Myndigheten för samhällsskydd och beredskap

En vägledning för arbete med riskhantering

Ett stöd riktat till dig som ska leda arbetet med riskhantering för samhällsviktig verksamhet

GUL-markerad text är referenser till ej befintliga hemsidor eller ej ännu publicerade dokument. Åtgärdas före publicering av lathunden.

En vägledning för arbete med riskhantering – Ett stöd riktat till dig som ska leda arbetet med riskhantering för samhällsviktig verksamhet

Enhet: Enhet

Foto omslag: Foto omslag
Text: Text/Författare
Tryck: Åtta45

Publikationsnummer: MSBxxxxx - månad år
ISBN-nummer: ISBN
Tidigare utgiven: Datum

Om materialet

Det här metodstödet vänder sig till dig som ska leda processen eller arbeta med riskhantering för samhällsviktig verksamhet i din organisation. Materialet är i första hand tänkt som ett stöd i ditt arbete och ska ses som förslag på hur en organisation kan arbeta med riskhantering, till exempel inom ramen för arbetet med motståndskraft i samhällsviktig verksamhet.

Begreppen risk och riskhantering är mycket breda och kan betraktas utifrån flera perspektiv. Syftet med denna vägledning är att ge stöd i systematiskt arbete med riskhantering som utgår från standarden ISO 31000:2018 – Riskhantering – Vägledning. Det finns flera regleringar och processer som styr arbete med risker. Den här vägledningen riktar sig främst till aktörer som tillhandahåller samhällsviktig verksamhet. Den kan även utgöra ett stöd till aktörer gällande andra riskanalyser, exempelvis utifrån:

- Förordning (2022:524) om statliga myndigheters beredskap.
- Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.
- CER-direktivet.[1].

Allt stödmaterial som vägledningen hänvisar till finns på www.msb.se/riskhantering.

Har du frågor om metodstödet är du välkommen att kontakta oss på riskhantering@msb.se.

[1] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.
Direktivet om kritiska entiteters motståndskraft (Critical Entities Resilience Directive, CER-direktivet), syftar till att minska sårbarheter och stärka motståndskraften hos samhällsviktig verksamhet (kritiska entiteter) inom EU.

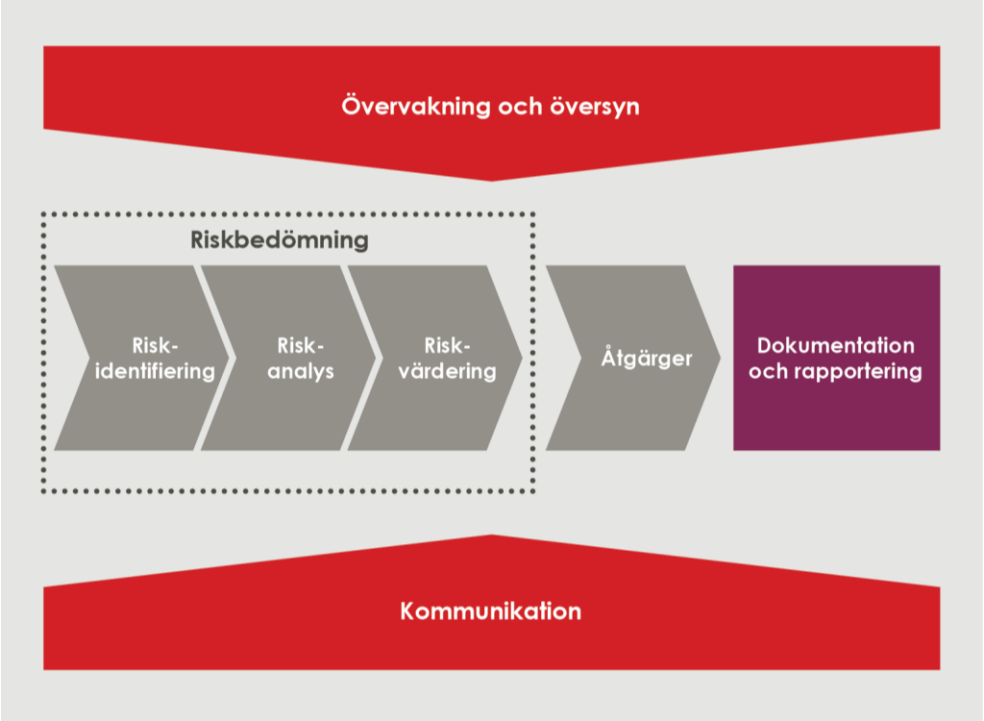
Innehåll

Vad är riskhantering?

Riskhantering är den systematiska process som identifierar, analyserar, värderar och hanterar risker. Risker är effekten av osäkerheter på en organisations mål. Det finns många olika typer av risker. Exempelvis finansiella risker, miljömässiga risker, varumärkesmässiga risker, eller vardagliga avbrottsrisker. Denna vägledning riktas i första hand till de organisationer, privata och offentliga, som arbetar med samhällsviktig verksamhet. I den bemärkelsen är risker och riskförståelsen framför allt något negativt antingen för upprätthållandet av den samhällsviktiga verksamheten som kan påverkas av en risk som inträffar eller för samhället i stort. Hanteringen av en risk i denna kontext syftar till att eliminera eller minska sannolikheten för att risken inträffar och/eller konsekvenserna av att den inträffar.

Genom att arbeta systematiskt med riskhantering kan sannolikheten för, och konsekvensen av, negativa händelser minimeras. Det är viktigt att riskhanteringsarbetet integreras i organisationens ordinarie processer eftersom det utgör en viktig del i en organisations samlade civila beredskapsarbete.

Figur 1 Riskhanteringsprocess

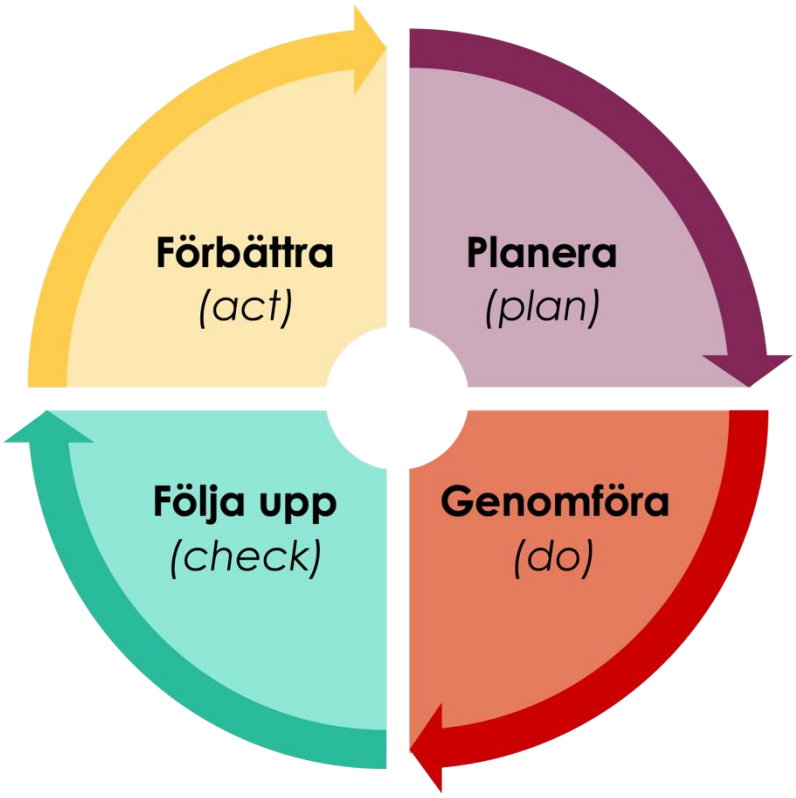


Principer för riskhantering

Processen för riskhantering omfattar enligt ISO 31000:2018 åtta övergripande principer som tillsammans utgör grunden för hantering av risker. Dessa ska därför beaktas när styrdokument, ramverk och processer för riskhantering ska utformas i organisationen.

