Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

SLU Säkerhet
Anette Lindberg

STYRANDE DOKUMENT

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Anvisning/Instruktion	Beslutsdatum: 2014-01-14
Beslutsfattare: Per-Olov Skatt	Träder i kraft: 2014-01-14
SLU Säkerhet	Giltighetstid: tills vidare
Handläggare: Anette Lindberg	Bör uppdateras före: [Datum]

Ev dokument som upphävs: -

Instruktion för riskhantering

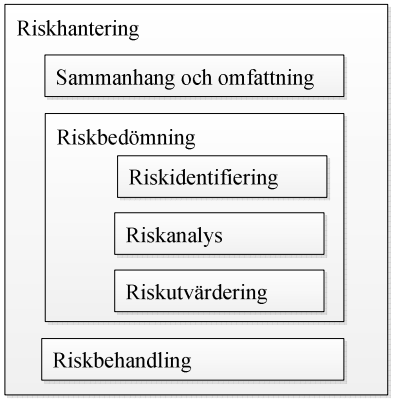
Syfte och avgränsning
Syftet med riskhantering är att identifiera, analysera, värdera och behandla de risker som kan komma att påverka verksamheten och dess värden alltför negativt.

Syftet med instruktionen är att beskriva processen för riskhantering, genomförandet i stort, ställa tankeväckande frågor och beskriva hur tillhörande mall kan användas. Instruktionen beskriver inte *när* riskhantering ska genomföras utan *på vilket sätt* den kan genomföras.

Beroende på om hela eller delar av beskriven riskhanteringsprocess ska genomföras kan hela eller delar av instruktionen och mallen användas, se exempel i kapitel ”Alternativ användning av modellen” på sid 7 i detta dokument.

Riskhantering

Denna instruktion har sitt ursprung i standarden SS-ISO-31000:2009 ”Riskhantering - Principer och riktlinjer som utgångspunkt” och har anpassats till SLU. Riskhanteringsprocessens huvudsakliga delsteg visas i bilden till höger och beskrivs i kommande kapitel. Med en miniatyrbild av standarden vid kapitlens inledning visas vilket delsteg i riskhanteringsprocessen som beskrivs. Instruktionen beskriver även genomförande i stort och på vilket sätt mallen bör fyllas i.



Riskhanteringsprocess enligt SS-ISO 31000:2009

Sammanhang och omfattning

Syfte

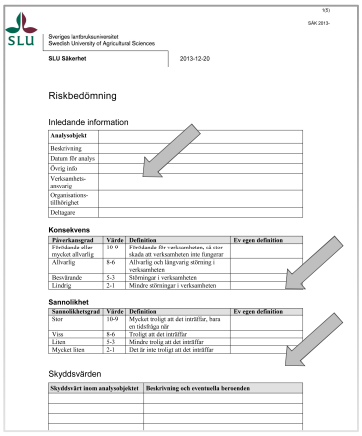
Riskhantering sker för ett avgränsat område, t.ex. verksamhet, projekt, system, område eller liknande. Detta kallas analysobjekt. För att förstå i vilket sammanhang riskhantering sker, ska analysobjektet identifieras, beskrivas och avgränsas samt och olika parametrar beskrivas.

Genomförande

Beskriv analysobjektet, dess speciella omgivning och relationer till andra, eventuella specifika mål och kriterier. Även roller, ansvar och eventuella tidsperspektiv kan beskrivas här.

Konsekvens- och sannolikhetsbedömning sker enligt en fyrgradig gradering i kombination med en tiogradig sifferskala för att nyansera bedömningen. Tänk igenom vilken kombination av konsekvens och sannolikhet (risknivå) som kan vara acceptabel för analysobjektet.

