Myndigheten för samhällsskydd och beredskap

EXEMPEL

Instruktion för riskhantering

– Region

Instruktion för riskhantering – Region

Enhet: CS-SI

Produktion: Advant

Publikationsnummer: MSB2090 – oktober 2022
ISBN: 978-91-7927-312-5

Innehåll

Instruktion för riskhantering

Inledning

En viktig del i riskhanteringsprocessen är riskanalys. Risker ska identifieras och analyseras, och ansvariga ska ta ställning till hur riskerna ska hanteras. Riskanalysen ska göras i förebyggande syfte och leda till att ett lämpligt val av skyddsåtgärder genomförs i syfte att minska verksamhetens risknivå.

Figur 1. Riskhantering

En riskanalys ska genomföras på ett metodiskt och strukturerat sätt, lämpligen i workshopform. Det är av stor vikt att deltagarna känner till det aktuella området väl och att de väljs så att alla nödvändiga riskperspektiv täcks in.

En riskanalys kan kort beskrivas som svaret på tre frågor:

- Vad kan hända?
- Hur sannolikt är det?
- Vad blir konsekvensen om det händer?
- En sårbarhetsanalys är svaret på varför det kan hända.

Använd mall ”Riskanalys”. Under flik Inledande information är avsedd för uppgifter om beställare av riskanalysen samt övrig information om riskanalysen.

Beskriv analysobjektet (projekt, process, rutin, organisation, system etc.) och dess avgränsning, så att det klart framgår vad som ska analyseras inklusive eventuella arbetsuppgifter, dess speciella omgivning och relationer till andra, eventuella specifika mål och kriterier.

Ange deltagare vid riskanalysen. Gruppen ska bestå av personer med kompetenser så att nödvändiga kunskapsområden täcks in.

Figur 2. Riskhanteringsmall

Inledande information			
1	**Beställare av riskanalysen** (Namn och kontaktuppgifter)		
2	**Namnge och definiera analysobjektet** (projekt, process, rutin, organisation, system etc. samt dess avgränsning) Även roller, ansvar och eventuella tidsperspektiv kan beskrivas här.		
3	**Datum för riskanalysen** (Första tillfälle och uppföljning)		
4	**Deltagare vid riskanalysen** (Namn och kontaktuppgifter)		
5	**Övrig information**		

Genomför riskanalysen enligt steg 1–3.

Överlämna analysen till beställaren för beslut om och genomförande av åtgärder (riskreduktion/kontroll).

Beställaren ansvarar för att följa upp de riskreducerande åtgärderna. Om effekten inte är den önskade, ska beställaren ta ställning till vilka ytterligare skyddsåtgärder som behöver genomföras.

Steg 1 – Analysobjekt, skyddsvärda tillgångar och identifiering av hot och sårbarheter

Inledningsvis kan analysobjektet utgå från vilka verksamheter och processer samt därtill hörande IT-tjänster som är mest verksamhetskritiska. Skyddsvärda tillgångar kan vara ett IT-system, information, personal, byggnader, en process. Utgå från kartläggning och verksamhetsanalys och omvärldsanalys för att identifiera lämpliga ingångsvärden till riskanalysen.

Se Instruktion Inledande kartläggning.

Figur 3. Hot- och sårbarhetsmall

Steg 1 - Identifiering av hot & sårbarheter				
Skyddsvärt Skyddsvärda tillgångar relevanta för analysen		**Hot** Möjlig, oönskad händelse med negativa konsekvenser		**Sårbarheter** Problem/brister/orsaker som ligger till grund för hoten
ID	*Tillgång*	*ID*	*Hot*	*Sårbarhet*
		1		
		2		
		3		

Hot

När skyddsvärda tillgångar identifierats är det dags att identifiera händelser som kan hota det skyddsvärda. Dessa hot dokumenteras i kolumn ”Hot”.

Risk/hotkälla - Ex. naturhändelser, stora olyckor, störningar i teknisk infrastruktur och försörjningssystem, handhavandefel samt antagonistiska händelser.

Som vägledning kan man fundera på om händelsen har sitt ursprung i följande:

- Människa – brister i utbildning, otydliga roller och ansvar, felaktigt handhavande, stress, slarv mm.
- Teknik – fel och buggar i mjukvara/hårdvara, installationsfel, fel i konfiguration, elavbrott mm.
- Natur – brand, översvämning, storm, kyla mm.
- Administration – rättsliga krav, interna styrdokument, rutiner, ansvar och roller, handböcker mm.