Tabell 1 Text

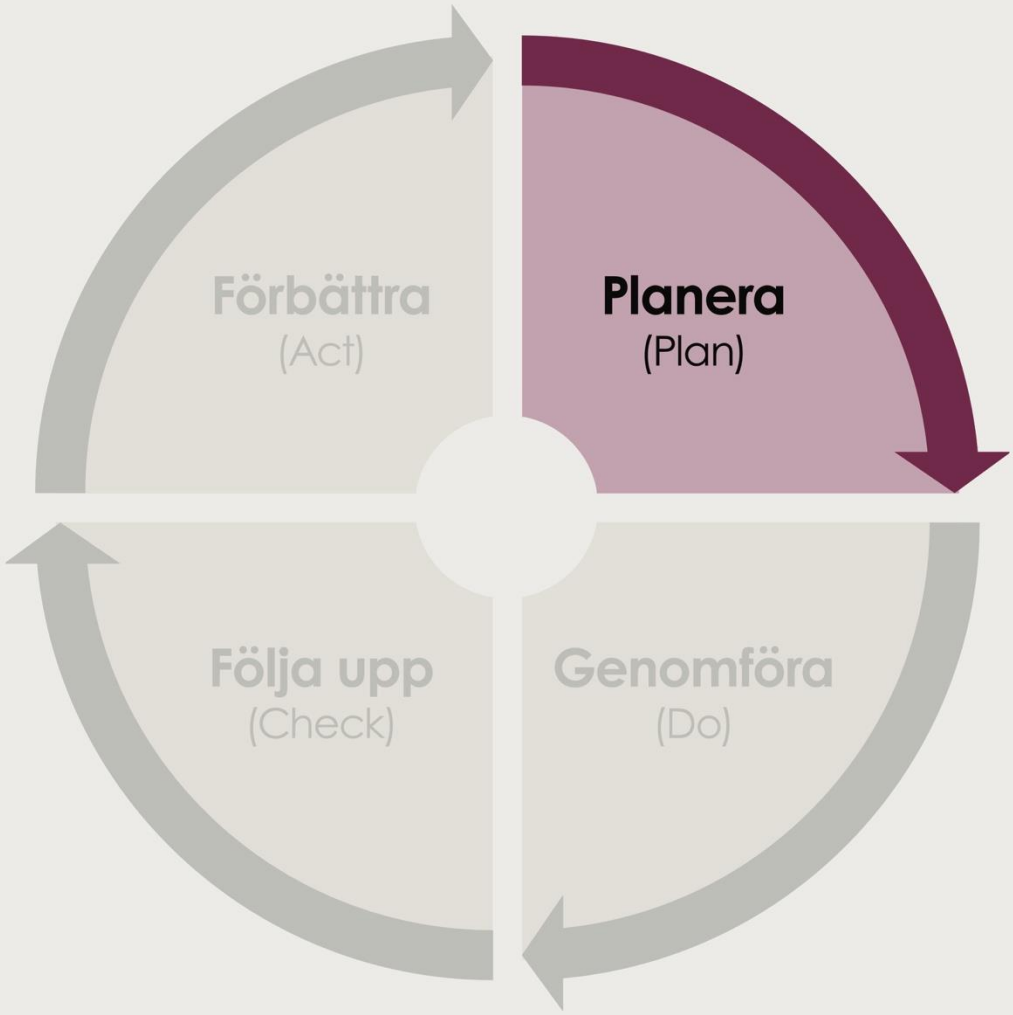
Titel	Titel
Integrerad	Riskhantering är en integrerad del av alla organisatoriska aktiviteter.
Strukturerad och heltäckande	Ett strukturerat och heltäckande tillvägagångssätt bidrar till konsekventa och jämförbara resultat.
Anpassad	Ramverk och processer för riskhantering är proportionerligt anpassade till organisationens externa och interna förutsättningar samt kopplade till mål.
Inkluderande	Att involvera intressenter på ett lämpligt och tidsanpassat sätt säkerställer att deras kunskaper, synpunkter och åsikter beaktas.
Dynamisk	Risker kan uppkomma, förändras eller försvinna om förutsättningar förändras. En dynamisk riskhantering kan dock förutse, upptäcka, fastställa och svara på sådana förändringar.
Bästa tillgängliga information	Underlag till riskhantering baseras på historiska och aktuella uppgifter samt prognoser. Hänsyn tas till begränsningar och osäkerhetsfaktorer. Intressenter ska få ta del av aktuell information.
Mänskliga och kulturella faktorer	Mänskliga beteenden och kulturella faktorer har en betydande inverkan på alla aspekter av riskhantering, på alla nivåer och i alla steg.
Ständiga förbättringar	Riskhantering förbättras ständigt genom lärande och erfarenhet.



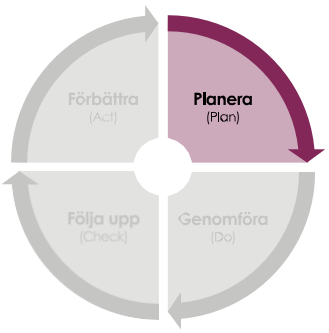
Hur genomförs arbetet på bästa sätt?

Arbetet med riskhantering kan med fördel följa den cykliska modellen Plan-Do-Check-Act (PDCA). På så vis blir arbetet med riskhantering strukturerat och systematiskt.

Vägledningen kommer att guida läsaren genom respektive del, i enlighet med PDCA-modellen, med tips på tillvägagångssätt, stödmaterial, fördjupande material och exempel.



Planera



Planera

Vad är viktigt att tänka på innan arbetet börjar?

Det är viktigt att planera organisationens arbete med riskhantering innan själva arbetet inleds. Arbetet med riskhantering samordnas lämpligen med andra liknande processer inom organisationen, till exempel arbetet med kontinuitetshantering, informations- och cybersäkerhet eller inom andra lagstiftningsområden.

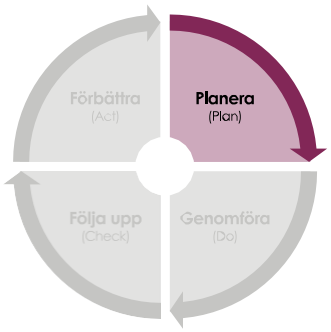
Eftersom riskhanteringsprocessen kan bedrivas på flera nivåer inom en organisation är det viktigt att följande punkter är genomförda innan organisationen påbörjar *Genomföra*-fasen:

- Bestäm övergripande syfte och mål samt ambitionsnivå med arbetet. Det behövs för att säkerställa att det sker inom ramen för organisationens mål.
- Bestäm omfattningen på arbetet, till exempel vilka delar av organisationen som ska ingå och vilka resurser som tilldelas för arbetet.
- Identifiera kontexten för arbetet, till exempel relevanta intressenter och lagkrav
- Fastställ nivåer för sannolikhet och konsekvens.

Det är viktigt att dessa delar inkluderas i organisationens policy och eventuellt tillhörande riktlinjer för arbetet, se nästa avsnitt.

Tänk på att planeringsarbetet ska göras på en organisatorisk nivå för att skapa förutsättningar för samordning mellan olika verksamheter och processer.

Viktigt att ta med inför arbetet:
Tänk på att göra en informationsklassning av materialet och att resultatet från arbetet kan generera konfidentiell skyddsvärd information som inte kan spridas till obehöriga.
Rekommendationer om informationssäkerhet finns på https://metodstod-informationssakerhet.msb.se/



Planera

Vikten av förankring och mandat

Riskhantering ska vara en systematisk, dynamisk och iterativ process. Riskhanteringsprocessen bör även stödja organisationens befintliga styrmodell eller styrprocess för att på ett naturligt sätt integreras i organisationens arbete.

Genom att förankra arbetet hos ledningen och få mandat för att driva arbetet, skapas förutsättningar för att verksamheten kan avsätta resurser för arbete med riskhantering. En viktig del är också att såväl ledning som verksamhet förstår nyttan med arbetet. Det ökar sannolikheten för att verksamheter avsätter resurser för att bidra till arbetet.

Ledningens ambitioner med riskhantering kan med fördel beskrivas i en policy som sätter ramarna för arbetet. Det kan vara ett fristående styrande dokument, exempelvis ett ramverk, eller ingå som en del i övergripande dokument gällande exempelvis styrdokument för civil beredskap eller säkerhetsarbete. I policyn beskrivs bland annat organisationens syfte och mål med arbetet, kontext och avgränsningar, riskacceptans, ansvar och roller samt hur risker ska rapporteras.

Din organisation kan även ta fram riktlinjer och rutiner som kompletterar policyn och som mer detaljerat beskriver hur arbetet ska genomföras, till exempel genom att ange vilken metod som ska användas för riskbedömningen, inklusive nivåer för sannolikhet och konsekvens (se nästa sida).

