centrala riskområden på en övergripande nivå. I denna analys ska alla risker som kan hindra Göta Lejon att uppnå de strategiska målen och kontinuitet identifieras och dokumenteras. Analysens resultat utgör en gemensam riskbild för hela bolaget, vilket ger vägledning om relevanta säkerhetsåtgärder och fungerar som underlag för mer detaljerade lokala riskanalyser.

Den övergripande riskanalysen genomförs under fjärde kvartalet varje år. Identifierade åtgärder följs upp löpande och rapporteras till styrelsen två gånger per år (juni och november).

Lokala riskanalyser

Med *lokala riskanalyser* avses avgränsade riskanalyser. Dessa kan t ex genomföras baserat på lagreglering, avgränsat till processer, informationssystem vid förändringar, i enlighet med de ovan beskrivna tillfällen när processen för riskhantering ska genomföras. Vid genomförande av en lokal riskanalys ska alltid bolagets övergripande riskanalys beaktas för att inhämta information, kalibrera risknivåer etc. Syftet med den lokala riskanalysen är att noggrant identifiera och dokumentera risker, vilka sedan registreras i ett riskregister.

Vid utförande av riskanalys på delområdesnivå bör man först identifiera vilka generella risker inom bolaget som påverkar delområdet. Därefter analyseras de riskspecifika faktorer som påverkar den aktuella avgränsningen. Efter genomförd lokal riskanalys ska riskägaren bedöma om det finns resultat i den lokala riskanalysen som ska lyftas till bolagets övergripande riskanalys.

I Tabell 1 beskrivs de lokala riskanalyser som bolaget regelbundet genomför.

[1] I Göteborgs stads vägledning för styrning, uppföljning och kontroll används begreppet ”samlad riskbild”

Tabell 1: Förteckning över bolagets lokala riskanalyser

Riskanalys	Beskrivning	Tidpunkt, periodicitet	Relevant reglering
Försäkrings-verksamhet	Riskanalys avseende försäkring och återförsäkring	Fjärde kvartalet, årligen	Solvens II
Informationssäkerhet	Riskanalys avseende bolagets informationssäkerhet	Första kvartalet, årligen	Dora-förordningen
Riskanalys personuppgifts-behandlingar	Riskanalys avgränsad till personuppgiftsbehandling, utgör en del av konsekvensbedömning	Vid behov	Dataskydds-förordningen
Arbetsmiljö	Riskanalys som genomförs i samband med skyddsrond	Fjärde kvartalet, årligen	Arbetsmiljölagen (1977:1160), AFS 2023:1/2023:2
Risk- och sårbarhetsanalys	Analys som omfattar förmågan att hantera samhällsstörningar	En gång per mandatperiod	Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
Riskanalys vid förändring	Avser systemförändringar, organisationsförändringar eller andra förändringar som berör bolaget	Vid behov	

Bedömningsmetod

I följande avsnitt redogörs för de graderingar som används vid bedömning av sannolikhet och konsekvens, riskmatris samt kriterier för riskacceptans.

Sannolikhetstabell

Vid bedömning av sannolikhet används Tabell 2.

Tabell 2: Tabell för bedömning av sannolikhet vid riskanalys.

Nivå	Sannolikhet	Kvantitativ bedömning
5	Mycket hög sannolikhet	Inträffar en gång per vecka
4	Hög sannolikhet	Inträffar en gång per månad
3	Medel sannolikhet	Inträffar en gång per år
2	Låg sannolikhet	Inträffar en gång per 1-10 år
1	Mycket låg sannolikhet	Inträffar mer sällan än vart 10e år

Skala för konsekvens

Konsekvensbedömning görs utifrån skada på individ, verksamhet, samhällsviktig funktion och organisationens förtroende/ekonomi. För att fastställa konsekvensen för brister i konfidentialitet, riktighet eller tillgänglighet hos skyddsvärda informationstillgångar används skalan i Tabell 3 eller Tabell 4 användas. Tabellerna har samma indelning men har olika omfattande beskrivning.

Tabell 3: Tabell för konsekvensbedömning, kortform.