Brister kan sedan identifieras som sårbarheter se nedan.

Sårbarhet

Sårbarheter kan även ses som brister i uppfyllnad av de krav som ställs på verksamheten.

Inom informationssäkerhet återfinns krav främst i målgruppsanpassade styrdokument.

Sårbarheter kan identifieras inom följande områden:

- organisation
- processer och rutiner
- hanteringsregler
- personal
- fysisk miljö
- konfiguration av informationssystem
- maskinvara, programvara eller kommunikationsutrustning
- beroenden av externa parter.

Steg 2 – Riskbedömning, konsekvens och sannolikhet

En risk kan beröra flera tillgångar. En risk kan bero av flera sårbarheter. En sårbarhet kan ge upphov till flera risker. Analysobjektet kan vara mer eller mindre motståndskraftigt för en negativ händelse under sin livscykel vilket också bör vägas in.

Figur 4. Riskbedömningsmall

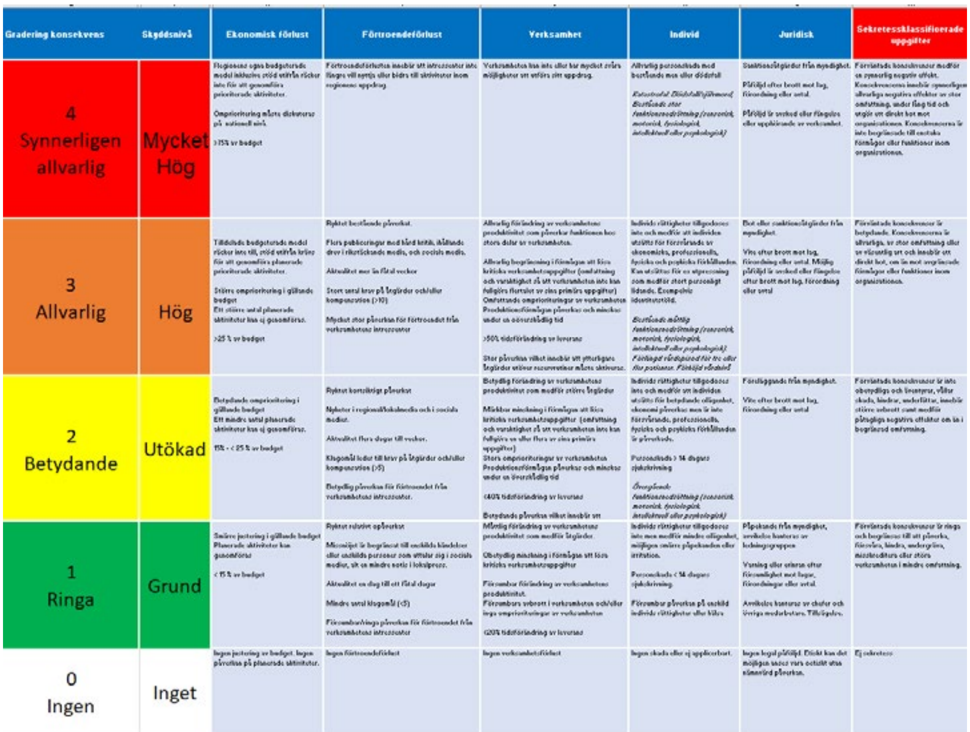
Konsekvensbedömning

Först görs en bedömning av hur stor konsekvens en händelse kan ha för verksamheten eller övriga intressenter och detta analyseras utifrån olika kategorier. Det kan vara en konsekvens som berör ekonomi, förtroende, verksamhet, individ eller legala påföljder. De olika konsekvenserna kan beskrivas men det är den högsta konsekvensen vars värde används i beräkning av risken. Ta stöd från kartläggning, verksamhetsanalys och omvärldsanalys för att identifiera kravställningar och förutsättningar.

Om tillgången som utsätts för hot redan har informationsklassats är det den konsekvensnivån som används. Det kan vara en klassning som är en aggregering av information som resursen hanterar som är dess klassning. Denna klassning är uppdelad på tre aspekter; Konfidentialitet, Riktighet och Tillgänglighet. Beroende av om risken avser någon av dessa aspekter är det just den nivå av konsekvens som används.

Bilden nedan ingår i mall för riskanalys.