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 5–6

Avsnitt 5.2 Ledarskap och engagemang

Avsnitt 5.3 Integrering

Avsnitt 5.4 Utformning

Stöddokument & fördjupning

MSB: Checklista

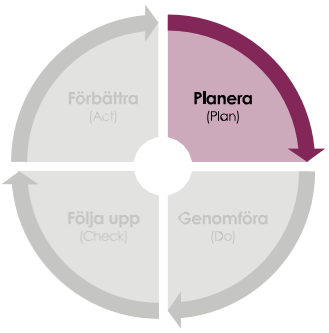
MSB: Skydd av samhällsviktig verksamhet – Ökad motståndskraft genom arbete med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och hantera oönskade händelser (MSB2401)

MSB: Fördjupning – Kontinuitetspolicy och riktlinjer (MSB1414 – reviderad december 2023).

MSB: Informationssäkerhet – Metodstödet – Utforma styrdokument, https://metodstod-informationssakerhet.msb.se/sv/utforma/styrdokument.

MSB: www.msb.se/rsa

www.msb.se/riskshantering.



Planera

Förbered genom att ta fram nivåer för sannolikhet och konsekvens

En viktig del i arbetet är att ta fram och besluta om nivåer för sannolikhet och konsekvens. Dessa är användbara verktyg som hjälper en organisation att analysera och värdera risker på ett likartat sätt.

Om riskbedömningar ska genomföras i en organisation med flera verksamheter[2] och utföras av olika personer rekommenderas att ta fram nivåer med beskrivningar för sannolikhet och konsekvens, se ytterligare stöd under *Stöddokument & fördjupningar*.

Nedan beskrivs en grundläggande modell om nivåer för sannolikhet och konsekvens.

Sannolikhet

Sannolikhet kan beskrivas med ord eller utifrån i förväg definierade nivåer, som i skalan nedan. Nivåerna sannolikhet bör även kvantifieras på ett objektivt sätt för att riskerna ska vara jämförbara.

Numrering av sannolikhet kan också ge ett förtydliga nivåer och underlätta i jämförande av risker. Ett exempel på hur sannolikhet kan definieras återfinns nedan:

Ett exempel kan vara risken för översvämning där sannolikheten för detta kan beskrivas som *inträffar 1 gång på 10 år*. Utifrån de förvalda nivåerna för

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 10–13

Avsnitt 6.3 Omfattning, förutsättningar och kriterier Ledarskap och engagemang

Avsnitt 6.4 Riskbedömning

Stöddokument & fördjupning

MSB: Fördjupning kriteriemodell (MSB2152 – december 2022).

MSB: Informationssäkerhet – Metodstödet – Utforma: Riskhantering, https://metodstod-informationssakerhet.msb.se/sv/utforma/riskhantering.

MSB: Informationssäkerhet – Metodstödet – Utforma: Klassningsmodell, https://metodstod-informationssakerhet.msb.se/sv/utforma/klassningsmodell.

www.msb.se/riskshantering.

[2] I detta sammanhang ska verksamhet förstås som ett vidare begrepp. Läs mer om samhällsviktig verksamhet Metod för identifiering av samhällsviktig verksamhet (ISBN-nummer 978-91-7927-450-4).

sannolikhet i skalan i tabell 2 skulle denna beskrivning kunna översättas till nivån *Trolig*.

Tabell 2 Text

Sannolikhet	Osannolikt 1	Mindre trolig 2	Trolig 3	Nästan säker 4
Sannolikhet eller frekvens	1 gång per 50 år – 1 gång per 100 år	1 gång per 10 år – 1 gång per 50 år	1 gång per 1 år – 1 gång per 10 år	1 gång per år eller oftare

Konsekvens

Konsekvens kan beskrivas med ord eller utifrån i förväg definierade nivåer, som i skalan nedan.

Även nivåerna för konsekvens bör kvantifieras på ett objektivt sätt för att riskerna ska vara jämförbara.

Ett exempel kan vara risken för översvämning där konsekvensen för detta kan beskrivas som *25–50% av infrastruktur har skadats inom ett begränsat område*. Utifrån de förvalda nivåerna för konsekvens i skalan nedan skulle denna beskrivning översättas till nivån *Allvarlig*.

Tabell 3 Text

Konsekvens	Försumbar 1	Måttlig 2	Allvarlig 3	Katastrofal 4

Genom att numrera nivåerna för sannolikhet och konsekvens underlättas en beräkning av riskens värde, dvs riskvärde. Ett *riskvärde* är riskens sammanvägda värde av både värdet för sannolikhet och värdet för konsekvens (t.ex. sannolikhet 3 x konsekvens 4= riskvärde 12). Riskvärdet ger en översikt som gör det enklare att utifrån en helhetssyn prioritera risker, vilket möjliggör att riskförebyggande åtgärder kan riktas och prioriteras på effektivast möjliga sätt.

Kriteriemodell

Konsekvenstyper kan även utvecklas i en kriteriemodell, se exempel i tabell 4. Genom att ta fram en kriteriemodell där olika konsekvenser beskrivs skapas en samsyn i organisationen kring vad som menas med exempelvis ”allvarlig” konsekvens.

En kriteriemodell möjliggör att organisationen bedömer konsekvenser på likartat sätt. På så vis minskar risken för subjektiva konsekvensbedömningar samtidigt som det är en viktig förutsättning för att riskernas bedömning bygger på samma grund och kan jämföras med varandra.

Exempel på konsekvenstyper som kan användas är *liv och hälsa, förtroende, ekonomi, leveranssäkerhet* eller *samhällets funktionalitet*. Dessa bör baseras på parametrar som är viktiga för organisationen.

Tabell 4 Text

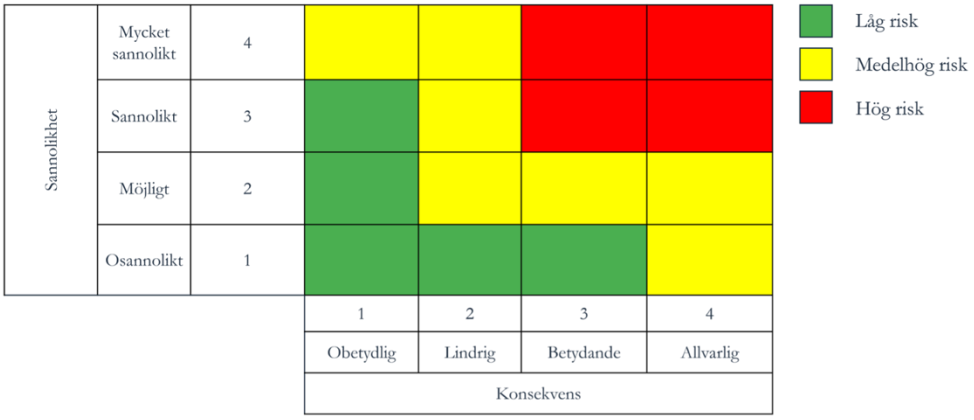
Titel	Obetydlig	Lindrig	Betydande	Allvarlig
Förtroende	Förtroendet är opåverkad och det finns inga negativa inslag i media.	Viss påverkan på förtroendet, enstaka negativa inlägg i sociala medier eller enskata negativa inslag i lokal media.	Förtroendet är märkbart påverkat, det finns negativa inlägg i sociala medier och det finns flera negativa inslag i lokal media under 2 veckors tid eller enstaka inslag i rikstäckande media.	Det finns stor påverkan på förtroendet, negativa inlägg i flera sociala medier och negativa inslag i flera rikstäckande medier.
Ekonomi	Ingen påverkan på ekonomin. Gällande budget håller.	Förlust <500 000 SEK. Vissa prioriteringar får göras i budget.	Förlust 500 000–2 000 000 SEK. Större prioriteringar får göras i budget.	Förlust >2 000 000 SEK. Gällande budget räcker inte.
Leveranssäkerhet	Obetydligt antal kunder drabbade <100.	Fåtal kunder drabbade 100–3 000.	Många antal kunder drabbade 3 000–10 000.	Mycket stort antal kunder drabbade >10 000. Produktionen står still.

Tänk på att en kriteriemodell ofta används även inom arbetet med kontinuitetshantering.
Om en kriteriemodell redan finns, eller om den utvecklas inom ramen för antingen riskhanteringsarbetet eller kontinuitetshanteringsarbetet, säkerställ att ni använder samma kriteriemodell oavsett vilket perspektiv du har.