Mallen


Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

SLU Säkerhet 2013-12-20

Riskbedömning

Inledande information

Analysobjekt	
Beskrivning	
Datum för analys	
Övrig info	
Verksamhets-ansvarig	
Organisations-tillhörighet	
Deltagare	

Konsekvens

Påverkansgrad	Värde	Definition	Ev egen definition
Förskumlig allar mycket allvarlig	10 9	Förskumlig för verksamheten, så stor skada att verksamheten inte fungerar	
Allvarlig	8-6	Allvarlig och långvarig störning i verksamheten	
Besvärande	5-3	Störningar i verksamheten	
Lindrig	2-1	Mindre störningar i verksamheten	

Sannolikhet

Sannolikhetsgrad	Värde	Definition	Ev egen definition
Sker	10-9	Mycket troligt att det inträffar, bara en tidsfråga när	
Viss	8-6	Troligt att det inträffar	
Liten	5-3	Mindre troligt att det inträffar	
Mycket liten	2-1	Det är inte troligt att det inträffar	

Skyddsvärden

Skyddsvärt inom analysobjektet	Beskrivning och eventuella hotsenden

Namnge analysobjektet och beskriv det kort under *Inledande information*. Vidare anges datum och vilka personer som har deltagit i arbetet, kompletterat med deras kontaktuppgifter. Under *Övrig information* antecknas sådant som kan anses relevant för bedömningarna.

I de fall egna eller kompletterande kriterier för konsekvens- och sannolikhetsbedömning önskas användas, anges det till höger i tabellerna *Konsekvens* och *Sannolikhet*. T.ex. kan ekonomiska värden definieras vid konsekvensbedömningen och tidsaspekter definieras vid sannolikhetsbedömningen.

Att tänka på

Låg tolerans mot risk fordrar stora insatser vid behandling av risker, medan hög tolerans medför större risk för negativ påverkan. Det är viktigt att göra en avvägning mellan skyddsvärdet, riskbehandlingens kostnader och vad risken skulle innebära om den inträffar.

Riskbedömning

I riskbedömningen ingår riskidentifiering, riskanalys och riskutvärdering.

Riskidentifiering

Syfte

Här identifieras risker i form av händelser som kan leda till skada för analysobjektet och dess värden. Observera att den som är ansvarig för analysobjektet också är ansvarig för risken.

Genomförande

För att identifiera risker måste först analysobjektets värden identifieras, vidare kallade skyddsvärden. Skyddsvärde kan vara information, material, varumärke, byggnader, beställningar, nyckelpersoner, beroenden, apparatur osv.

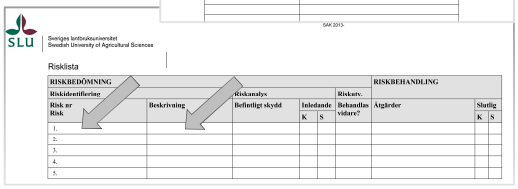
Därefter ska risker identifieras i form av händelser riktade mot dessa skyddsvärden.

Mallen


Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences
SLU Säkerhet 2013-12-20
Riskbedömning
Inledande information
Konsekvens
Sannolikhet
Skyddsvärden

Identifierade skyddsvärden noteras och kompletteras eventuellt med beskrivning, beroenden och prioritering i tabellen *Skyddsvärden*.

I *Risklista* skrivs risken in i formen ”Det finns risk för att…”. Uttryck risken i form av händelse som riktar sig mot analysobjektets skyddsvärden. Skriv risken mellan punkterna så uppdateras risklistan under riskmatrisen automatiskt för de sju första riskerna.
För att underlättar kommande bedömning och senare förståelse kan risken beskrivas utförligare under rubriken *Beskrivning*.


Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences
Risklista
RISKBEDÖMNING
RISKBEHANDLING
Riskidentifiering
Riskanalys
Risketv.
Risk nr
Risk
Beskrivning
Befintligt skydd
Inledande
K
S
Behandlas vidare?
Åtgärder
Slutlig
K
S
1.
2.
3.
4.
5.