Figur 5. Konsekvensbedömningsmallsexempel



Konsekvensbedömning avseende säkerhetsskyddsklassificerad information har lite annan beskrivning i sin gradering men följer samma princip och nivåer. Denna typ av information kan ha motsvarande samma säkerhetsåtgärder som för andra typer av information men säkerhetsåtgärderna mer strikt styrda och informationen ska vara åtskild och inte befinna sig i samma miljö som annan typ av information.

Sannolikhetsbedömning

Sannolikhetsbedömningen är ett mått på hur troligt det är att ett hot realiseras dvs att en oönskad händelse kan inträffa alternativt frekvensen av oönskade händelser. Detta har ett stort samband med allvarligheten i identifierade sårbarheter.

Bedömningen kan göras kvantitativt eller kvalitativt eller som en kombination av de två.

Kvantitativ bedömning

- Baserad på erfarenhet och statistik.

Kvalitativ bedömning

- Hotstyrka – motivation och förmågan hos hotkällor.
- Bedömning av befintliga säkerhetsåtgärder där en brist innebär en sårbarhet.

Bilden nedan ingår i mall för riskanalys.

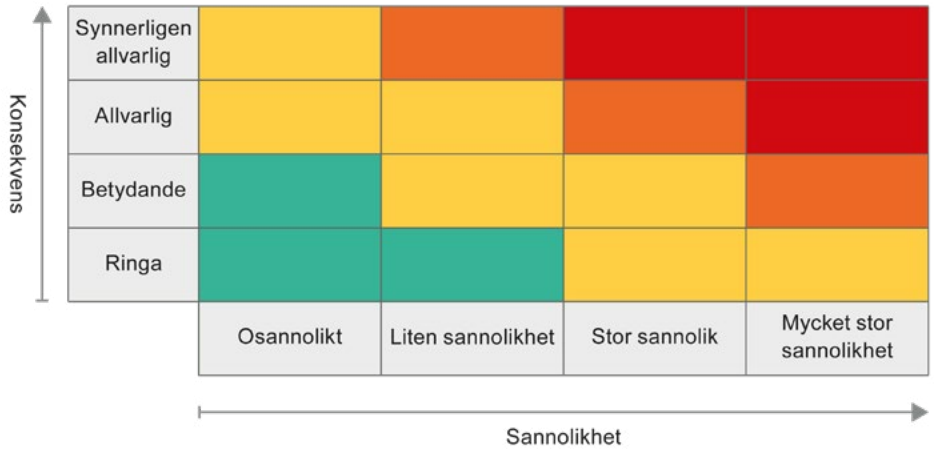
Figur 6. Exempel för sannolikheten att en risk inträffar

Sannolikhet		Kvantitativ bedömning	Kvalitativ bedömning	
4	Mycket stor sannolikhet	Inträffar en gång dygn	Sannolikheten är stor att det ska inträffa. Det är bekräftat att hotet är verklighet i väsentliga delar av verksamheten redan i dag eller att den väntas bli det i närtid.	Ett stort antal vitala säkerhetsåtgärder saknas eller är bristfälliga. Hotet är mycket kompetent
3	Stor sannolikhet	Inträffar en gång per vecka	Kan mycket väl inträffa men troligtvis inte särskilt frekvent. Det finns tydliga tecken på att hotet är verklighet i vissa delar av verksamheten redan i dag.	Ett antal vitala säkerhetsåtgärder saknas och eller är bristfälliga. Hotet är bedömt som kompetent.
2	Liten sannolikhet	Inträffar en gång på per månad	Inträffar sannolikt inte under normala omständigheter och i vart fall inte frekvent. Det finns vissa tecken på att hotet är verkligt i mindre omfattning i dag.	Ett mindre antal vitala säkerhetsåtgärder saknas eller några är bristfälliga.
1	Osannolikt	Inträffar en gång per år	Det finns mycket få eller inga tecken på att hotet är verklighet i dag.	Alla vitala säkerhetsåtgärder är på plats. Bristfälliga säkerhetsåtgärder kan ge obetydlig skada.

Riskvärde

Produkten av sannolikhet och konsekvens ger riskvärde. Använd mall för riskanalys. Denna kommer automatiskt ge riskvärdet.