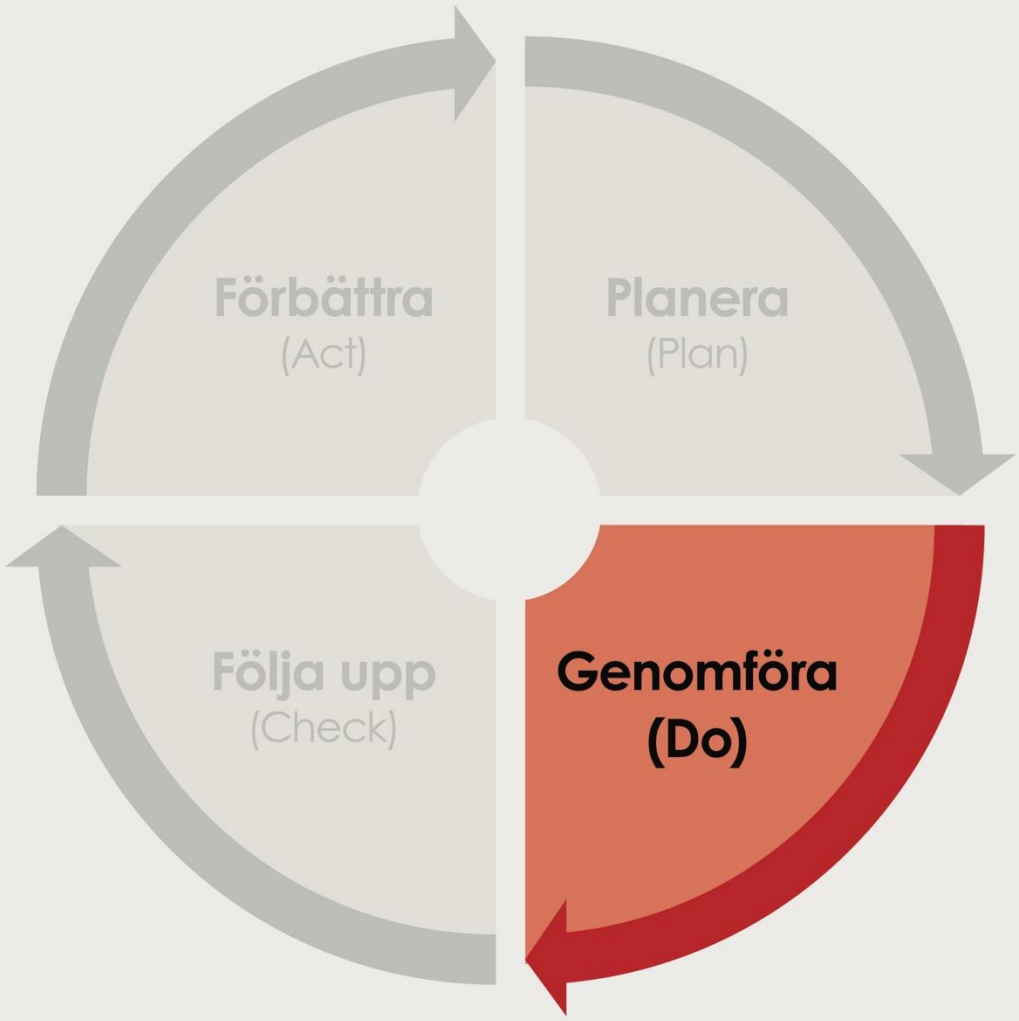
Visualisera risker genom en riskmatris

För att underlätta att hantera, kommunicera och rapportera risker kan en riskmatris användas. En riskmatris är ett verktyg som genom tydliga färgsättningar kan ge en överblick av identifierade risker. En organisations riskmatris bör utgå från de redan definierade nivåerna av sannolikhet och konsekvens.

Figur 2 Se förslag nedan



Om en riskmatris används ska denna vara väl förankrad i organisationen och dess styrande dokument. Riskmatrisen definieras i *Planera*-fasen av PDCA-cykeln, sedan används den i *Genomföra*-fasen vid riskbedömningen.

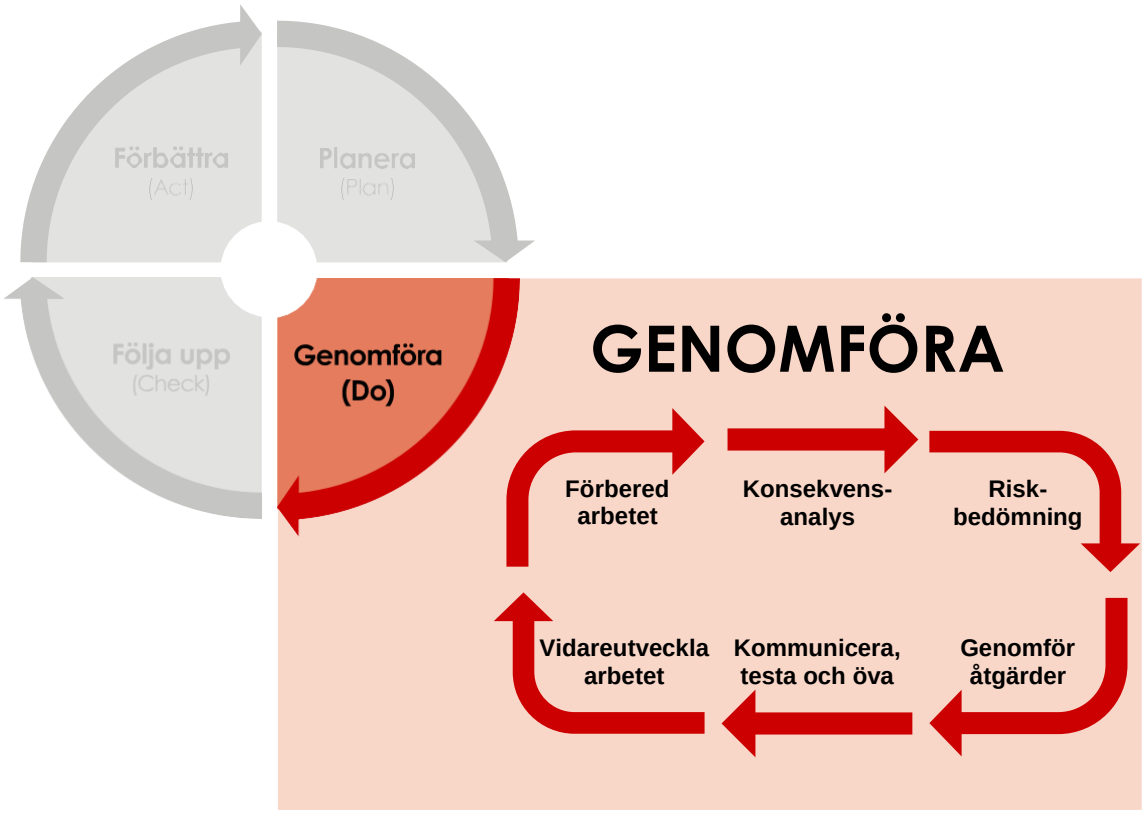


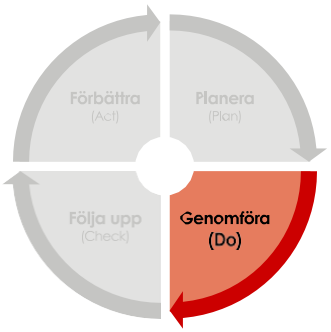
Genomföra

Hur kan samhällsviktiga verksamheter riskhanteras?

Genom att utgå från en systematisk och cyklisk process för arbetet med riskhantering ges förutsättning för kontinuerlig förbättring och utveckling inom organisationens riskarbete.

För att säkerställa att det praktiska arbetet hos verksamheterna sker systematiskt underlättar det att även se fasen Genomföra som en cyklisk process. Här planeras och förbereds det praktiska analysarbetet utifrån organisationens process med hänsyn till verksamhetens förutsättningar. Resultatet av den interna uppföljningen i det praktiska arbetet utgör sedan underlag till organisationens uppföljning av den övergripande processen för riskhantering.

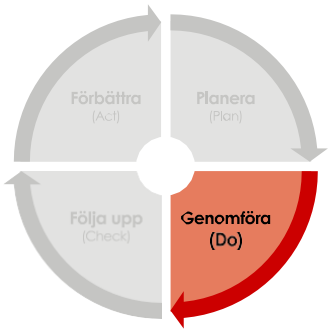




Förbered arbetet

Genomförandet av arbetet bör planeras tillsammans med representanter från den eller de utvalda verksamheterna. En tidplan bör tas fram där vilka som bör bjudas in att delta i arbetet identifieras. Det är även bra att inventera om det redan finns underlag som kan vara till nytta, till exempel processkartläggningar, risk- och sårbarhetsanalyser eller säkerhetsskyddsanalyser.

Ett väl förberett arbete underlättar arbetsprocessen.



