Ett samarbete mellan Sambruk och eSam

Inför workshop om Plan B- Amerikanska nyheter och offentlig sektors riskarbete kring digital beredskap

Syftet med det här materialet är att vara förberedande och väcka tankar inför workshoppen om hur offentlig verksamhet kan planera för geopolitiska störningar och minska sitt beroende av utländskägd it.

Friskrivning

Detta dokument kan användas som ett stödmaterial för myndigheters egna riskanalysarbete. Varje myndighet måste göra sin egen bedömning kring sina risker och sin omvärldsbevakning. Länkar till nyheter som exempel längre ner i detta dokument måste tolkas och utvärderas av varje organisation. Dokumentet är inte en officiell färdig rapport för beslut.

Bakgrund – ett samhälle i beroendeställning

Sverige har ett mycket ett stort beroende av USA. Genom affärer, internet, kultur och vardagsliv är amerikansk engelska det vanligaste ”främmande” språket i Sverige sedan 1939.[1] Ekonomisk säkerhet och handel bygger på amerikanska system och med USD som grundgarant även globalt. Energi, försvar[2], försörjning, kemikalieindustri, livsmedel, samverkan, transport och vård har alla mycket stora beroenden av USA. Svensk offentlig sektor har till stor del sina digitala system, it-tjänster och it-infrastruktur som har en grund i amerikanskt ägande.

Alt text: Antagligen är en stor andel av it-systemen och it-tjänsterna som används i offentlig sektor, amerikanskägda eller är byggda på amerikansk it-infrastruktur, givet den leverantör som dominerar marknaden.

Genom samhällets löpande investeringar fortsätter den globala innovationskraften att centreras till USA och därmed bibehålls USA:s ledande marknadsställning utan möjlig förändring över tid. Globala utmanare – däribland svenska innovatörer - köps snabbt upp av amerikanska bolag.[3]

Offentlig sektors grunduppdrag

Offentlig sektor har och får genom EU direktiven NIS2/CER/CRA ett förtydligat samhällskrav att rimligen bibehålla en god motståndsförmåga och beredskap. De största hoten mot ett fungerande och allt mer digitalt svenskt samhälle är t.ex. aktivism, handhavandefel, hybridkrig, politiska aktiviteter (egna eller andras), terrorism och osunda vinstintressen.

Digital beredskap

När kritiska samhällstjänster är beroende av amerikanska produkter och tjänster, blir det utmanande att garantera Sveriges egen rådighet enligt uppdrag. Den höga graden av digitalisering i svenska

---

[1] Mer information i sakfråga; https://sv.wikipedia.org/wiki/Engelska_spr%C3%A5ket_i_Sverige

[2] Artikel som även beskriver svenskt investerande i amerikanska försvarslösningar; https://www.politico.eu/article/punching-allies-in-the-face-how-trump-is-making-europe-question-us-arms-deals/

[3] Kommentar som beskriver amerikanska uppköp av svenska teknik- innovatörer; https://www.svd.se/a/kEjzqB/bjorn-jeffery-amerikanska-jattar-slukar-svenska-techsucceer

samhället, knyter beroendet hårdare till USA på flera olika plan. Detta gäller inom offentlig sektor som en direkt risk och för alla som interagerar med offentlig sektor - medborgare och privata leverantörer - som en indirekt risk.

Geopolitiken och nya risker

It-området används allt oftare som påtryckningsmedel mellan länder. Den stora kända starten på geopolitik genom it, var Kinas Golden Shield Project (1998)[4] där internet för hela landet skulle styras av den kinesiska staten. Därmed kunde man också styra alla utländska tjänster som levererades via internet, till Kina.

USA har under lång tid nyttjat sin it-dominans för att styra den global politiken.[5] Genom amerikansk it bedrivs massövervakning[6] och allt oftare påverkanskampanjer[7] mot omvärlden.

När demokratin drastiskt devalveras i USA, medför detta nya risker för svensk offentlig sektor där den drivna geopolitiken medför risker i offentlig sektors val av it-lösning. Risken för att Sverige skulle tvingas agera mot vår egen vilja, genom de it-system vi valt, blir allt större.[8]

Detta dokument tar upp hur offentlig sektor kan resonera kring dessa risker.

