Myndigheten för samhällsskydd och beredskap

EXEMPEL

Riktlinje riskhantering

– Region

Riktlinje riskhantering

Enhet: CS-SI

Produktion: Advant

Innehåll

Inledning

Det är viktigt att organisationen känner till, bedömer och hanterar de risker som kan inverka på möjligheten att uppfylla verksamhetens uppdrag och uppsatta mål.

Riskhantering är ett proaktivt systematiskt arbete för att kunna identifiera och prioritera åtgärder för att undvika en oönskad situation och ska användas för att leda och styra en organisation med avseende på risk. Att identifiera risker innebär även en beredskap för de åtgärder som krävs om en risk ändå inträffar. Om denna händelse påverkar vår förmåga att fortsätta vår verksamhet ska vi ha en beredskap i form av kriskommunikation och kontinuitetsplaner.

Figur 1. Samband mellan riskhantering, incidenthantering och kontinuitetshantering

Syfte och mål

Syftet med detta dokument är att tydliggöra ansvar och användningsområden för riskhantering samt specifikt för hantering av de risker som kan påverka förmågan att utföra regionens uppdrag och systematiskt hantera de risker som verksamheten kan utsättas för vid regionen. Detta inkluderar risker för information och resurser kopplat till informationshantering och bearbetning.

I enlighet med kommunallagen ska Regionens ledning säkerställa att det finns en intern styrning och kontroll som fungerar på ett betryggande sätt. Detta innebär att regionen bör arbeta aktivt med riskhantering i syfte att identifiera omständigheter som utgör en väsentlig risk för att regionen inte ska kunna fullgöra sina uppgifter, uppnå verksamhetens mål och uppfylla kraven på att verksamheten bedrivs effektivt.

Dokumentet kompletteras med beskrivning av grundläggande metodstöd och rutin för riskanalys.

Dokumentet ska årligen revideras.

Riskhanteringsprocess

Syftet med riskhantering är att med samordnade aktiviteter identifiera, analysera, värdera och hantera de risker som kan komma att negativt påverka en verksamhet och dess förmåga att uppfylla sina mål. Riskarbete är dessutom grundläggande för att uppnå ständiga förbättringar.

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

Figur 2. Riskhantering

Modellen ska tillämpas i all verksamhet och vara en del av beslutsunderlag vid åtgärder med anledning av risk samt vid all typ av förändring eller initiativ till nyutveckling av verksamhetsprocesser eller systemstöd.

Modellen har sin utgångspunkt från standarden SS-ISO-31000:2018 ”Riskhantering - Principer och riktlinjer samt SS-ISO/IEC 27005:2018 Riskhantering för informationssäkerhet.