Figur 7. Riskmatris



Prioritering och beslut om fortsatt hantering av risk

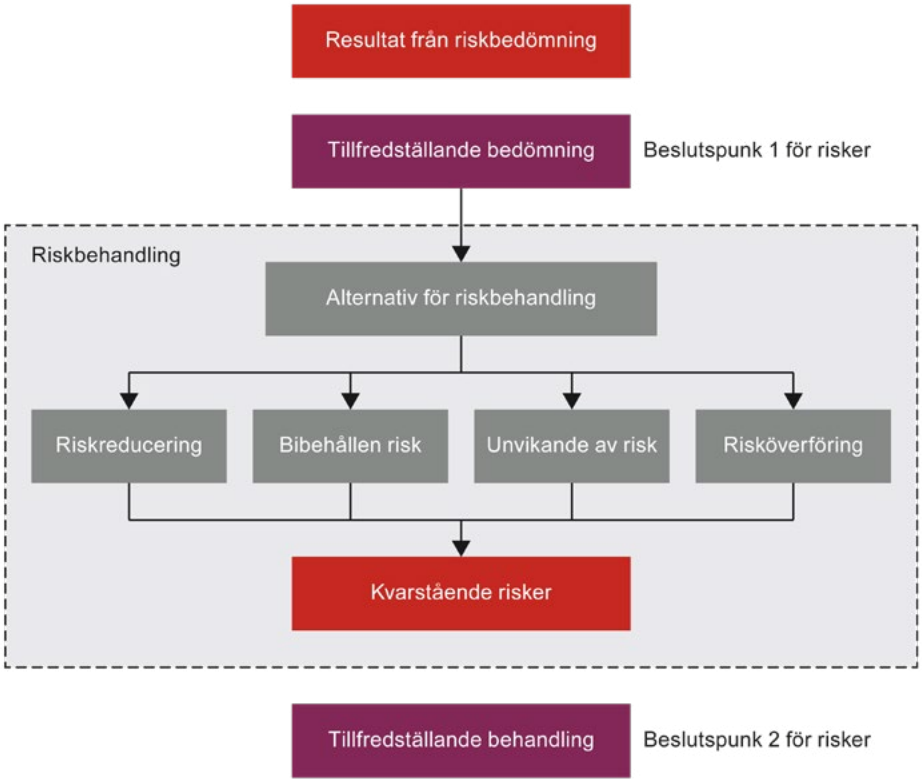
Riskägaren har det övergripande ansvaret för beslut om hur risken ska fortsätta hanteras och vilka åtgärder som ska genomförs.

Riskvärdet kan översättas till nivå av risk och därmed hur angeläget det är att risken prioriteras eller alternativt helt lämnas ohanterad.

Figur 8. Riskbedömningsmall

Steg 2 - Riskbedömning				
Konsekvensbeskrivning Beskrivning av de troliga konsekvenserna om hotet inträffar.	**Riskbedömning innan åtgärd**			**Fortsatt analys?** Vilka risker som ska vidare till steg 3?
Konsekvens	Konsekvens	Sannolikhet	Riskvärde	

Figur 9. Struktur för riskbedömning och riskbehandling



Alternativ för riskbehandling:

- Reducering – åtgärder för att reducera risk.
- Bibehåll – acceptera risken.
- Undvik – utsätt inte för risk – avbryt behandling.
- Dela – Försäkring mm.

Tabell 1. Nivåer för riskacceptans

Acceptabel nivå	Risker som inte kräver någon åtgärd alternativt bedömts som låga. Risken har värderats lågt och det har bedömts att den inte medför störningar i organisationen. Risk som kan accepteras men som ska bevakas. Dessa risker kan hanteras i den löpande verksamheten.
Medel nivå	Risker som behöver analyseras djupare. Riskerna ska bevakas i syfte att snabbt kunna sätta in åtgärd om händelsen inträffar.
Hög nivå	Höga risker som behöver åtgärdas. Dessa risker kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.
Oacceptabel nivå	Allvarliga risker som behöver åtgärdas snarast. Riskerna har värderats med hög sannolikhet eller hög konsekvens. Dessa risker kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.

Steg 3 – Riskbehandling

Med anledning av riskbedömningen har riskvärdet inneburit att fortsatt hantering av risken ska ske.

Förslag till åtgärdsplan

Skyddsåtgärder ska vidtas för att kontrollera och reducera risker som identifierats vid riskanalyser. Vid reducering av risk används de sårbarheter som har identifierats som förslag på åtgärder.

Förslag på åtgärder, ansvarig för åtgärd och tidplan tas fram och dokumenteras. Åtgärder ska vara konkreta, realistiska och möjliga att genomföra inom accepterad tidsram.