Konsekvens-nivå	1. Obetydlig/ lindrig	2. Kännbar/ Betydande	3. Allvarlig	4. Mycket allvarlig
Finansiell påverkan	0-2,5 mkr **Ringa skada på egendom, obetydlig återställningskostnad (i tid och/eller pengar)**	2,5-10 mkr **Betydande skada på egendom, låg återställningskostnad (i tid och/eller pengar)**	10-20 mkr **Allvarlig skada på egendom, hög återställningskostnad (i tid och/eller pengar)**	>20 mkr **Mycket allvarlig skada på egendom, mycket hög återställningskostnad (i tid och/eller pengar)**
Förtroendeförlust	Ringa påverkan på externa relationer.	Obekvämt men äventyrar inte kunder och leverantörer. Ryktet kortsiktigt påverkat.	Affärsrelationer påverkas allvarligt men bara på kort sikt. Rykte bestående påverkat.	Affärsverksamheten och kundrelationer påverkas långvarigt.
Verksamhet/ Leveransförmåga	**Ringa påverkan på leveransförmåga**	**Betydande påverkan på leveransförmåga**	**Allvarlig påverkan på leveransförmåga**	**Mycket allvarlig påverkan på leveransförmåga**
Individ	Lindrig påverkan på enskild individs rättigheter eller hälsa.	Betydande påverkan på enskild individs rättigheter eller hälsa.	Allvarlig påverkan på enskild individs rättigheter eller hälsa.	Mycket allvarlig personskada med bestående men eller dödsfall
Juridisk	Påpekande från myndighet, avvikelse hanteras internt.	Föreläggande från myndighet. Vite efter brott mot lag, förordning eller avtal.	Bot eller sanktionsåtgärder från myndighet. Vite efter brott mot lag, förordning eller avtal.	Sanktionsåtgärder från myndighet. Påföljd efter brott mot lag, förordning eller avtal.

Tabell 4: Tabell för konsekvensbedömning, utökad form.

Konsekvensnivå	**1. Obetydlig/lindrig** *MSB:* ***Ringa***	**2. Kännbar/Betydande** *MSB:* ***Betydande***	**3. Allvarlig**	**4. Mycket allvarlig** *MSB:* ***Synnerligen allvarlig***
Finansiell påverkan	0-2,5 mkr **Ringa skada på egendom, obetydlig återställningskostnad (i tid och/eller pengar)**	2,5-10 mkr **Betydande skada på egendom, låg återställningskostnad (i tid och/eller pengar)**	10-20 mkr **Allvarlig skada på egendom, hög återställningskostnad (i tid och/eller pengar)**	>20 mkr **Mycket allvarlig skada på egendom, mycket hög återställningskostnad (i tid och/eller pengar)**
Förtroendeförlust	Ringa påverkan på externa relationer. Ryktet relativt opåverkat. Missnöje begränsat till enskilda händelser eller enskilda personer som uttalar sig i sociala medier. Mindre notiser i lokalpress. Lokal negativ medieuppmärksamhet Aktualitet en dag till ett fåtal dagar. Mindre antal klagomål.	Obekvämt men äventyrar inte kunder och leverantörer. Ryktet kortsiktigt påverkat. Nyheter i media och i sociala medier, aktualitet i flera dagar till veckor. Klagomål leder till krav på åtgärder och/eller kompensation. Återkommande lokal negativ medieuppmärksamhet.	Affärsrelationer påverkas allvarligt men bara på kort sikt. Rykte bestående påverkat. Flera publiceringar med hård kritik, ihållande drev i rikstäckande media och social media. Aktualitet med än fåtal veckor. Stort antal krav på åtgärder och/eller kompensation. Långvarig lokal negativ medieuppmärksamhet.	Affärsverksamheten och kundrelationer påverkas långvarigt eller avbryts. Förtroendeförlusten innebär att intressenter inte längre vill samarbeta med bolaget Återkommande negativ nationell medieuppmärksamhet.
Verksamhet/ Leveransförmåga	**Ringa påverkan på leveransförmåga**	**Betydande påverkan på leveransförmåga**	**Allvarlig påverkan på leveransförmåga**	**Mycket allvarlig påverkan på leveransförmåga** Affärskritiska system eller processer påverkas allvarligt.