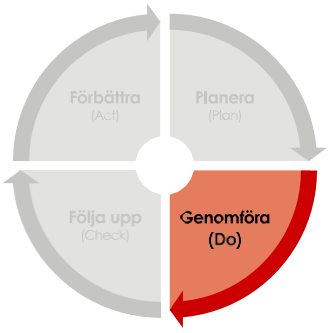
Förbered arbetet

Hur genomförs förberedelserna?

I vissa fall finns interna styrande dokument, exempelvis riktlinjer, som anger vilken arbetsmetod organisationen ska använda för arbetet. Om inte detta finns behöver ni välja metod nu. Riskhantering bör alltid genomföras i nära samarbete med personal från den aktuella verksamheten, såväl beslutsfattare som operativ personal.

Tänk på att göra en informationsklassning av materialet och att resultat från arbetet kan generera konfidentiell information som inte ska spridas till obehöriga.

Genomför arbetet i workshopformat. Det är ofta ett effektivt sätt för att samla rätt kompetens till arbetet.



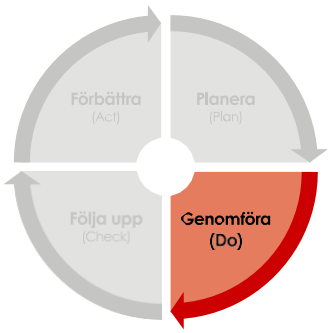
Riskbedömning

Inom ramen för arbetet med riskhantering utgör riskbedömning den övergripande processen för att:

- Identifiera risker
- Analysera risker
- Värdera risker

Riskbedömningen resulterar i en kartläggning över vilka potentiella risker verksamheten eller organisationen kan utsättas för. Den utgör ett underlag för nästa steg om riskhanteringsåtgärder.

Arbetet med riskbedömning bör ske systematiskt och utifrån aktuell information med utgångspunkt i organisationens och verksamhetens förutsättningar, uppgifter och skyldigheter.



Riskbedömning

Hur identifieras risker?

Syftet med riskidentifiering är att upptäcka, beskriva och förstå risker som kan förhindra att verksamhetens mål uppfylls. Riskidentifieringen resulterar i en bruttolista med risker, ett så kallat riskregister. Riskregistret kan omfatta mer övergripande risker, ex. översvämning, eller mer specifika risker, ex. elfel i brandcentral. Riskregistret kommer över tid att utökas och blir därmed en hjälp för kommande riskanalyser

En risk beskrivs ofta som effekt av en osäkerhet där effekten är en avvikelse från det förväntade. Ett annat vanligt förekommande sätt att prata om risk är som en sammanvägning av sannolikheten för att en oönskad händelse ska inträffa och de konsekvenser händelsen kan leda till.

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 1 och 11–12

Avsnitt 6.4.2 Riskidentifiering

Stöddokument & fördjupning
MSB: dokumentationsmall
MSB: checklista
MSB: Riskkatalog
www.msb.se/riskshantering.

Riskidentifiering kan med fördel ske genom informationsinhämtning från en bred representation från verksamheten. Detta kan exempelvis ske genom workshops, enkäter, intervjuer etc. För att identifiera risker kan verksamheten:

- Utgå från tidigare händelser och samla in tidigare erfarenheter från organisationen
- Ta hjälp av data och dokumentation från inträffade händelser och incidenter
- Ta hjälp av rapporter och andra underlag, exempelvis MSB:s riskkatalog

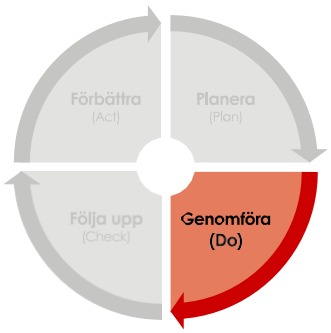
Exempel på hur en riskidentifiering kan dokumenteras:

Riskidentifieringen ska dokumenteras för att underlätta det efterföljande analysarbetet. Det är viktigt att beskriva risken utförligt hur riskerna kan påverka organisationens möjligheter att nå sina uppsatta mål, samt hur den fortsatta hanteringen av riskerna kan ske på bästa sätt. Även att tydliggöra vem som äger den, det vill säga vem i organisationen som har ansvar för att risken hanteras (riskägare). En tydlig dokumentation inledningsvis underlättar det fortsatta analysarbetet.

Tabellen nedan är ett förslag på hur risker kan dokumenteras i ett så kallat *riskregister*.

Tabell 5 Text

Namn på risk	Beskrivning av risk	Riskägare
Namn på risk	*Kort beskrivning av risken*	*Vem äger risken och har mandat att genomföra eventuella åtgärder?*
Översvämning	Översvämningar kan ske på grund av kraftigt regn, stigande vattennivåer i floder.	Avdelningschef
Förlust av nyckelpersonal	Personal med nyckelkompetens försvinner till följd av ex avslutad tjänst eller sjukskrivning.	Personalchef



Riskbedömning

Hur analyseras och värderas risker?

Att analysera och värdera risker handlar om att förstå riskers karaktärer, egenskaper och nivåer, och utifrån det göra en bedömning avseende riskers sannolikhet och konsekvens. Genom denna sammanvägning kan risken utvärderas med avseende på om risken kan accepteras och lämpliga åtgärder kan identifieras.

Att analysera och värdera risker kan genomföras med varierande detaljnivå och komplexitet beroende på tillgängliga resurser och syfte, men även utifrån vilken tillförlitlig information som finns att tillgå.

Analysmetoder kan vara kvalitativa, kvantitativa eller en kombination av båda.

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 12–13
Avsnitt 6.4.3 *Riskanalys*
Avsnitt 6.4.4 *Riskvärdering*

Stöddokument & fördjupning
MSB: dokumentationsmall
MSB: checklista
www.msb.se/riskshantering.

Kvalitativa metoder

Kvalitativa metoder fokuserar på beskrivande bedömningar av risker. De används när det saknas tillräckliga data för att göra exakta beräkningar eller när man vill ha en bredare bild av risker. Målet är att få insikter om erfarenheter, motiv eller beteenden kopplat till den identifierade risken.

Kvantitativa metoder

Kvantitativa metoder bygger på numeriska data och statistiska beräkningar för att kvantifiera sannolikheten och konsekvenserna av risker. De används när det finns tillräckligt med data för att göra exakta beräkningar, till exempel utifrån enkätsvar eller statistik över en inträffad risk. Med hjälp av denna kan det gå att identifiera trender, samband eller mönster.

När din organisation utformar ert arbete med riskhantering är det viktigt att bestämma på vilket sätt ni vill värdera era risker. Alla metoder har sina för-respektive nackdelar. Många organisationer väljer att använda en kombination av kvalitativ och kvantitativ metod i arbetet med värdering av risk. På så vis möjliggörs att få en så god helhetsbild som möjligt i arbetet med riskhantering

Följande frågor kan vara ledande i arbetet med att analysera och värdera risker:

- Vilka är orsakerna till risken? Finns det flera olika scenarion som är troliga?
- Hur stor är sannolikheten att risken inträffar? Har risken inträffat tidigare? Finns det några särskilda tidsramar, tidsrelaterade faktorer som påverkar sannolikheten?
- Vilka kan konsekvenserna bli om risken inträffar?
- Vad är karaktären och omfattningen på konsekvenserna?
- Finns det någon inbördes relation mellan riskerna?
- Finns det någon pågående åtgärd på plats, och har denna fått effekt?

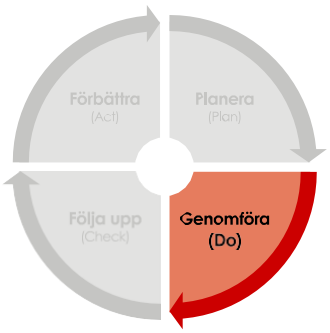
Exempel på hur en analys och värdering kan dokumenteras:

Riskanalysen ska dokumenteras på lämpligt vis. Tabellen nedan är ett förslag på hur risker kan dokumenteras i *riskregister*. Detta exempel inkluderar enbart helt kvalitativa perspektiv.

Tabell 6 Text

Risk	Orsak	Beskrivning av sannolikhet	Beskrivning av konsekvens	Kan risken accepteras?
Namn på risk	*Vilka bakomliggande faktorer finns som kan påverka konsekvens och sannolikhet av?*	*Beskriv sannolikheten att risk inträffar*	*Beskriv konsekvensen av att risk inträffar*	*Beskriv huruvida risken kan accepteras eller ej*
Översvämning	Översvämningar kan ske på grund av kraftigt regn, stigande vattennivåer i floder	**Troligt** Åter-kommande händelse till följd av snösmältning och höstregn.	**Allvarlig** Förlust av egendom, skador på infrastruktur (vägar, broar, elnät)	Nej
Förlust av nyckelpersonal	Hög arbetsbelastning, missnöje med kompensation, etc.	**Troligt** Troligt att detta inträffar, finns tidigare exempel på att nyckelpersoner väljer att avsluta sin anställning.	**Katastrofal** Organisationen kan inte utföra sitt uppdrag utan nyckelpersoner	Nej

En väldokumenterad och genomarbetad identifiering och bedömning av risker kan användas som beslutsunderlag i ledningsgrupper för exempelvis utveckling av strategier, genomförande av investeringar eller förändringar i arbetsprocesser.