Figur 3. Riskhanteringsprocess

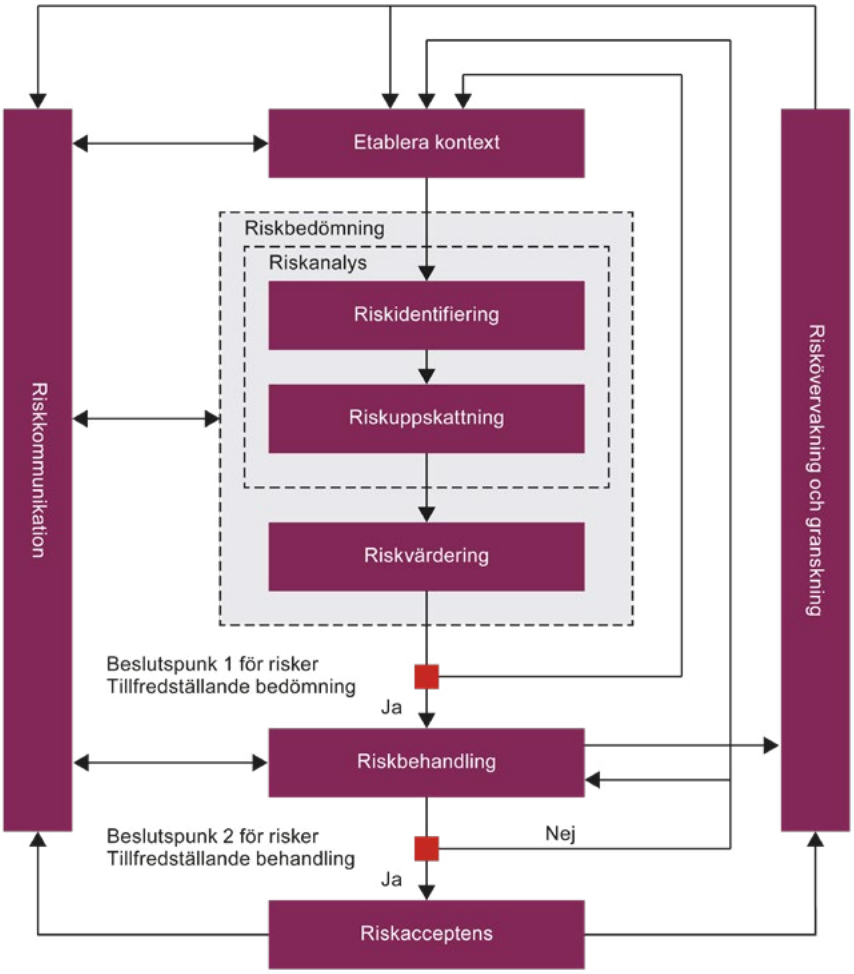


Bild av riskhanteringsprocessen ur standarden ISO 27005

Användningsområden

Riskhantering ska ingå i organisationens styrande processer så som planerings- och budgetprocess och att riskhantering finns som en återkommande punkt på ledningens agenda.

Riskanalys sker för ett avgränsat objekt eller ett område, t.ex. verksamhet, projekt, system, arbetsmiljö, miljö, intern kontroll, verksamhetsförändringar, säkerhetsfrågor eller liknande. Detta kallas analysobjekt.

Ett analysobjekt kan vara

- mål och budget samt verksamhetsplanering
- strategier och policyer
- verksamhetsprocesser
- organisationens funktioner och struktur
- krav enligt lämplig lagstiftning, föreskrifter och ingångna avtal
- riktlinjer för Informationssäkerhet
- organisationens övergripande metod för riskhantering
- informationstillgångar
- lokaliseringar av organisationens enheter och deras geografiska egenskaper
- begränsningar som påverkar organisationen
- intressenternas förväntningar
- extraordinära händelser
- särskilda händelser.

Riskhantering bör även ta hänsyn till angränsande områden/analysobjekt för samordning av åtgärder men även prioriteringar. Detta framgår av omvärld- samt verksamhetsanalyser.

Figur 4. Omvärlds- och verksamhetsanalys

Hantering av risker för specifika områden

Områden för riskhantering kan vara men är inte begränsade till:

Verksamhetens risker avseende förmåga inom krisberedskap

- RSA (MSBs förordning).

Verksamhetens risker avseende kärnuppdrag

- Metodstöd, uppfyllnad av uppdrag.

Verksamhetens risker avseende arbetsmiljö

- styrdokument, roller och ansvar, nyckelpersoner.
- resultat från skyddsronder, fackliga frågor, medarbetarundersökningar osv.

Verksamhetens risker avseende informationssäkerhet

- styrning, roller och ansvar, efterlevnad inkl dataskydd.
- IT-miljö, fysisk miljö och övriga resurser (projektrisker, bristande skydd, behov av förändring eller nyutveckling).

Specifikt risker vid personuppgiftsbehandlingar

- En organisation ska tillämpa processen för bedömning av risken för den personliga integriteten för att identifiera risker relaterade till behandlingen av personuppgifter. En organisation ska bedöma de potentiella konsekvenser för både organisationen och de registrerade som skulle bli resultatet om de risker som identifieras skulle uppstå.
  - Privacy Impact Assessment (PIA) Särskilda risker kopplat till personuppgiftsbehandling och privacy by design – åtgärder för skydd av personuppgifter (hantering och åtgärder i system).
  - Data Protection Impact Assessment (DPIA). Risker förknippade med riskfyllda personuppgiftsbehandlingar och uppfyllnad av dataskyddsförordningen.

Riskhantering för informationssäkerhet ska som minimum genomföras vid:

- etablering av nya IS/IT-system
- organisations-/processförändringar som kan påverka informationsbehandlingen
- tekniska förändringar i infrastruktur eller programvaror, som kan påverka informationsbehandlingen.

En väsentlig förändring kan ta sig uttryck på många olika sätt, men skulle exempelvis kunna vara när:

- ett befintligt informationssystem ska hantera uppgifter med en högre klassning än tidigare
- ett befintligt informationssystem ska integreras eller kommunicera med andra informationssystem.
- om molntjänster eller outsourcing av funktioner eller IS/IT-tjänst övervägs.

Ansvar

Ledningen har ansvar för att risker hanteras. Det övergripande ansvaret för kravställning och samordning av riskhanteringsarbetet kan delegeras inom organisationen. Det övergripande ansvaret innebär att vara sammanhållande för eventuell utveckling och förbättring av metodstödet för riskhantering.