Svårighet att bedöma nya risker

Det är svårt för organisationer att hänga med i händelseutvecklingen i USA och det som påverkar det svenska samhället på olika sätt. Det är svårt för offentliganställda analytiker och beslutsfattare att navigera bland alla händelser som behöver inkluderas i riskarbetet.

I huvudsak är en hållbar demokrati i USA en nyckelfråga att bevaka. Utan fungerande demokrati som styrsystem får myndigheter svårigheter att teckna affärer med standard samhällsförutsättningar. Hälsosam demokrati bedöms enligt en skala, Sverige låg på tredje plats globalt under mätningar år 2024[9] och USA på 28:e plats. Med de samhällsändringar som sker i USA sedan nya regeringen tillträdde gör att i nästa års bedömning tros USA rankning falla.[10]

Allmän risk att Sverige är för beroende av amerikanska molntjänster. Länk

Nedan finns fem huvudrisker beskrivna utifrån: Varför är de av betydelse, vad ska vi leta efter vid omvärldsbevakning samt en del kända exempel i skrivande stund.

---

[4] Förklaring och historik; https://www.britannica.com/topic/Great-Firewall

[5] Förklaring på ett exempel på tidig geopolitiskt agerande, Echelon, ett amerikansk initierat signalövervakningsprogram framförallt riktat mot EU men också globalt; https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2014)538877

[6] Artikel om amerikansk massövervakning; https://www.politico.com/news/magazine/2024/02/28/government-buying-your-data-00143742

[7] Artikel på exempel där USA systematiskt använder IT tjänster för informationskampanjer; https://amp.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks och https://gizmodo.com/facebook-twitter-us-disinformation-russia-china-iran-1849452348

[8] Artikel som tar upp hotbilden i närområdet; https://www.aftonbladet.se/nyheter/a/W018aG/dataexpert-usa-kan-stanga-ner-danmark-om-gronland-inte-saljs

[9] Exempel på demokrati index mätning; https://ourworldindata.org/grapher/democracy-index-eiu

[10] Utalande om USA:s framtida demokrati ranking: https://www.v-dem.net/news/press-release-restrictions-to-freedom-of-expression-as-democracy-loses-ground/

1. Politisk styrning av it-leverantörer

Kina, Iran, Ryssland och USA har samtliga påvisat en stor vilja att åstadkomma direkt påverkan genom att nyttja it-system i omvärlden. Sverige befinner sig sedan flera år i ett hybridkrig[11] på grund av detta hot. Vanligtvis visar sig dessa aktiviteter som försök att störa samhällsfunktioner, digitala och fysiska (t.ex. sabotage mot knytpunkter inom tågtrafik eller basnätverket för el) eller som påverkansförsök som t.ex. sabotage mot tågtrafik eller elförsörjning. Irans beställningar av skjutningar och sprängningar i Sverige kan också vara exempel på detta.[12] Det kan också vara fråga om en presidentorder till en leverantör om att stoppa it-leveranser till ett visst land.

Exempel på aspekt att titta efter i omvärldsbevakning:

- Artiklar där leverantörer eller kund hävdar politiska beslut vid tvingande åtgärder.

Möjliga exempel kring denna risk:

- Juni 2013, NSA har en lagenlig, tvingande och hemligstämplad teknisk bakdörr (programnamn: Prism) in till Microsoft och dess Skype-division, Google och dess YouTube division, Yahoo; Facebook, AOL, Apple och PalTalk samt en chattjänst från AVM Software. Länk
- Oktober 2019, En executive order (EO) tvingade Adobe neka Venezuela access till molntjänst. Länk
- Juni 2022, Kammarrätten avslår Huawei Technologies Sweden AB: s överklagan för två mål som rör villkor för 5G-tillstånd och slår fast Post- och telestyrelsens beslut mot nyttjandet av denna leverantör i Sveriges bärande 5G infrastruktur. Länk
- Mars 2024, Microsoft väljer att blockera några av sina molntjänster i Ryssland p.g.a. kriget. Länk
- Juni 2024, Presidenten beslutar om verksamhetsförbud i USA för Ryska Kaspersky Lab p.g.a. stark misstanke om att antivirusprodukter från tillverkaren hjälper rysk underrättelsetjänst. Länk
- Januari 2025, En executive order tvingade Microsoft neka International Criminal Court (ICC) access till molntjänst och ICCs lagrade bevismaterial i denna tjänst. Länk
- Mars 2025, En executive order beordrar satellitföretaget Maxar neka Ukraina access till bilder. Länk
- April 2025, DOGE tvingar åt sig samlad access till känslig digital information på flera olika amerikanska myndigheter enligt presidentorder. Visselblåsare vittnar om ryska hacker metoder i DOGE insamlingsarbete och access till den känsliga informationen från ryska IP adresser. Länk1, Länk2 och länk3