	Mindre fel i processer system, Ringa förseningar. Mindre avbrott i processer eller system. Måttlig förändring av verksamhetens produktivitet som medför åtgärder. Ringa minskning i förmågan att lösa kritiska verksamhetsuppgifter.	En eller flera huvudansvarskrav uppfylls inte. Större förseningar. Betydande förändring av verksamhetens produktivitet som medför större åtgärder. Betydande minskning i förmågan att lösa kritiska verksamhetsuppgifter. Stora omprioriteringar av verksamheten. Produktionsförmågan minskas under en överskådlig tid.	Höga kostnader uppstår. Driftstopp. Allvarlig förändring av verksamhetens produktivitet som pågår under oöverskådlig tid. Allvarlig begränsning i förmågan att lösa kritiska verksamhetsuppgifter. Omfattande omprioriteringar av verksamheten. Reservrutiner måste aktiveras.	Driftstopp. Verksamheten kan inte eller har mycket svårt att utföra sitt uppdrag.
Individ	Individs rättigheter tillgodoses inte och medför ringa olägenhet, möjligen smärre påpekanden eller irritation. Personskada <14 dagars sjukskriving. Försumbar påverkan på enskild individs rättigheter eller hälsa.	Individs rättigheter tillgodoses inte och medför att individen utsätts för betydande olägenhet, ekonomi påverkas men är inte försvårande, professionella, fysisk och psykiska förhållanden är påverkade. Personskada med över 14 dagars sjukskrivning	Individs rättigheter tillgodoses inte och medför att individen utsätts för försvårande av ekonomiska, professionella, fysiska och psykiska förhållanden, stort personligt lidande. T ex identitetsstöld. Allvarlig personskada utan bestående men.	Allvarlig personskada med bestående men eller dödsfall
Juridisk	Påpekande från myndighet, avvikelse hanteras internt. Föreläggande kring avvikelse mot föreskrift från tillsynsmyndighet med krav på åtgärd med tidsfrist. Varning eller erinran efter försumlighet mot lagar, förordningar eller avtal.	Föreläggande från myndighet. Vite efter brott mot lag, förordning eller avtal.	Bot eller sanktionsåtgärder från myndighet. Vite efter brott mot lag, förordning eller avtal. Möjlig påföljd är avsked eller fängelse efter brott mot lag, förordning eller avtal.	Sanktionsåtgärder från myndighet. Påföljd efter brott mot lag, förordning eller avtal. Påföljd såsom avsked eller fängelse eller upphörande av verksamhet.

Riskmatris

I Tabell 5 visas den riskmatris som anger risknivåerna efter genomförd bedömning av sannolikhet och konsekvens.

Tabell 5: Riskmatris

Konsekvens							
	Mycket allvarlig	4	Hög nivå	Hög nivå	Hög nivå	Oacceptabel nivå	Oacceptabel nivå
	Allvarlig	3	Medelhög nivå	Medelhög nivå	Hög nivå	Oacceptabel nivå	Oacceptabel nivå
	Kännbar/Betydande	2	Acceptabel nivå	Medelhög nivå	Medelhög nivå	Hög nivå	Hög nivå
	Lindrig/Ringa	1	Acceptabel nivå	Acceptabel nivå	Acceptabel nivå	Medelhög nivå	Medelhög nivå
			1	2	3	4	5
			Mycket låg sannolikhet	Låg sannolikhet	Medelhög sannolikhet	Hög sannolikhet	Mycket hög sannolikhet
	Sannolikhet						

Skala för riskacceptans

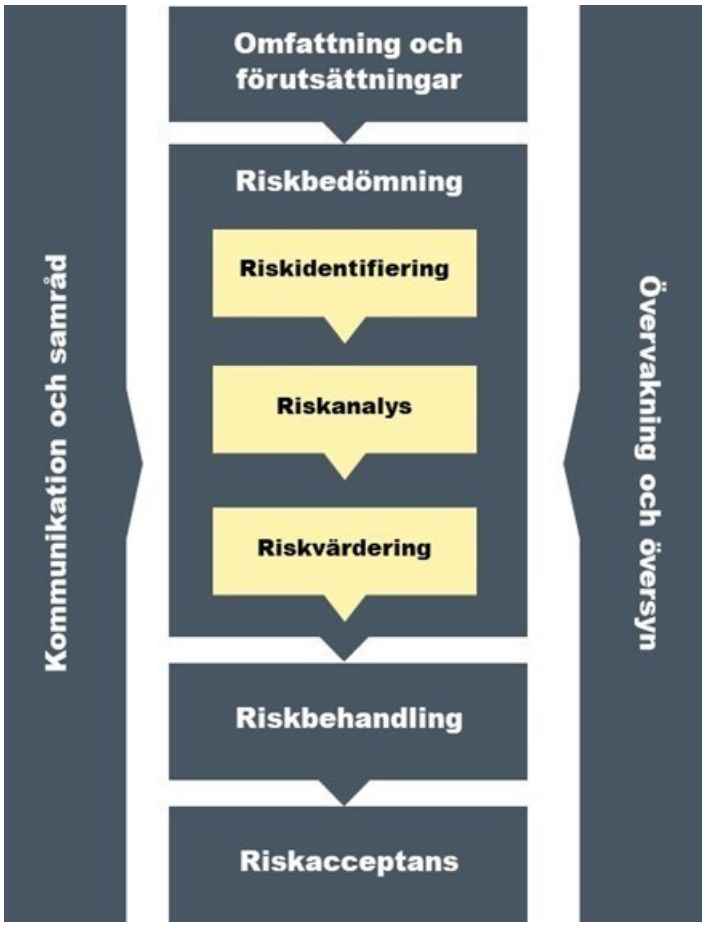
När riskvärdering genomförs används Tabell 6 för att bedöma hur risken ska hanteras.