Figur 10. Riskhanteringsmall

Steg 3 - Riskhantering			
Åtgärdsförslag Vad kan göras för att eliminera, begränsa eller bevaka riskerna och dess sårbarheter?	**Ansvarig för åtgärd** Vem/vilka ansvarar för åtgärderna?	**Ägare risk** Vem äger risken och har övergripande ansvar för att åtgärderna genomförs?	**Tidplan** När ska åtgärden vara genomförd

Exempel på åtgärder:

- kunskapshöjande
- tekniska (lås, larm, kameror, kryptering, inloggning)
- administrativa (styrande dokument, processbeskrivningar)
- ekonomiska (omfördelning av budget, utökning av budget)
- personal (Extra resurser, undvika nyckelpersonsberoende).

Beslut om åtgärdsplan

Den som fattar beslutet måste också väga kostnaden för skyddsåtgärden mot kostnaden för eventuellt inträffad händelse och besluta i vilka fall det inte är relevant att vidta åtgärder, då det medför en högre kostnad än vad som kan motiveras utifrån konsekvens och kostnad för inträffad händelse.

Krav på dokumentation:

Beslut om godkännande ska dokumenteras. Av dokumentationen ska de överväganden som ligger till grund för beslutet framgå.

Dokumentationen ska vara tydlig och kunna förstås av personer som inte deltagit i arbetet. Läsaren ska genom dokumentationen kunna följa en risk från identifiering till behandling. Om inte sekretesskäl föreligger, ska dokumentationen av riskhanteringen kommuniceras till andra som kan ha nytta av den.

Uppföljning

Målet är att riskerna efter vidtagna skyddsåtgärder ska ligga på en acceptabel nivå. Avslutningsvis görs även en riskbedömning av sannolikhet och konsekvens om hotet inträffar efter genomförd skyddsåtgärd.

Figur 11. Riskuppföljningsmall

Uppföljning	Riskbedömning efter åtgärd		
Åtgärd genomförd?	Konsekvens	Sannolikhet	Riskvärde

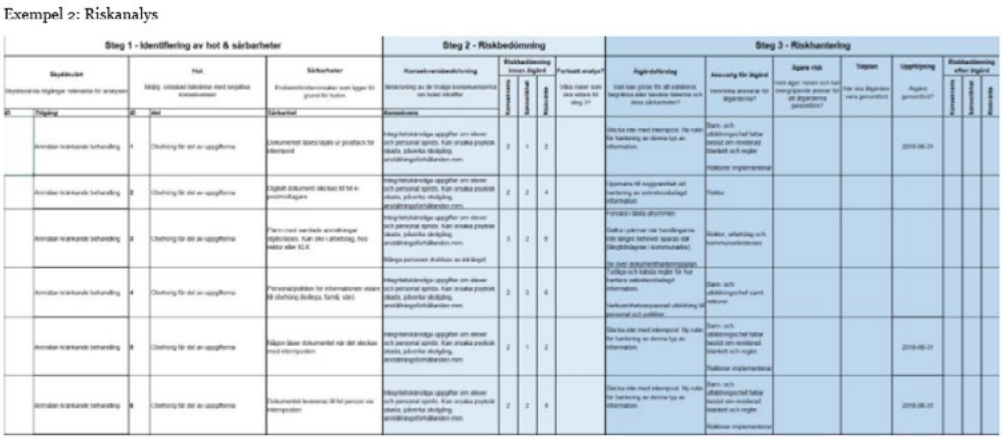
Om det inte finns tillgängliga riskhanteringsåtgärder eller om åtgärder inte leder till att risken förändras i tillräcklig utsträckning bör risken dokumenteras och kontinuerligt ses över.

För att kontrollera om effekten är den önskade ska genomförda aktiviteter och fattade beslut dokumenteras och följas upp.

Referensinformation

Det finns en beskrivning av hur arbetet med riskanalys har genomförts i en verksamhet. Detta återfinns i MSB metodstöd i bilagan Framgångsfaktorer och exempel. Organisationen har valt att använda samma verktyg för riskanalyser och nedan är ett utdrag från en ifylld riskanalys.

Figur 12. Exempel genomförd riskanalys



Exempel på riskanalys se sidan 6 i bilagan på MSB metodstöd1

1. https://www.informationssakerhet.se/siteassets/mediegalleriet/bilaga-framgangsfaktorer-och-exempel.docx.pdf

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**