2. Risker avseende rättssäkerhet

Lag går alltid före avtal men om demokratin fallerar så styrs lag genom politik (auktoritärt styrsystem). Där it-risken tidigare handlat om t.ex. GDPR, FISA 702 och lagligt, amerikanskt agerande kring it-lösningar och dess leverantörer, kan risken nu istället handla om direkt politisk inblandning och korruption, t.ex. att sälja offentlig sektors känsliga information. Vidare kan riskerna med demokratiskt förfall resultera i brist på tillsynsorgan alternativt att tillsynsorganen får en uttalad uppgift att låta bli

[11] Försvarsmakten förtydligande; https://www.forsvarsmakten.se/sv/aktuellt/2025/01/hybridoperationer-skadar-sverige/

[12] Artikel om hur SÄPO kartlagt Irans påverkans- och sabotagekampanjer i Sverige; https://edition.cnn.com/interactive/2025/world/iran-israel-swedish-teenagers-shadow-war-intl-invs/

att skydda svensk offentlig sektor i amerikanska it-lösningar. Utan lagefterlevnad, med anti-demokratiska lagar eller avsaknad av fungerande tillsynsmyndigheter för dessa lagar, står svensk offentlig sektor helt oskyddad med amerikanskägda it-lösningar. Svenska avtal och samhällsskydd (t.ex. cert.se, FRA, NCSC, Polisen, SÄPO) blir helt betydelselösa för berörda system.

Några aspekter att titta efter i omvärldsbevakning:

1. Demokratiskt förfall – Tecken på att ”checks and balances”[13] fallerar.
2. Regeringens lagbrott – kända fall där regeringen bryter mot egna landets lagkrav eller inte följer domslut.
3. Exempel där korruption uppstår hos leverantörer eller i regeringen
4. Där juridiska systemet fallerar i sin kontroll t.ex. om högsta domstolen dömer för regeringen mot etablerat lagrum
5. Där relevanta tillsynsmyndigheter avvecklas, görs obrukbara eller styrs till ett myndighetsuppdrag där regeringen dikterar vilka lagkrav eller målgrupper (utvalda) som skall bevakas, kontrolleras eller hanteras.

Möjliga exempel kring denna risk:

- Lista flera misstänkta lagöverträdelser kring utlämning av immigranter med giltiga uppehållstillstånd till fängläger i El Salvador eller felaktigt borttagna medborgarskap. Länk
- Regeringen följer ej ålagda domslut från federal domare. Länk
- Regeringen följer inte dombeslut från högsta domstolen. Länk
- Oberoende juridisk översyn minskar och blir ej beslutsför. Länk
- Högsta domstolen låter presidenten använda krigslag från 1798 i fredstid för att deportera personer men nu med viss rätt till juridisk prövning. Länk
- Pressfriheten ifrågasätts av domare i Mississippi. Länk
- National Public Radio (NPR) beskriver att landets fria press är under attack från regeringen. Länk

3. Tecken på auktoritärt styrsätt

Om demokratin avvecklas eller skendemokrati införs, kommer rättssäkerheten falla i nästa steg. Systematisk korruption följer också som konsekvens i alla auktoritära styrsätt. Korruption kan göra lagar och avtal praktiskt åsidosatta. Därför är det av stort intresse att bevaka tecken på auktoritära tendenser.

Enligt Juan Linz[14] beskrivning av auktoritarianism karaktäriseras auktoritära regimer av fyra egenskaper[15]:

1. Begränsad, icke representativ politisk pluralism; det vill säga begränsning inom de politiska institutionerna, såsom lagstiftare, politiska partier, intresseorganisationer med flera.