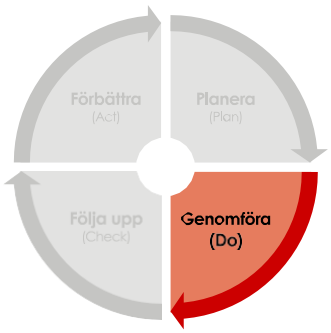
Åtgärder

Momentet omfattar att:

- Välja lämpliga åtgärder
- Formulera en åtgärdsplan
- Kommunicera och genomföra åtgärder

Momentet utgör en iterativ process för att identifiera, planera för och vidta åtgärder i syfte att hantera risker som har identifierats i riskbedömningen.

I denna vägledning används begreppet *åtgärder* istället för *riskhanteringsåtgärder* som används i standarden SS-ISO 31000:2018 Riskhantering.



Åtgärder

Hur formuleras, väljs och hanteras åtgärder?

I standarden för riskhantering (ISO 31000:2018) presenteras riskhanteringsåtgärder och riskhanteringsplan, vilket denna vägledning benämner som åtgärder respektive åtgärdsplan. Innebörden av dessa begrepp är desamma. Syftet med riskhanteringsåtgärder (åtgärder) är att välja och implementera alternativ för att ta hand om risker och möjligheter. Syftet med en riskhanteringsplan (åtgärdsplan) är att ange hur de valda åtgärderna kommer att implementeras och följas upp.

Baserat på riskbedömningen identifieras åtgärder för att hantera de identifierade riskerna. De åtgärder som formuleras syftar i huvudsak till att hantera risker som bedöms som oacceptabla. Även risker som bedöms som acceptabla kan vara föremål för åtgärder, exempelvis med bevakning och efterkontroller eller om åtgärderna bedöms vara relativt enkla att genomföra eller bidra till att flera andra risker minimeras. Det kan handla om att bibehålla och/eller förändra risker, exempelvis via processer, policyer, utrustning, rutiner och beslutspunkt, dvs. i vilket läge en åtgärd måste vidtas.

Följande frågor kan vara ledande vid val av åtgärder:

- Kan risken undvikas? Detta kan exempelvis göras genom att inte inleda/ fortsätta med den aktivitet som ger upphov till risken.
- Kan orsaken till risken elimineras? Exempelvis kan risken för mänskliga fel elimineras med hjälp av automatisering.
- Kan sannolikheten för att risken inträffar minimeras? Exempelvis genom nya säkerhetsrutiner.
- Kan konsekvensen av risken minimeras? Exempelvis genom tecknande av försäkring.

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 13–15
Avsnitt 6.5 *Riskhanteringsåtgärder*
Avsnitt 6.6 *Övervakning och översyn*
Avsnitt 6.7 *Dokumentation och rapportering*

Stöddokument & fördjupning
MSB: dokumentationsmall
MSB: checklista
www.msb.se/riskshantering.

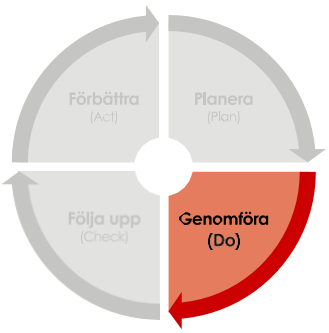
- Vilka fördelar finns med den valda åtgärden? Fördelarna ska vägas mot eventuella nackdelar med åtgärden samt kostnader och insatser för införandet.
- Kan åtgärderna medföra målkonflikter för organisationen eller verksamheten?
- Kan flera åtgärder ge synergieffekter och tillsammans hantera flera risker parallellt samt effektivisera genomförande och spara resurser?

Tabellen nedan är ett förslag på hur risker kan dokumenteras i ett *riskregister*, där även val av åtgärder kan specificeras:

Risk	Riskhanteringsåtgärd	Ansvarig	Tidsplan
Namn på risk	*Vilken åtgärd ska användas för att hantera konsekvenserna av eller minska sannolikheten för risken? Motivera kort.*	*Vilken befattning som är ansvarig för att genomföra åtgärden?*	*Vilket datum ska åtgärden vara genomförd?*
Översvämning	Permanent invallning/översvämningsskydd av kopplingspunkt A17, stadsnät.	Avdelningschef	XXXX-XX-XX
Förlust av nyckelpersonal	Lär upp flera anställda inom aktuell arbetsprocess.	Personalchef	XXXX-XX-XX

I samband med att åtgärder identifieras är det viktigt att tydliggöra kronologisk ordning och stödjande åtgärder, som behov av utredning eller förstudie föregående inför genomförande av en sannolikhets- eller konsekvensreducerande åtgärd.

Det är även viktigt att försöka bedöma effekten (kostnad och nytta) av åtgärdsförslaget för att kunna bedöma dess lämplighet och identifiera eventuellt kvarstående risk. Om den kvarstående risken inte bedöms som godtagbar behöver ytterligare åtgärder identifieras.



Åtgärder

Hur sammanställs åtgärder?

En åtgärdsplan är ett strategiskt verktyg som kan användas för att hantera åtgärderna strukturerat. Syftet med åtgärdsplaner är att underlätta för prioritering av åtgärderna, specificera ange hur de valda åtgärderna kommer att införas och i vilken ordning. På så sätt får alla berörda parter kännedom om åtgärdsprocessen, vilket även möjliggör uppföljning av åtgärderna och dess effekt.

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 13–15
Avsnitt 6.5 *Riskhanteringsåtgärder*
Avsnitt 6.6 *Övervakning och översyn*
Avsnitt 6.7 *Dokumentation och rapportering*

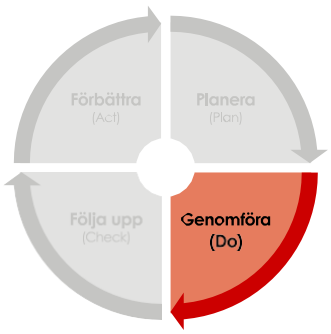
En åtgärdsplan ska innehålla följande information:

- motivering till valet av åtgärder, samt de fördelar och effekt som förväntas erhållas
- vilka som ansvarar för att godkänna och införa planen
- föreslagna aktiviteter
- ansvarig för genomförande
- begränsningar
- erforderlig rapportering och övervakning (uppföljning)
- när åtgärder förväntas genomföras och vara slutförda (i detta sätt samtidigt en prioriteringsnivå för åtgärderna)

Stöddokument & fördjupning
MSB: dokumentationsmall
MSB: checklista
www.msb.se/riskshantering.

Åtgärdsplanen behöver förankras genom ett beslut från någon med beslutsmandat i organisationen, rimligtvis en ledningsgrupp. Efter att åtgärdsplanen är beslutad ska den kommuniceras och delas med varje verksamhet som berörs och sedan följas upp i enlighet med utsatta hålltider i planen.

Uppföljningen av åtgärdsarbetet kan för enkelhetens skull integreras i organisationens planer och arbetsprocesser.



Åtgärder

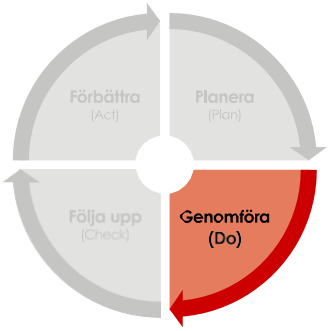
Hur kommuniceras och genomförs åtgärder?

När åtgärdsplanen är beslutad ska åtgärderna genomföras enligt överenskommen tidplan. Ofta ligger ansvaret på verksamheten, men en processledare kan behöva stötta i arbetet. Åtgärderna kan med fördel inkluderas i den ordinarie verksamhetsplaneringen. I detta skede är det viktigt att ha en dialog med ledningen om roller och ansvar, exempelvis vem som ska kommunicera beslut om åtgärder till berörda verksamheter och intressenter.