Att tänka på

Observera att en kedja av händelser kan öka risken.
Även sammanhang och tillfälle påverkar konsekvenserna av en potentiell risk. En risk som inträffar vid ett tillfälle kan vara betydligt allvarligare än om den inträffar vid ett annat tillfälle, vilket gör att den kan behöva uttryckas som två olika risker. Även att inte tillvarata en möjlighet kan vara en risk. En risk kan vara mycket svårupptäkt. Eventuellt kan tidpunkt, dess omfattning och utbredning, följdhändelser beskrivas.

Nedan listas förslag på frågeställningar vid framtagande av skyddsvärden:

- Vad är viktigt? Vad är viktigast?
- Vilka mål, kritiska processer, prioriterade åtaganden och ömma punkter finns?
- Vad måste alltid fungera alternativt hur länge kan det vara borta?
- Vad är analysobjektet beroende av?

Nedan listas förslag på diskussionsfrågor vid riskidentifiering:

- Vad kan gå fel?
- Vad oroar du dig för?
- Vilka är de fem största riskerna?
- Vad ligger bakom inträffade incidenter? Fundera kring orsakerna.
- Vad händer i omvärlden?
- Finns det konflikter mellan skyddsvärden?
- För att förtydliga risken kan frågan ”varför skulle det inträffa” ställas.

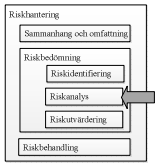
Nedan följer några kategorier på risker som kan användas vid riskidentifiering.

- **Finansiella risker:**
  - ✓ ränterisk, skatteregler, kreditrisk, valutarisk, kapitalförvaltningsrisk
- **Strategiska risker:**
  - ✓ legala hot (nya lagar och regelverk, ev. kommande lagstiftning)

- ✓ ny teknik (Cloud-computing)
- ✓ marknad och konkurrenter (marknadsekonomi, marknadstillväxt, priskrig, konkurreraande produkter och tjänster)
- ✓ politisk påverkan (politiska förändringar, EU-påverkan, mediabevakning)
- ✓ social påverkan (samhällsförändring, demografi, förändrat kundbeteende, kundmakt – krav – protest)

- **Operativa risker:**
  - ✓ interna processer (processrisker, organisation, management, intern kontroll, strategi)
  - ✓ humanfokus (arbetsmiljö, kompetens, resurser, etik och moral)
  - ✓ tekniska system (tekniska system, it-säkerhet, it-resurser, tillgänglighet)
  - ✓ externa hot (händelser kriser, miljöhot, kriminella hot)

Riskanalys

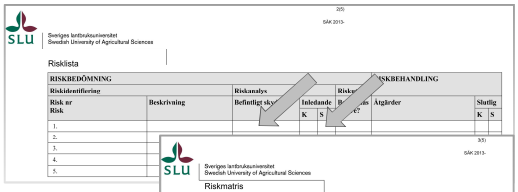


Syfte

Syftet med riskanalysen är att för varje identifierad risk bedöma både konsekvens och sannolikhet, dvs. vilka effekter en inträffad risk skulle få och hur sannolikt det är att risken inträffar. Konsekvens- och sannolikhetsbedömningarna möjliggör en tydlig redovisning och ett jämförande av risker riktade mot analysobjektet. För att kunna göra bedömningen är det viktigt att förstå risken, dess befintliga skydd och eventuella orsaker till att risken inträffar.

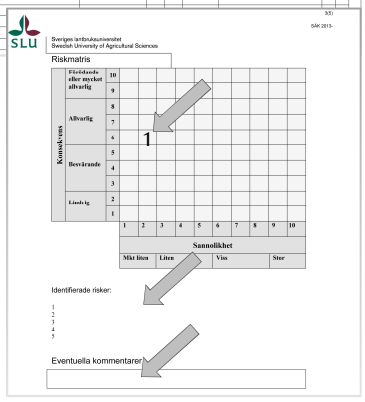
Genomförande

Det befintliga skyddet beskrivs övergripande. Därefter bedöms konsekvens för analysobjektet om risken inträffar och hur stor sannolikheten är att risken inträffar. Risken bedöms i förhållande till hur värdefullt skyddsvärdet är, dvs. vad det ger för fördel och nytta för analysobjektet och dess verksamhet.