2. Legitimitet genom känslor och regimens centrala betydelse för att mota det onda i samhället, såsom lätt igenkännbara samhällsproblem.

[13] Förklaring av begreppet; https://www.britannica.com/topic/checks-and-balances
[14] Förklaring vem Juan Linz var; https://www.britannica.com/biography/Juan-Linz
[15] Länk till publikation;
https://www.academia.edu/39203506/I_B_33_An_Authoritarian_Regime_The_Case_of_Spain?f_ri=36135

3. Varken koncentrerad eller omfattande politisk mobilisering är tillåten samt begränsningar för massmöten vilket fungerar som repressiv metod mot motståndare och ett förbud mot politisk verksamhet som undergräver regimen (till exempel uppror eller subversion).
4. Den formella, verkställande makten är inte tydligt definierad, ofta skiftande och vag.

Några aspekter att titta efter i omvärldsbevakning:

- Leta efter tecken på något av Juan Linz fyra egenskaper (ovan).
- Där lagar ändras från allmänhetens bästa till förmån för auktoritärt styrsätt t.ex. att presidenten får total juridisk frihet.
- Tecken på korruption som involverar högsta lagren av regeringen.
- Extrem personkult kring politisk ledare.
- Tecken på krav eller regler för hur personer skall tänka.

Möjliga exempel kring denna risk:

- Tysk Ambassadör i USA varnar för konstitutionell förändring med kommande regering. Länk
- Teknikbolagen ”donerar” stora belopp till presidentens installation. Länk
- Inga myndigheter får agera oberoende t.ex. i juridisk tolkning, presidentämbetet har sista tolkningsrätt. Länk
- Presidenten exekutiva orders mot flera kända advokatfirmor lyfter oro för konstitutionellt problem. Länk
- Regeringen byter namn på ”Golf of Mexico” och kräver att it-bolag och media bara nämner nya valda namnet på platsen. Nyhetsorganisationen AP vägrar (Google ändrar i Google maps) och blir blockerade från vita huset event. Länk
- Presidenten kan se sig som president en tredje period. Länk
- USA försöker tvinga företag i EU att ifrågasätta likabehandlingsprinciper. Länk
- Svenska bolaget Ericsson ändrar sin egen policy att utesluta ”mångfald och inkludering” efter amerikanska regeringens påtryckningar. Länk
- Misstänkt miljonmiddag exkluderar vissa Nvidia produkter från tulltaxa. Länk
- Misstänkt lobbyverksamhet får presidenten att ändra migrationsfrågan. Länk
- Knappnålshuvud av presidenten i guld för att visa lojalitet. Länk
- Anställda på USA:s utrikesdepartement ska anmäla kollegor som har antikristna fördomar, organiserad brist på religionsfrihet. Länk

4. Handelskrig och handelsregler

USA inledde våren 2025 ett handelskrig med nästan hela världen (ej Ryssland).

För offentlig sektor kan detta medföra dyrare it-lösningar från leverantörer i USA.

Det föreligger en risk att höjda licenskostnader kan mana offentlig sektor att vilja ”nyttja licensen mer” d.v.s. även använda de delar av tjänsten som man tidigare bedömt vara oförenliga med gällande lagkrav.

Det finns också en uttalad risk att EU kräver leveransstopp av amerikanska it-lösningar inom EU, som en handelskrigsmotåtgärd. Åtgärden har planerats av EU under flera år och kallas Anti-Coercion Instrument (ACI).[16]

Några aspekter att titta efter i omvärldsbevakning:

- Stigande priser oavsett given orsak
- Nya licensupplägg och tjänsteupplägg inom molntjänster

Möjliga exempel kring denna risk:

- Svåra följder för teknikbolagen kring USA:s tulltaxa, kommer få stora konsekvenser. Länk
- Frankrike pekar ut tekniksektorn för EU motdrag för USA:s tulltaxa. Länk

5. Totalförsvar och myndigheters digitala beredskap

Enligt både statsministern och överbefälhavaren är Rysslands invasion av Ukraina Sveriges i särklass största säkerhetsfråga[17] och har fått Sverige att gå med i NATO. Vårt land gör nu den största omställningen av samhället i modern tid (nuvarande upprustning av totalförsvaret).