Funktionen för ett sammanhållande ansvar förväntas eller är ålagda att:

- förstå vilka huvudsakliga risker som verksamheten står inför i sin strävan efter att uppfylla organisationens mål och uppdrag
- säkerställa att risker beaktas i tillräcklig utsträckning när mål sätts upp vilket sker i samband med den årliga verksamhetsplaneringen
- säkerställa att information om risker, och det sätt som de hanteras på, kommuniceras på lämpligt sätt.

Riskhanteringsgrupp

För att samordna riskhanteringsarbetet finns en riskhanteringsgrupp som består av ansvarig för samordning av organisationens risker, informationssäkerhetssamordnare, ansvarig för arbetsmiljö, Dataskyddsombud (DSO). Ytterligare personer kan ingå vid behov.

Riskhanteringsgruppen behandlar främst följande frågor:

- Utveckling av riskhanteringen och stödjande mallar och dokumentation.
- Beredning av frågor som rör riskstrategi, risktolerans, riskaptit och regelefterlevnad.
- Uppföljning av tidigare identifierade brister och bedömning av om de åtgärder som vidtagits för att avhjälpa dessa är effektiva och tillräckliga.
- Sammanställa och rapportera risker till högsta ledningen.

Ansvariga i organisationen

Ansvaret för riskhanteringen följer linjen, vilket innebär att respektive ansvarig ska integrera riskhanteringsprocessen och dess aktiviteter inom det egna området.

För att bereda beslut om åtgärder kan en riskhanteringsgrupp sättas samman där deltagare kan anpassas utifrån analysobjektet som riskanalys ska utföras.

Termer

Riskhantering
En systematisk process för identifiering och behandling av risker och som syftar till att verksamhetens uppdrag uppnås. I processen ingår följande delmoment:

- förberedelser
- riskidentifiering
- riskanalys
- riskvärdering
- riskbehandling
- uppföljning.

Riskbedömning
Den övergripande processen för riskidentifiering, riskanalys och riskvärdering

Riskidentifiering
Ett arbete som syftar till en kunskapsbaserad identifiering av risker i verksamheten. Detta innebär att upptäcka, förstå och beskriva risker som kan bidra till eller förhindra att målen uppfylls.

Riskanalys
En grundlig beskrivning av risk, av dess orsaker, egenskaper och av vilka konsekvenser den kan få för verksamheten och dess måluppfyllelse. Riskanalysen omfattar noggrant beaktande av osäkerheter, riskkällor, konsekvenser, sannolikhet, händelser, scenarion, riskhanteringsåtgärder och vilken effekt de har. En händelse kan ha flera orsaker och konsekvenser och kan påverka flera mål.

Riskvärdering
Gradering av de identifierade riskernas sannolikhet och konsekvens. Ska ge stöd vid beslut om hur en risk ska behandlas; utredas vidare åtgärdas eller om andra faktorer ska ifrågasättas som att ompröva mål.

Riskbehandling
Kan omfatta ett eller flera av följande alternativ:

- Att undvika risken genom beslut om att inte inleda eller fortsätta med den aktivitet som ger upphov till risken.
- Att ta eller öka risken för att kunna tillvarata en möjlighet.
- Att eliminera risk/hotkällan.
- Att förändra sannolikheten.
- Att förändra konsekvenserna.
- Att dela risktagandet (t.ex. genom avtal eller genom att teckna försäkringar).
- Att bibehålla risken genom att fatta informerade beslut.

Risk/hotkälla
Faktor som i sig självt eller i kombination har potential att utgöra en risk. Kan delas in i olika hotgrupper.

- För informationssäkerhetsrisker se bilaga C i ISO 27005:2013.

Hot
En oönskad händelse eller omständighet som kan ge negativa konsekvenser för verksamheten och dess möjligheter att utföra sitt uppdrag och att uppnå sina mål.

Konsekvens
Resultat av en händelse med negativ inverkan för verksamheten eller övriga intressenter. Kan vara ekonomisk, dåligt anseende eller t ex legal påverkan.
Se konsekvensmatris.

Sårbarhet
Bristande förmåga hos en organisation, en process eller ett IT-system, att motstå och återhämta sig från olika former av påfrestningar. Bristen kan uttryckas som ett gap i förhållande till kravställning.

Sannolikhet
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.

Risk
Produkten av sannolikhet och konsekvens för att ett hot realiseras. Dvs möjligheten att ett hot eller annan oönskad händelse ska inträffa och de skadliga konsekvenserna därav. Risker uttrycks ofta som riskkällor, potentiella händelser, dess konsekvenser och dess sannolikhet.

- Informationssäkerhetsrisk innebär möjligheten att ett givet hot utnyttjar sårbarheten hos en informationstillgång eller en grupp av informationstillgångar och därigenom orsakar organisationen skada.