Mallen

Fyll i *Befintligt skydd* och sedan *Inledande konsekvens* för risken i *risklistan*. Bedöm konsekvens utifrån de fördefinierade alternativt de egendefinierade bedömningskriterierna på sidan 1 och därefter sannolikhet på motsvarande sätt.
Bedömningen kan kompletteras med förklarande text under rubriken *Eventuella kommentarer* under *riskmatrisen*. Här kan även anges om det t.ex. är stor osäkerhet i bedömningen.
Skriv in riskens nummer i *riskmatrisen* utifrån inledande konsekvens- och sannolikhetsbedömning. För att undvika en i förväg bestämd accepterad respektive oaccepterad kombination av konsekvens och sannolikhet för riskerna, är *riskmatrisen* inte färgsatt i t.ex. rött, gult och grönt i förväg.
Lista gärna identifierade risker i tabellen under matrisen för att öka överskådligheten.



Att tänka på
Många faktorer kan påverka konsekvens- och sannolikhetsbedömningen: hur lätt risken upptäcks, hur stor del av analysobjektet som påverkas och hur kraftigt det påverkas, hur länge risken påverkar, vilket geografiskt område som påverkas, hur lätt det är att återställa, konsekvenser för samhället, vid vilken tid på året eller dygnet eftersom olika tidpunkter för inträffande kan ge olika konsekvenser.

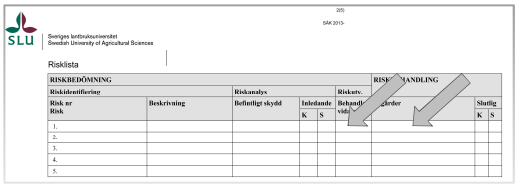
Riskägare har troligtvis störst insikt om risken och bör vara aktiv i bedömningarna.

Riskutvärdering

Syfte
Syftet med riskutvärdering är att identifiera vilka risker som kan accepteras som de är och vilka risker som kräver åtgärder för att risknivån, dvs kombination av konsekvens och sannolikhet, är oacceptabel för analysobjektet.

Genomförande
Utifrån bedömd konsekvens och sannolikhet pekas de risker ut som kräver behandling i form av t.ex. åtgärd, fördjupad analys, kontroll, övervakning eller att lyftas till annan nivå inom organisationen.

Mallen
I *risklistan* redovisas om riskerna ska behandlas vidare. Om svaret är ”ja”, fortsätt med *Riskbehandlingen.* I annat fall accepteras risken som den är.



Att tänka på
Om risken får en mycket hög risknivå kan det finnas anledning att lyfta risken inom organisationen.

Riskbehandling

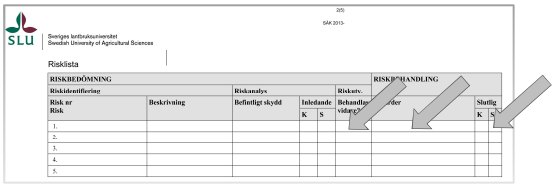
Syfte
Syftet med riskbehandling är att hitta åtgärder som påverkar riskens konsekvens och sannolikhet så att risken vidare kan anses acceptabel.

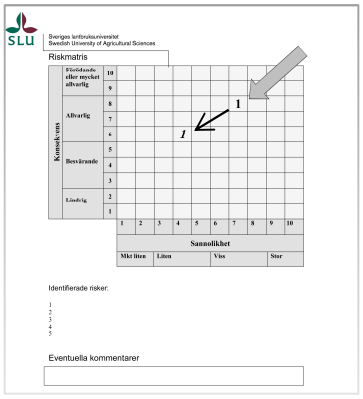
Genomförande
Identifiera förslag på åtgärder som kan eliminera, reducera, försäkra eller bevaka de oacceptabla riskerna. En risk kan bemötas av flera åtgärder och en åtgärd kan också bemöta flera risker.