USA har helt vänt om i stödet för Ukraina. USA röstar med Ryssland i FN:s säkerhetsråd och har avbrutit det finansiella och militära stödet till Ukraina. USA försöker tvinga Ukraina till eftergifter för att få fram en temporär men sannolikt instabil fred. Från att ha varit Sveriges viktigaste försvarsallierade är landet nu istället på samma sida som Sveriges största militära säkerhetshot, Ryssland.

Det här påverkar offentlig sektors digitala beredskap i kris och krig. USA har avvecklat det mesta av sin cybersäkerhetsförmåga mot Ryssland[18] (hybridkrig och signalvärde) och använt geopolitik för att, genom it-lösningar tvinga Ukraina till eftergifter kring ockuperad mark och egna mineralintäkter. Vidare hotar USA vårt grannland Danmark med invasion av Grönlandregionen (för en källa se första exemplet nedan). Ett svensk it-beroende till amerikanska it-lösningar kan utsätta den egna rådigheten över digital beredskap, för en ökad sårbarhet.

Några aspekter att titta efter i omvärldsbevakning:

- Hot om invasion av suveräna länder, inklusive NATO-medlemmar
- Amerikanska beslut och aktiviteter som gynnar Ryssland och/eller motverkar Ukrainas suveränitet
- Uttalanden och direkta eller indirekt hot i försvarssamarbeten exempelvis, men inte enbart, genom NATO.

Möjliga exempel kring denna risk:

- USA hotar att invadera Grönland (Danmark), Kanada, Panama. Länk
- USA röstar med Ryssland om Ukraina i FN:s säkerhetsråd. Länk
- USA drar in militärt stöd till Ukraina. Länk
- USA uppmanar Ryssland att attackera NATO-länder som inte betalar tillräckligt. Länk

---

[16] EU kommissionens förklaring av ACI; https://policy.trade.ec.europa.eu/enforcement-and-protection/protecting-against-coercion/qa-regarding-anti-coercion-instrument_en?prefLang=sv

[17] Regeringens deklaration om högsta prioritering kring säkerhetsläget; https://www.regeringen.se/regeringens-politik/regeringens-prioriteringar/sakerhetspolitiska-laget/om-regeringens-prioritering-sakerhetspolitiska-laget/

[18] Artikel om det nedmonterade cyberförsvaret av den nya administrationen; https://observer.com/2025/04/trump-cybersecurity-firings-cisa-nsa-china-threats/

- USA utövar påtryckning på Ukraina för tvingande avtal kring mineraler. Länk
- USA startar handelskrig mot allierade och Ukraina men inte Ryssland. Länk
- USA har sannolikt en inbyggd fjärrstyrd ”stoppknapp” på jaktflygplanet F35. Länk
- USA minskar sin cybersäkerhetsförmåga och avskedar NSA-chef. Länk
- Sverige har stor mängd militärt material med ett beroende till USA, 92 % av alla inköp mellan 2020–2024 kom från amerikanska tillverkare och tjänster. Länk
- Flera ”mystiska” undervattenskabelsabotage hotar svensk access till omvärldens internet. Länk

Bilaga 1 Att jobba med risker i offentlig verksamhet

All offentlig verksamhet har en beslutad riskmodell.

Sannolikt är denna beslutade riskmodell i ringa grad anpassad till it-beredskap för en offentlig verksamhet med en hög grad av digitalisering i globala ekosystem. Därmed är tidigare riskmodeller sannolikt inte väl förberedda till nya geopolitiska it-risker. Viss anpassning kommer troligtvis behöva göras till nuvarande beslutade riskmodeller så att de bättre speglar konsekvenserna av en hög digitaliseringsgrad, eventuell nyligen uppdaterad bedömning av sina informationsmängder och eventuella justerade uppdrag kring totalförsvaret.