Risktolerans

Riskaptiten är den nivå för risk som organisationen är beredd att acceptera i syfte att nå uppsatta mål.

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.

Det finns tre 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)

Riskbehandling

För genomförande av riskanalys och därtill riskbehandling finns ett bifogat metodstöd.

Vid framtagning av konsekvensmatris samt riskmatris och därmed riskbehandling utgår man från riskkategorier och risktolerans.

Risker som inte innebär en negativ konsekvens kan ses som positiva risker. Dessa risker lämnas helt och behandlas inte varför de inte är upptagna i riskmatrisen.

Bedömning av vad som är en acceptabel nivå ska göras utifrån

- verksamhetens interna krav
- lagstiftning och andra externa krav
- kostnaden för att vidta skyddsåtgärder jämfört med kostnaden om risken förverkligas.

Processen för godkännande av risk ska minst innefatta:

- kontroll av att gällande regler följs
- analys av om risknivåer kan öka eller om nya risker kan uppstå
- kontroll av att det finns tillräckligt med personal och tillgång till kompetens, interna regler, verktyg och processer i verksamheten samt stöd- och kontroll-funktioner för att kunna förstå och övervaka riskerna.

Riskmatris

Skala för acceptans

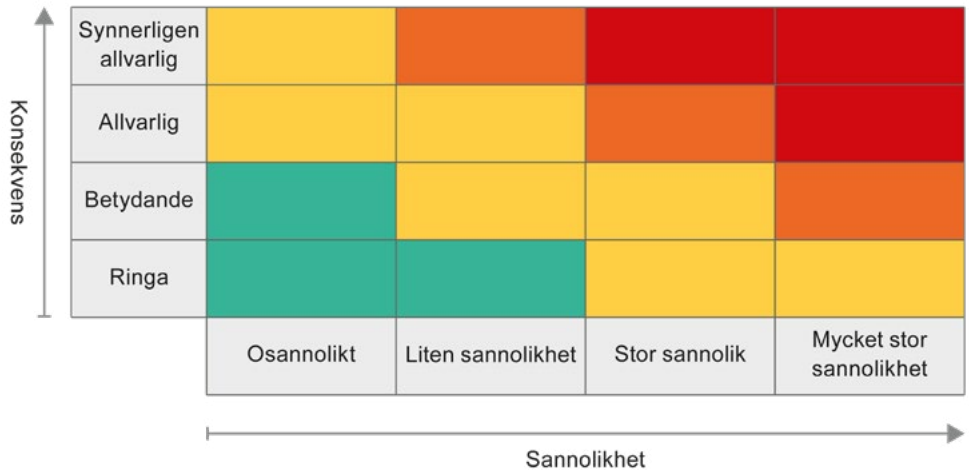
När riskanalys genomförs bör följande skala användas för att bedöma om en risk kan accepteras eller inte.

Tabell 1. 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.

Riskmatrisen nedan kan användas för att få en grov överblick över de risker som identifierats. Färgerna i riskmatrisen beskriver om en risk är acceptabel eller inte enligt toleransnivåerna, se ovan.

Figur 1. Riskmatris



Övervakning och granskning

Planer som är kopplade till de risker som identifierats, värderats och bedömts som väsentliga ska följas upp. Resultatet av dessa uppföljningar ska dokumenteras och kommuniceras till andra som kan ha nytta av att känna till det.

Riskkommunikation

Rapportering av verksamhetsrisker, ska rapporteras till närmast ansvarig och övergripande till ledningen.

Vid beslut om förändring i process eller IT-system ska det fastställas vilken funktion eller organisatorisk enhet som ska ansvara för att hantera risker förenade med dessa.

Eskalering av hot och risker

Hot och risker som inte kan hanteras av beställaren ska eskaleras till ledningen för beredning och därefter beslut i enlighet med delegationsordning.

Riskhantering och kontinuitetshantering

Kontinuitetshantering syftar till att prioritera och införa förebyggande skydd för att undvika otillgänglighet av resurser och tjänster.

Detta innebär att verksamheten ska klassificera vilka verksamheter och processer samt därtill hörande IT-tjänster som är mest verksamhetskritiska.

Kontinuitetshanteringen ska identifiera och hantera risker som kan leda till allvarliga störningar eller avbrott i leveransen av dessa tjänster samt ta fram åtgärdsplaner för att undvika otillgänglighet eller minimera konsekvenserna. I kontinuitetshanteringen ingår även att ta fram planer om en otillgänglighet uppstår.

Myndigheten för
samhällsskydd
och beredskap

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