Tabell 6: Tabell för riskhantering och riskacceptans.

Risknivå	Bedömning	Risk får accepteras av	Krav på information	Krav på behandling	Risk-register
Oacceptabel nivå	Allvarliga risker som behöver åtgärdas snarast. Riskerna har värderats med hög sannolikhet eller hög konsekvens. Riskerna kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.	Ledning	Ledning, styrelse och bolags-controller	Snarast	Övergripande och lokalt
Hög nivå	Höga risker som behöver åtgärdas. Riskerna kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.	Ledning	Ledning	Inom 3 månader	Övergripande och lokalt
Medel nivå	Risker som behöver analyseras djupare. Riskerna ska bevakas i syfte att snabbt kunna sätta in åtgärd om händelsen inträffar.	Riskägare	Ansvarig chef	Inom 12 månader	Övergripande och lokalt
Acceptabel nivå	Risker som inte kräver någon åtgärd alternativt bedömts som låga och/eller bedömts inte medföra störningar i organisationen. Risk som kan accepteras men som ska bevakas. Dessa risker kan hanteras i den löpande verksamheten.	Riskägare	Inga krav	Inga krav	Lokalt

Genomföra riskanalys

Att genomföra en riskanalys innebär att systematiskt identifiera och utvärdera säkerhetsrisker. Processen följer de steg som illustreras i Figur 2. Vid genomförandet av vissa analyser så kan det finnas särskilda formkrav att ta hänsyn till, t ex staden-gemensamma mallar, andra bedömningskriterier och/eller riskmatriser. Om det är fallet justeras genomförandet med hänsyn till detta.



Figur 2: Riskhanteringsprocessen

Förberedelser – omfattning och förutsättningar

Innan analysen påbörjas ska omfattning och samtliga förutsättningar klargöras. Detta innebär att fastställa följande:

- **Syfte och omfattning:** Vilka processer eller delar av försäkringsverksamheten berörs? Vad syftar analysen till? Vad är målet med analysen? Finns det rättsliga krav som ska beaktas eller nödvändiga gränsdragningar som behöver göras?
- **Deltagare:** Vilka funktioner är lämpliga för deltagande i analysen? Säkerställ en lämplig representation av personal med rätt kompetens och beslutsnivå. Analysen genomförs med fördel i workshopformat.

- **Underlag:** Inventera befintliga processkartläggningar, tidigare händelser och incidentstatistik. Finns resultat från revisioner eller tidigare riskanalyser?
- **Förbered analysen:** Sammanställ relevant underlag och skicka ut till analysens deltagare.

Riskbedömning och riskbehandling

Riskbedömningen är kärnan i själva analysgenomförandet och består av tre delar: riskidentifiering, riskanalys och riskvärdering.

- **Riskidentifiering** handlar om att upptäcka och beskriva de händelser som kan hindra bolaget från att nå sina mål eller uppfylla sina skyldigheter. Beroende på analysens omfattning finns olika typer av metodstöd som kan användas. Risker ska beskrivas i formen ”Risk för X, på grund av Y, vilket leder till Z”. En tydlig riskbeskrivning ökar möjligheten till gemensam förståelse för risken och underlättar vid bedömning av sannolikhet och konsekvens.
- **Riskanalys** handlar om att identifiera vilka negativa effekter som kan uppstå för en person eller verksamhet ur bolagets perspektiv om ett hot skulle bli verklighet. Vid bedömningen av riskvärdet används denna anvisnings skalor för sannolikhet och konsekvens, om det inte finns en tydlig anledning till att använda andra skalor.
- Vid **riskvärdering** placeras det sammanvägda riskvärdet i bolagets riskmatris. Värdet jämförs med fastställda nivåer i bolagets fastställda skala för riskacceptans vilken visar om och hur risken bör hanteras. Skalan fungerar som beslutsunderlag för vidare riskbehandling.