”En vägledning för arbete med riskhantering”

MSB kommer inom kort publicera en vägledning *En vägledning för arbete med riskhantering* för den som ska leda arbetet med riskhantering för samhällsviktig verksamhet.[19]

MSB Vägledning kring riskarbete

Begreppen risk och riskhantering är mycket breda och kan betraktas utifrån flera perspektiv. Syftet med MSB:s 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:

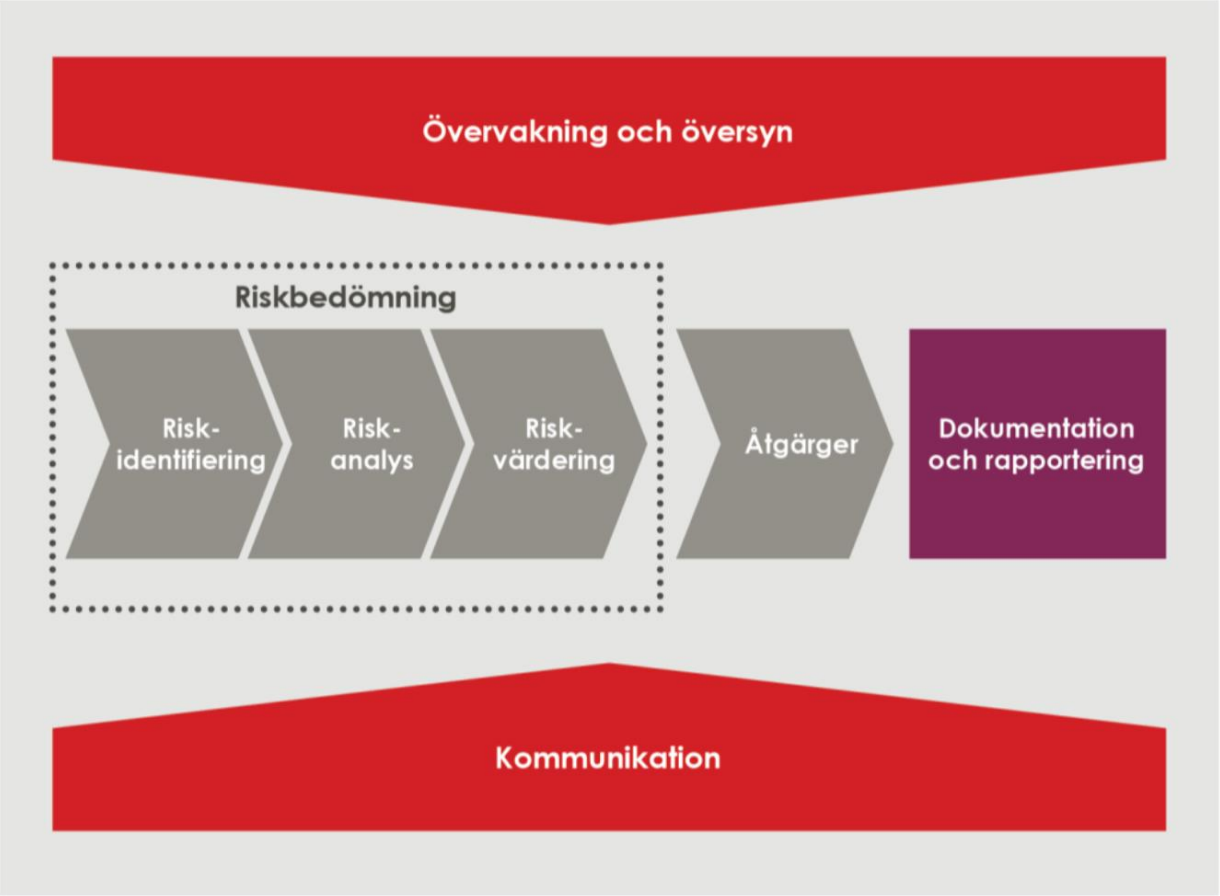
- Förordning (2022:524) om statliga myndigheters beredskap.
- Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.
- CER-direktivet.

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.