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 13–15
Avsnitt 6.5 *Riskhanteringsåtgärder*
Avsnitt 6.6 *Övervakning och översyn*
Avsnitt 6.7 *Dokumentation och rapportering*

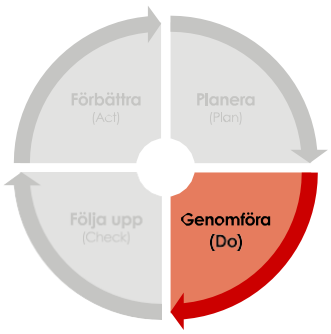
Exempel på information att kommunicera är

- vilka åtgärder som ska genomföras
- vilka åtgärder som har prioriterats ned
- om de genomförda åtgärderna påverkar innehållet i redan befintliga planer och rutiner.



Kommunicera och rapportera risker

En viktig del i arbetet med riskhantering är att systematiskt kommunicera och rapportera risker inom organisationen, både till ledningen, verksamheter och andra intressenter.



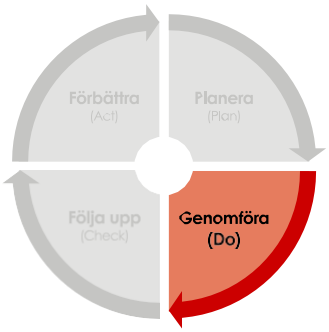
Kommunicera och rapportera risker

Hur kommuniceras och rapporteras risker?

Resultatet av riskhanteringsprocessen ska kommuniceras och rapporteras till relevanta parter, både internt och externt.

Kommunikationen ska även belysa varför riskhantering bedrivs inom organisationen. Bra kommunikation bidrar även till att beslutsfattare får underlag för beslut samt en ökad förståelse för riskhantering.

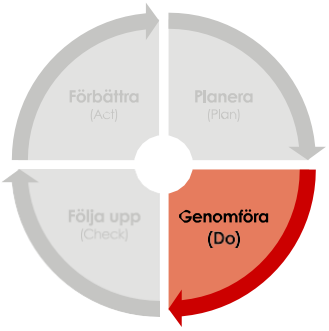
Hur risker rapporteras ska vara beskrivet i organisationens styrande dokument, till exempel riktlinje eller rutin.



Vidareutveckla arbetet

Arbetet med riskhantering kräver ständig utveckling och förbättring. Både inre och yttre faktorer gör att verksamhetens förutsättningar är föränderliga, vilket är något som kan påverka resultatet av riskbedömningen och val av åtgärder. Det kan i sin tur resultera i nya åtgärdsbehov för att hantera organisationens risker. På så sätt säkerställs att riskhanteringen är aktuell.

Att följa upp och vidareutveckla det praktiska arbetet med riskhantering i verksamheten är också viktiga ingångsvärden för uppföljning och förbättring av organisationens övergripande riskhanteringsprocess (PDCA-cykel).



Vidareutveckla arbetet

Hur kan verksamhetens arbete med riskhantering utvecklas?

Riskhanteringen bör vara en del av vardagen och det ständiga förbättringsarbetet inom verksamheten.

Förbättring kan exempelvis uppnås genom att ta fram en tidplan och arbetssätt för att regelbundet och utifrån behov

- uppdatera riskbedömningen
- följa upp åtgärdslistan

Stöddokument & fördjupning

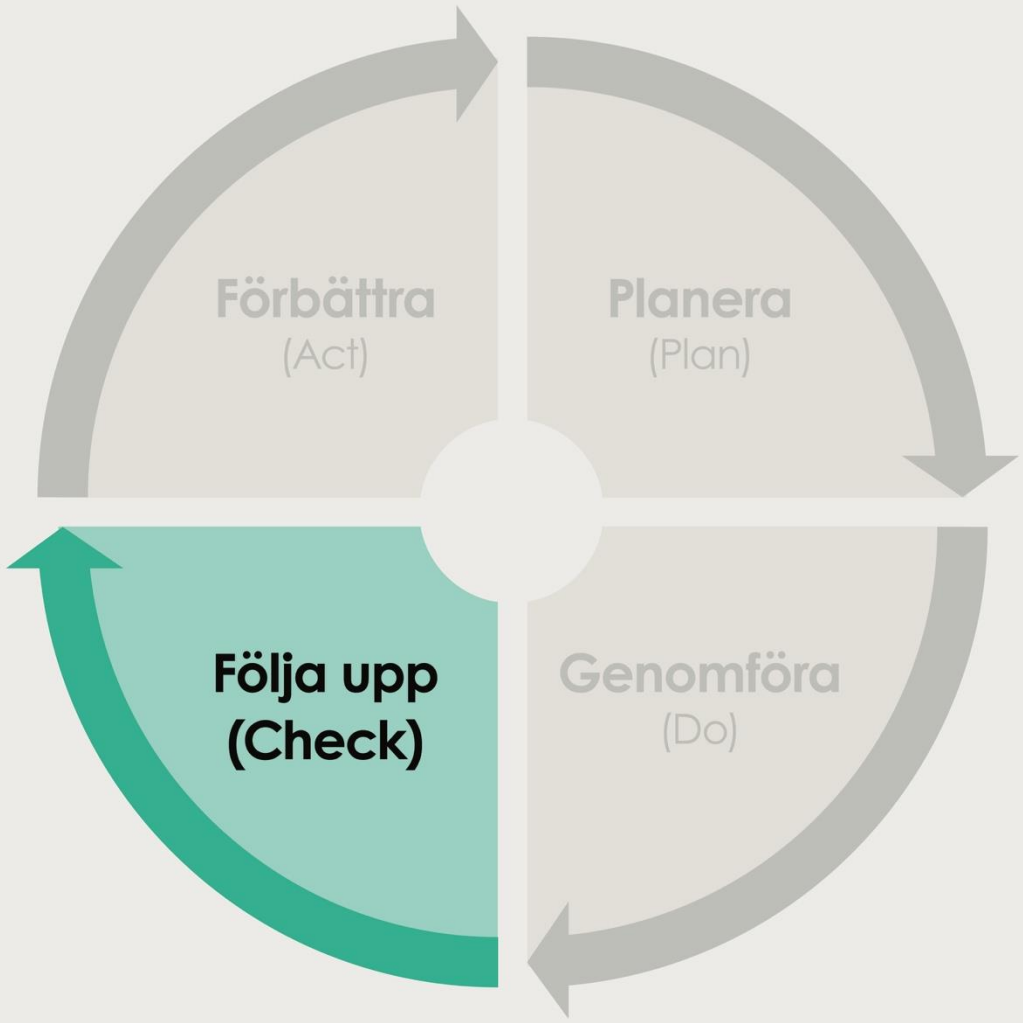
- **MSB:** Checklista
- **MSB**: Uppföljning för förbättrad kontinuitetshantering (MSB2150 – december 2022).

www.msb.se/riskshantering.

Förbättring och vidareutveckling kan även ske genom att följa upp och utvärdera arbetet till exempel enligt en framtagen rutin för uppföljning. Här ges möjlighet att identifiera vad som har gått bra respektive mindre bra samt ta fram åtgärdsförslag för att utveckla verksamheternas arbete med riskhantering.

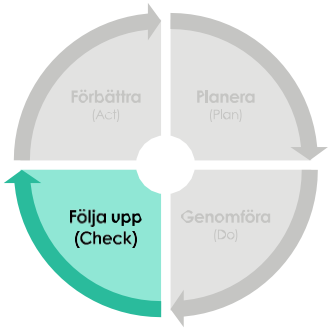
Det är viktigt att berörda medarbetare får en sammanfattning av den genomförda uppföljningen för att känna ansvar och delaktighet. Uppföljningen blir också ett underlag till ledningen för övergripande beslut om resurser och prioriteringar.

Uppföljningen för verksamheten bör dokumenteras. Ta med både det som har gått bra och det som har gått mindre bra.



Följa upp

-



Följa upp

Varför ska arbetet med riskhantering följas upp?

Att kontinuerligt följa upp arbetet med riskhantering är centralt för att säkerställa att arbetet leder till önskade resultat, att metoderna som används är flexibla och anpassningsbara efter ständigt föränderliga förutsättningar, samt att arbetet ligger i linje med organisationens mål och de interna och externa krav som finns.

Uppföljningen leder till kunskap om huruvida styrande dokument, arbetssätt, mallar et cetera är relevanta, uppdaterade och anpassade efter förändringar i organisationen eller i omvärlden. Resultatet från uppföljningen kan identifiera möjliga förbättringar och omprioriteringar gällande exempelvis arbetssätt och resurser.