Riskbehandling

För de risker som ska behandlas måste *åtgärder* identifieras och genomföras. Målsättningen med riskbehandlingen är att risken ska kunna accepteras och dokumenteras. Processen innebär att säkerhetsåtgärder föreslås för att:

- **Välj åtgärd** – överväg om risken kan undvikas, om orsaken kan elimineras eller om sannolikheten/konsekvensen kan minimeras.
- Upprätta en **åtgärdsplan** baserat på föreslagna åtgärder. Planen ska innehålla beskrivning av åtgärder och förväntad effekt, ansvarig för genomförande, samt tidplan. Vid riskbehandling ska kostnaden för åtgärden vägas mot eventuell skada av inträffad händelse.

Åtgärder bör så långt som möjligt integreras i den ordinarie verksamhetsplaneringen.

Slutligen utförs en förnyad bedömning per risk, där sannolikhet och konsekvens efter föreslagen åtgärd uppskattas. Uppföljningsansvaret för implementering av beslutade säkerhetsåtgärder ligger hos riskägaren.

Riskbedömningen och åtgärdsplan dokumenteras i bolagets mall för riskanalys och förs in i aktuellt riskregister. Detta omfattar riskidentifiering, riskanalys samt riskvärdering samt åtgärder. Analysen diarieförs i enlighet med bolagets dokumenthanteringsplan. Information som ingår i riskhantering kan vara mycket känslig. Värdera om riskanalysen bör sekretessbeläggas med hänvisning till paragraf i offentlighet- och sekretesslagen.

Kommunikation, övervakning och utveckling

Resultatet av riskanalysen ska *kommuniceras* till relevanta intressenter och ledning. I samband med detta ska även riskägaren bedöma om det finns resultat i den genomförda (lokala) riskanalysen som ska lyftas till bolagets övergripande riskanalys. I kommunikationen ska det också tydliggöras vem som är riskägare för de identifierade riskerna.

Tänk på att analysresultat kan innehålla skyddsvärd information. Genomföra alltid en informationsklassning av materialet innan spridning.

Risker behöver löpande övervakas eftersom resultatet av riskbedömning och val av åtgärder kan påverkas av förändrade förutsättningar. Övervakning och översyn omfattar även analys och utvärdering av incidenter, förändringar, trender, framgångsfaktorer samt andra händelser som kan bidra till identifiering av nya framväxande risker. Det kan i sin tur resultera i nya åtgärdsbehov för att hantera organisationens risker. Att övervaka riskerna är också en viktig del i förbättring av bolagets riskhanteringsarbete.

Följa upp

För att säkerställa att riskhanteringsåtgärderna är verkningsfulla och relevanta behöver riskhanteringsarbetet följas upp. Verksamhetens riskägare ska regelbundet följa upp att beslutade åtgärder genomförs enligt plan och att de ger avsedd effekt. Riskregistret ska hållas levande och uppdateras vid väsentliga förändringar i omvärlden eller inom bolaget verksamheten. I den mån det är möjligt bör uppföljningsarbetet integreras med eller anpassas till andra uppföljningsaktiviteter inom organisationen, exempelvis genom att utgöra en del av organisationens övergripande verksamhetsplanering och verksamhetsuppföljning.

Förbättra

Genom att systematiskt identifiera vad som fungerat bra och vad som kan förbättras i själva riskprocessen bidrar vi till bolagets långsiktiga mål och stabilitet.

Förbättringsarbetet sker genom att omhänderta resultatet av uppföljningen. Det är nödvändigt att återkommande undersöka om rätt arbetssätt och metod används, om resurser och kompentens är tillräcklig och om det finns områden som behöver ytterligare fokus. Baserat på svaren på dessa frågor kan styrande dokument, vägledningar och arbetssätt förbättras.

Bilaga 1

Kompletterande material som stöd vid riskanalys avseende informationssäkerhet

Utgångspunkten är att först identifiera potentiella hot som skyddsvärda informationstillgångar kan utsättas för, för att sedan gå vidare och identifiera vilka sårbarheter som hoten kan utnyttja.

Därefter analyseras sannolikheten att hoten blir verklighet och deras potentiella konsekvens för verksamhet och individ. Det ingår även att planera för åtgärder för att behandla risken.