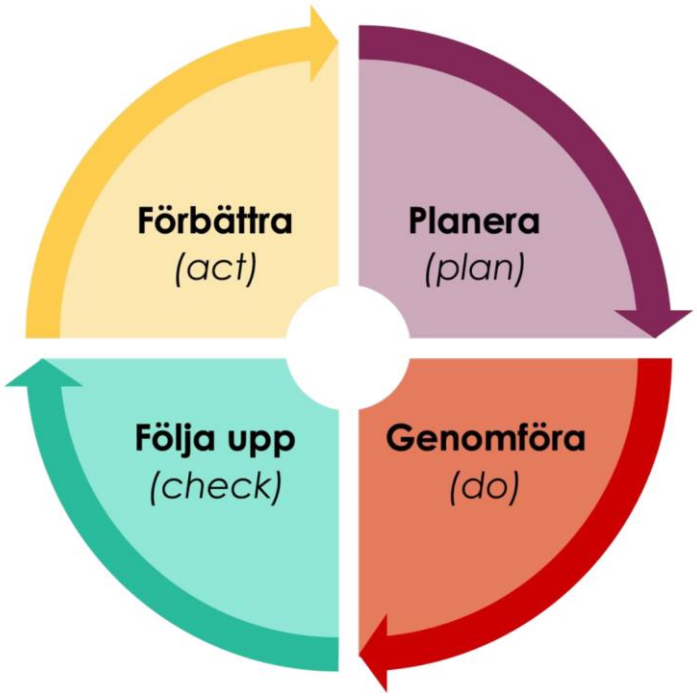
Genom att arbeta systematiskt med riskhantering kan sannolikheten för, och konsekvensen av, negativa händelser minimeras. Det är viktigt att riskhanteringsarbetet integreras i organisationens ordinarie processer eftersom det utgör en viktig del i en organisations samlade civila beredskapsarbete.

[19] Alla rekommendationer hädanefter i bilaga 1 och nedan bilder kommer från remissutgåvan av kommande vägledning för riskarbete; https://www.msb.se/sv/aktuellt/nyheter/2025/mars/ny-vagledning-for-riskhantering--lamna-dina-synpunkter/

Figur 1 Riskhanteringsprocess



Enligt MSB rekommenderas verksamheter att följa cykliska modellen Plan-Do-Check-Act (PDCA). På så vis blir arbetet med riskhantering strukturerat och systematisk. Se MSB:s bild för detta riskhanteringskretslopp här:



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.

Planera

Här sätt ambitionsnivån och syftet med arbetet, där blir vikten av förankring och mandat hög för framgång i riskarbetet.

Sannolikhet

Är något som tas upp i denna första viktiga del av riskarbetet och organisationer kan jobba enligt tabeller likt:

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

Riskvärde

Detta sätts i paritet med konsekvens för att få fram ett riskvärde.

Tabell 3 Text

Konsekvens	Försumbar 1	Måttlig 2	Allvarlig 3	Katastrofal 4

Kriteriemodell

Konsekvenstyper kan även utvecklas i en kriteriemodell, se exempel i tabell 4. 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.

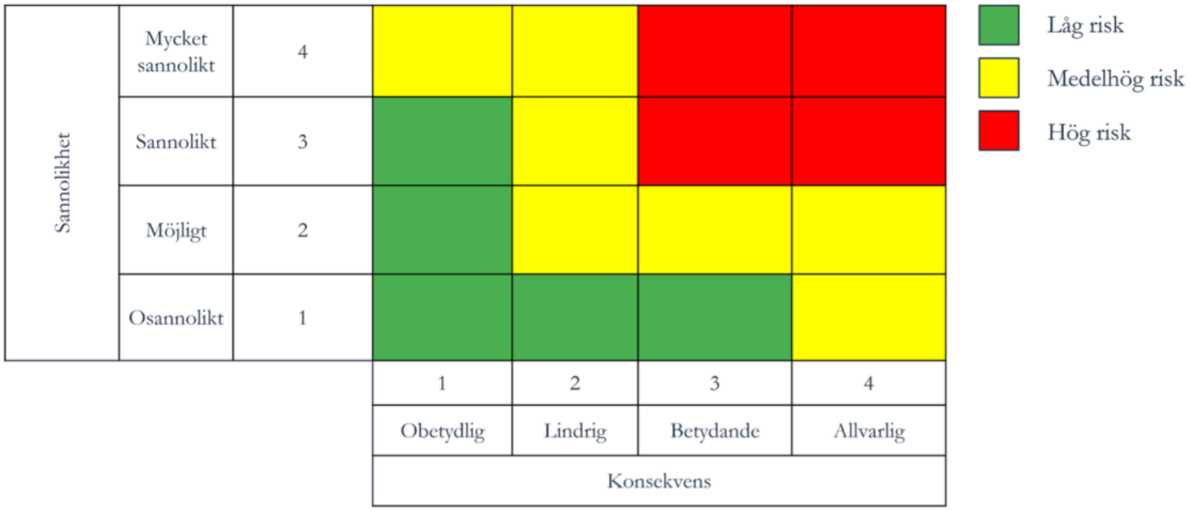
Tänk på att en kriteriemodell ofta används även inom arbetet med kontinuitetshantering.
Om en kriteriemodell redan finns, eller om den utvecklas inom ramen för antingen riskhanteringsarbetet eller kontinuitetshanteringsarbetet, säkerställ att ni använder samma kriteriemodell oavsett vilket perspektiv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