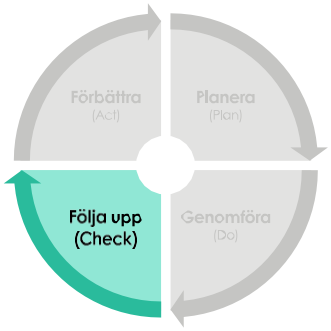
Kontinuerlig och strukturerad uppföljning, dokumentation och rapportering avseende arbetet med riskhantering leder till en stärkt förmåga att hantera risker effektivt och därmed ökade möjligheter att uppnå organisationens mål.

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 8
Avsnitt 5.6 Utvärdering

Stöddokument & fördjupning

- **MSB:** Checklista
- **MSB:** Uppföljning för förbättrad kontinuitetshantering (MSB2150 – December 2022).
- **MSB:** Informationssäkerhet – Metodstödet – Följa upp och förbättra – Utvärdera och följa upp, https://metodstod-informationssakerhet.msb.se/sv/folja-upp/ utvardera-och-folja-upp.

www.msb.se/riskshantering.



Följa upp

Hur kan organisations arbete med riskhantering följas upp?

För att följa upp arbetet är det viktigt att gå tillbaka till de mål som beslutades i policyn eller motsvarande styrande dokument. Uppföljningen görs utifrån framtagen rutin om en sådan finns. Annars kan det göras utifrån organisationens eget arbetssätt för uppföljning, till exempel genom egenkontroller eller andra former av internkontroll. Uppföljningen kan göras av både interna och externa parter.

Uppföljningen kan genomföras genom följande aktiviteter:

- Genomgång av styrande dokument, det vill säga policy och riktlinjer för arbetet. Det innebär att följa upp mål, arbetssätt och -metoder samt mallar och verktyg som används för arbetet.
- Genomgång av underlag och analyser som genererats av arbetet, till exempel riskregister och åtgärdsplaner.

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 (årshjul eller motsvarande).

En viktig del av uppföljningen är att kommunicera resultatet till relevanta intressenter, såsom ledning, tillsynsmyndigheter, berörda verksamheter och medarbetare.

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 8
Avsnitt 5.6 Utvärdering

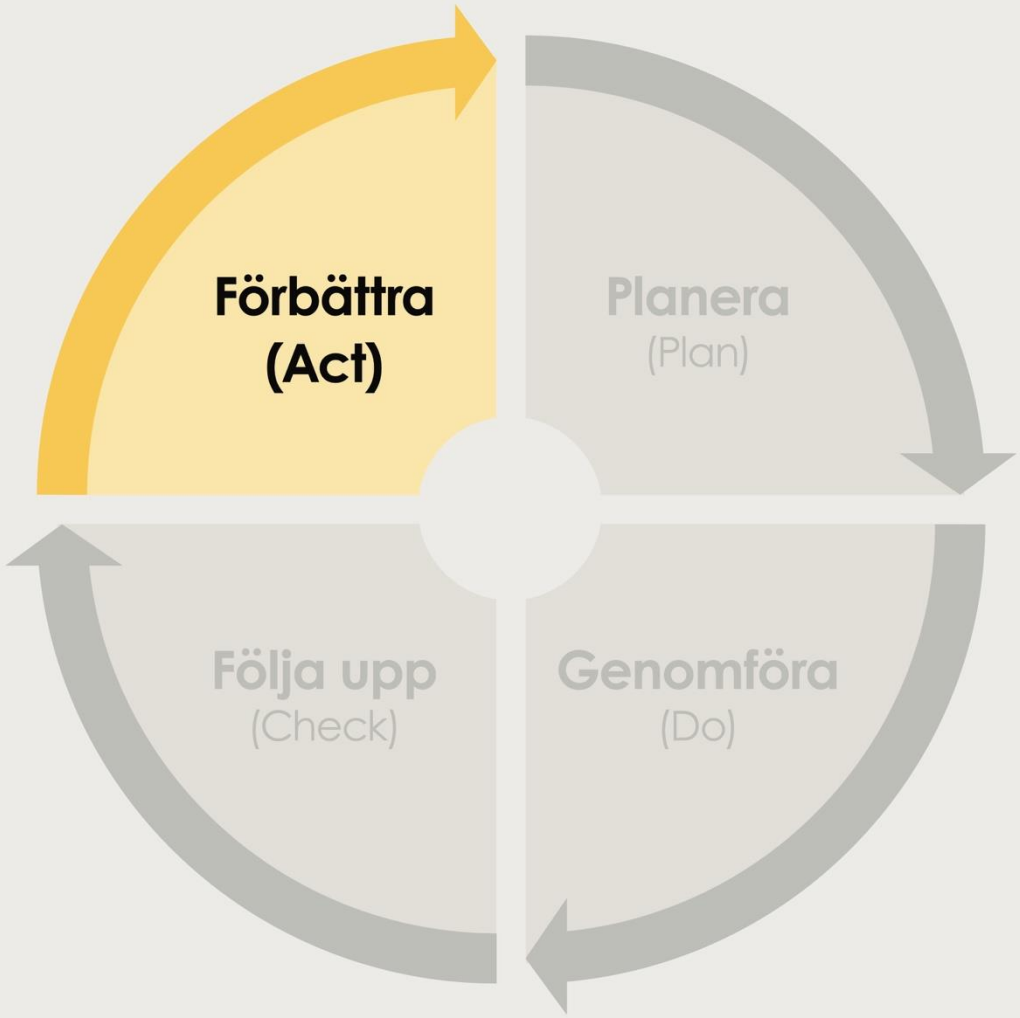
Stöddokument & fördjupning

- **MSB:** Checklista
- **MSB:** Uppföljning för förbättrad kontinuitetshantering (MSB2150 – December 2022).
- **MSB:** Informationssäkerhet – Metodstödet – Följa upp och förbättra – Utvärdera och följa upp, https://metodstod-informationssakerhet.msb.se/sv/folja-upp/ utvardera-och-folja-upp.

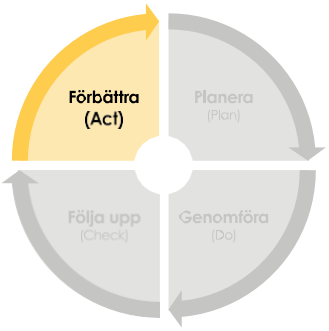
www.msb.se/riskshantering.

Ledningen ska regelbundet få information om resultatet av riskhanteringsarbetet. Detta kan exempelvis genomföras genom ledningens genomgång där ansvarig för riskhantering presenterar en övergripande bild av arbetet. Genomgången ska ge ledningen en nulägesbild av arbetet och resultera i en inriktning för det fortsatta arbetet med riskhantering.

Kommunikation kan ske via exempelvis möten, nyhetsbrev eller interna/externa rapporter. Internt bidrar kontinuerlig och transparent kommunikation till organisationens kultur gällande delaktighet och ansvar i arbetet med riskhantering.



Förbättra



Förbättra

Hur kan organisationens arbete med riskhantering förbättras?

Att kontinuerligt förbättra arbetet med riskhantering kräver ett strukturerat tillvägagångssätt som integrerar utvärdering, revisioner och kontroller som en del av den dagliga verksamheten och det ständiga förbättringsarbetet inom organisationen.

Förbättringsarbetet sker genom att omhänderta resultatet av uppföljningen, se sida 34–35.

I arbetet med att förbättra arbetet med riskhantering kan organisationen ställa sig följande frågor:

- Används rätt arbetssätt och metod för riskhantering inom organisationen?
- Finns tillräckliga resurser för att bedriva riskhantering enligt uppsatta mål?
- Behöver organisationen ytterligare kompetens inom riskhantering?
- Finns det specifika områden (verksamheter eller moment) som organisationen bör fokusera på i kommande arbete med riskhantering?

Riskhantering, Vägledning SS-ISO 31000 2018
Läs sidorna: 8
Avsnitt 5.6 Utvärdering
Avsnutt 5.7 Förbättring

Stöddokument & fördjupning

- **MSB:** Checklista
- **MSB:** Uppföljning för förbättrad kontinuitetshantering (MSB2150 – december 2022).

www.msb.se/riskshantering.

Svaret på dessa frågor ger ingångsvärden till fortsatt arbete med riskhanterings-processen enligt PDCA-cykeln. Utifrån resultatet av Följa upp blir nästa steg att se över organisationens styrande dokument, avgränsning, resurstilldelning, processen/arbetssätt för riskhantering eller samordning med andra processer i fasen Planera. Att säkerställa kontinuiteten i den cykliska processen är avgörande för att upprätthålla och utveckla arbetet med riskhantering o organisationen.

Myndigheten för samhällsskydd och beredskap

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