Riskhanteringsarbetet är en fortlöpande aktivitet som kräver regelbunden uppföljning och dokumentation. Riskhantering förutsätter ett löpande arbetssätt där det kan finnas behov av att gå tillbaka och komplettera med tillkommande risker och dokumentera genomförda säkerhetsåtgärder

Riskidentifiering

Att genomföra en noggrann riskidentifiering innebär ofta att kartlägga vilka resurser som är kritiska för verksamheten, till exempel kunddatabaser, affärssystem eller personalinformation. Man analyserar potentiella hot, såsom cyberattacker, naturkatastrofer eller interna misstag, och bedömer deras sannolikhet och möjliga effekter. Vidare identifierar man sårbarheter som svaga lösenord, gamla systemversioner eller bristande rutiner kring backup. Genom workshops, intervjuer och tekniska analyser samlar man in relevant information från både interna och externa källor. Syftet är att skapa ett underlag för prioriterade åtgärder, så att organisationen kan vidta rätt säkerhetsinvesteringar och förbättra sitt skydd mot framtida risker.

Följande behöver beaktas:

- Värdefulla informationstillgångar och resurser som kan drabbas av säkerhetsrisker
- Hot som kan orsaka skada, utifrån sannolikhet och konsekvens
- Sårbarheter, alltså brister i skyddet som hot kan utnyttja

Riskanalys

Riskanalys handlar om att identifiera vilka negativa effekter som kan uppstå för en person eller verksamhet om ett hot skulle bli verklighet. Vid bedömningen av riskvärdet används skalorna för sannolikhet och konsekvens.

Riskanalys handlar om att systematiskt kartlägga och utvärdera de konsekvenser som kan uppstå för individer, organisationen eller dess intressenter om ett identifierat hot skulle bli verklighet. Vid denna process används särskilda skalor för sannolikhet och konsekvens, vilket gör det möjligt att bedöma och rangordna riskerna utifrån hur troliga de är och vilken påverkan de kan få på verksamheten.

Analysen omfattar inte bara hoten i sig, utan även de sårbarheter och skyddsåtgärder som finns på plats. Genom att väga samman sannolikheten för att ett hot utnyttjar en sårbarhet

med de potentiella följderna, får organisationen en tydlig bild av sitt risklandskap. Det innebär exempelvis att en risk med låg sannolikhet men mycket allvarliga konsekvenser kan få hög prioritet för åtgärd, medan mindre allvarliga risker eventuellt kan accepteras.

Under riskanalysen tas även hänsyn till externa faktorer som förändringar i lagstiftning, teknisk utveckling eller nya affärsprocesser, vilka kan påverka hotbilden eller skapa nya risker. Genom att dokumentera och analysera dessa aspekter kan verksamheten fatta mer informerade beslut kring var resurser och säkerhetsåtgärder behöver stärkas, och vilka risker som kan accepteras inom ramen för den fastställda riskacceptansen.

Resultatet av en riskanalys ger insikt vilka risker bolaget berörs av och vad som händer om risken inträffar.

Riskvärdering

Vid värdering används en fastställd skala för riskacceptans vilken visar om och hur risken bör hanteras. Skalan fungerar som beslutsunderlag för vidare riskbehandling.

Det finns fyra principer som utgångspunkt vid värdering av risk:

1. **Rimlighetsprincipen**

En verksamhet bör inte innebära risker som med rimliga medel kan undvikas. Detta innebär att risker som med tekniskt och ekonomiskt rimliga medel kan elimineras eller reduceras alltid skall åtgärdas (oavsett risknivå).

2. **Proportionalitetsprincipen**

De totala risker som en verksamhet medför bör inte vara oproportionerligt stora jämfört med de fördelar (intäkter, produkter, tjänster, etc.) som verksamheten medför.

3. **Fördelningsprincipen**

Riskerna bör vara skäligt fördelade inom samhället i relation till de fördelar som verksamheten medför. Detta innebär att enskilda personer eller grupper inte bör utsättas för oproportionerligt stora risker i förhållande till de fördelar som verksamheten innebär för dem.

4. **Principen om undvikande av katastrof**

Händelsen kan om den inträffar accepteras om den drabbar resurser som kan hantera effekten än att händelsen resulterar i en katastrof. (dvs offra något för att mildra en större konsekvens)

Bilaga 2

Mall för genomförande av riskanalys (excel).

Läs instruktionen på första flikar i excelmallen.