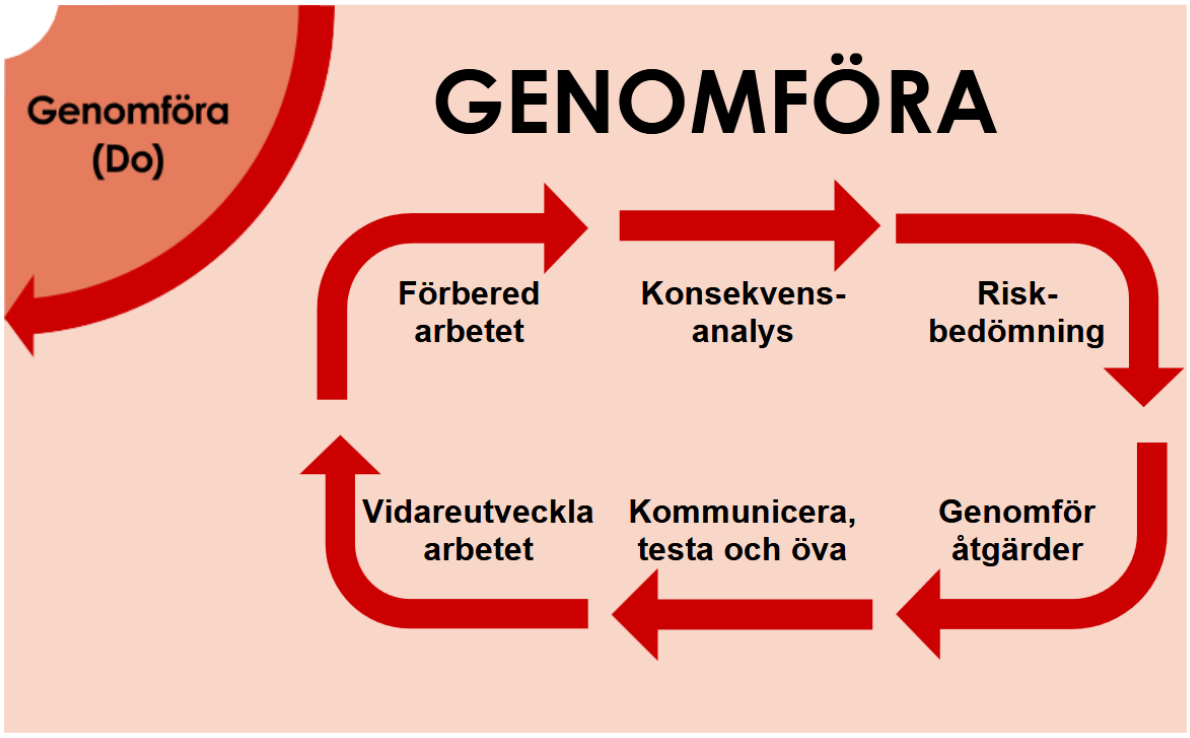
Om en riskmatris används ska denna vara väl förankrad i organisationen och dess styrande dokument. Riskmatrisen definieras i Planera-fasen av PDCA-cykeln, sedan används den i Genomföra-fasen vid riskbedömningen. Förslag på riskmatris:

Figur 2 Se förslag nedan



Genomföra

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



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.

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.

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

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

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

Åtgärder - Hur formuleras, väljs och hanteras 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.

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
- 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.

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.

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)

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.

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.

Följa upp

Hur kan organisationens arbete med riskhantering följas upp?

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.

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

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 ovan.

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?

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 och organisationen.