Gör en förnyad konsekvens- och sannolikhetsbedömning av risken med de föreslagna åtgärderna inkluderade och avgör om den nya risknivån nu är acceptabel. Om inte, måste åtgärderna modifieras eller kompletteras. Sedan görs en ny konsekvens- och sannolikhetsbedömning tills risknivån anses acceptabel.

Mallen

För de risker som ska behandlas, dvs. ”ja” är angivet i rutan för *Behandlas vidare*, beskrivs en eller flera åtgärder. Därefter görs en förnyad konsekvens- och sannolikhetsbedömning för att avgöra om åtgärderna är anpassade till att bemöta risken på ett avvägt sätt, dvs. att risknivån blir acceptabel. Om risken fortfarande inte är acceptabel måste åtgärderna korrigeras eller kompletteras med ytterligare åtgärd. Dessutom kan risken behöva lyftas inom organisationen.





Riskens slutliga konsekvens- och sannolikhetsbedömning redovisas genom att risknumret skrivs i kursivt format i riskmatrisen och en pil från inledanade bedömning till slutlig bedömning visar hur riskvärdet förändras utifrån föreslagna åtgärder.

Åtgärder identifierade i *risklistan* skrivs in i *åtgärdslistan* och kopplas mot en eller flera risknummer. Ansvarig för åtgärden anges. Det behöver inte vara samma person som äger risken och inte heller samma som ska utföra åtgärden. Ange när åtgärden ska vara utförd och komplettera med uppföljningsdatum om åtgärden är omfattande, alternativt om den planerade klartiden är långt fram i tiden. Status för åtgärden fylls i, t.ex. ej påbörjad, påbörjad och slutförd. Åtgärdslistan kan med fördel användas i ett uppföljningsdokument.

Att tänka på

För att identifiera bra åtgärder är det viktigt att förstå orsaken till händelsen och inte bara dess symptom. Använd gärna ”Toyotas fem varför”, dvs. ställ frågan ”*varför skulle det kunna hända*” fem gånger så finns en stor möjlighet att kommer nära grundorsaken till händelsen. Diskutera även ”hur gör vi om verksamheten inte fungerar” och ”hur ska vi komma igång igen”. Vid val av åtgärder behöver aspekter som kostnadseffektivitet, lätthet i genomförande och ”tillräckligt bra” värderas. Räcker det t.ex. att minska sannolikhet eller konsekvens lite för att risken ska bli acceptabel eller måste risken helt elimineras?

Observera att föreslagen åtgärd kan leda till andra risker, antingen för egen eller för annans verksamhet.

Alternativ användning av modellen

Det är även möjligt att använda den här modellen på annat sätt. Till exempel kan analys behöva genomföras som pekar på risker om viss aktivitet eller liknande genomförs alternativt inte genomförs.

- Analysobjektet kan vara föreslagen ändring, t.ex. ”ombyggnation av befintlig byggnad”, ”ekonomisk aspekt på ny verksamhet inom SLU”. Beskriv var förändringen kommer genomföras, typ av förändring, berörda grupper osv.
- Skyddsvärdet kan vara bibehållen verksamhet, bibehållen miljö, säker arbetsmiljö, projektbudget etc.
- Risker identifieras mot dessa skyddsvärden, t.ex. ”det finns risk att verksamheten blir olönsam pga för få kunder”, ”det finns risk att utbyggnaden drar över budget pga underleverantörers låga bemanning”, ”det finns risk att verksamheten måste stängas pga att miljökontoret hittar oegentligheter” osv.
- Därefter bedöms konsekvens och eventuellt sannolikhet, åtgärder identifieras och förnyad konsekvens- och eventuell sannolikhetsbedömning genomförs.