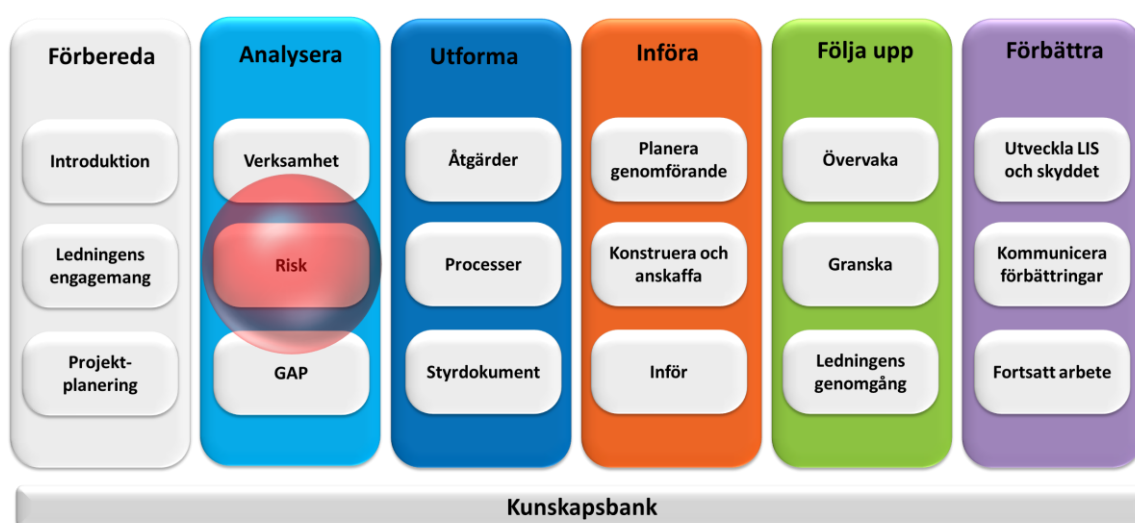




Risikanalyt



Det här dokumentet är en del av Ramverket för informationssäkerhet som finns att tillgå på www.informationssäkerhet.se



Upphovsrätt

Tillåtelse ges att kopiera, distribuera, överföra samt skapa egna bearbetningar av detta dokument, även för kommersiellt bruk. Upphovsmannen måste alltid anges som "MSB, www.informationssäkerhet.se". Vid egna bearbetningar får det inte antydast att MSB godkänt eller rekommenderar bearbetningen eller användningen av det bearbetade verket. Dessa villkor följer licensen "Erkännande 2.5 Sverige (CC BY 2.5)" från Creative Commons. För fullständiga villkor, se <http://creativecommons.org/licenses/by/2.5/se/legalcode>.

Författare

Helena Andersson, MSB
Jan-Olof Andersson, RPS
Fredrik Björck, MSB konsult (Visente)
Martin Eriksson, MSB
Rebecca Eriksson, RPS
Robert Lundberg, MSB
Michael Patrickson, MSB
Kristina Starkerud, FRA

Publicering

Denna utgåva publicerades 2011-12-15

Innehållsförteckning

1. Inledning	4
1.1 Olika typer av riskanalyser	4
1.2 Fördelar med riskanalyser	5
1.3 Metodens delar	5
1.4 Mallar	6
2. Förberedelser inför analysen	7
2.1 Analysgruppens sammansättning	7
2.2 Information inför analysen	8
2.3 Lokal och utrustning	9
2.4 Tidsplanering	9
2.5 Att inleda en riskanalys	10
3. Riskanalysens arbetsuppgifter	11
3.1 Välj och beskriv analysobjekt	11
Flera analysobjekt	11
Resultat av arbetsuppgiften	11
3.2 Identifiera hot	12
Att tänka på i gruppdiskussionen:	12
Goda råd till analysledaren:	12
Resultat av arbetsuppgiften	13
3.3 Sammanställ och gruppera hot	13
Gruppering av hot	13
Att tänka på i gruppdiskussionen:	13
Goda råd till analysledaren:	13
Resultat av arbetsuppgiften	14
3.4 Bedöm risken – konsekvens och sannolikhet	14
Inplacering av hoten i en matris	14
Att tänka på i gruppdiskussionen:	16
Goda råd till analysledaren:	17
Resultat av arbetsuppgiften	17
3.5 Ta fram åtgärdsförslag	17
Att tänka på i gruppdiskussionen:	18
18	
Goda råd till analysledaren:	18
Resultat av arbetsuppgiften	18
4. Sammanställning och rapport	19
5. Nästa steg	19
Bilaga A: Mall för dokumentation av hot	20
Bilaga B: Dokumentation för handlingsplan	22

1. Inledning

En riskanalys används för att anpassa skyddet så att det passar verksamhetens informationstillgångar. Om man inte känner till vilka risker som finns är det svårt att utforma ett säkert och kostnadseffektivt skydd. Skyddet måste också bygga på någon form av riskanalys om man följer standarden ISO/IEC 27001 när det gäller styrning av informationssäkerhet.

Riskanalys är ett brett område och det finns många metoder och teorier. Den som inte har någon tidigare erfarenhet av riskanalys kan finna mängder av intressant litteratur för att få en djupare förståelse. Syftet med det här dokumentet är dock att ge tillräcklig praktisk kunskap för att komma igång med riskanalysarbetet, och för det krävs inga större förkunskaper.

1.1 Olika typer av riskanalyser

Riskanalyser för informationssäkerhet kan göras i många olika situationer och på många olika nivåer – för verksamheten som helhet, för en särskild informationstillgång, för en specifik applikation, för en serverhall, för en verksamhetsprocess och så vidare. Det är också vanligt att man gör en riskanalys inför större organisationsförändringar. I det här dokumentet gäller diskussionen de riskanalyser som rör verksamhetens befintliga informationstillgångar som identifierats i verksamhetsanalysen. Det är viktigt att komma ihåg att man inte alltid behöver göra en riskanalys per informationstillgång eller objekt utan att man kan också ha ett helhetsperspektiv som ansats för analysen.

Det finns många olika metoder för att göra en riskanalys. Till stor del är det ett hantverk som helt enkelt måste utföras av de personer som vet hur systemen och organisationen fungerar. Metoden som presenteras i det här dokumentet är väl beprövad och bygger på underlag från Rikspolisstyrelsen. Den uppfyller också kraven i 27001-standardens.

1.2 Fördelar med riskanalyser

Riskanalysens viktigaste resultat är en förteckning över de risker som finns, deras potentiella skadeverknin g och tänkbara sätt att hantera riskerna på. Själva arbetsprocessen ger dock ytterligare ett antal positiva bieffekter som till exempel:

- Verksamheten lär sig att hantera risker.
- Verksamheten blir medvetna om hoten.
- Analysgruppen tar fram en realistisk bild av verkligheten.
- Analysgruppen gör en realistisk och trovärdig värdering av riskerna.
- Analysgruppen tar fram beslutsunderlag för att kunna fatta rätt beslut.

1.3 Metodens delar

Erfarenheterna visar att metodiken inte är det svåra med en analys, utan administrationen. Därför är det väldigt viktigt med förberedelser och att deltagarna faktiskt avsätter tid för analysen. Den här metodbeskrivningen fokuserar därför på praktiska tips och råd för att förbereda riskanalysen. När analysgruppen väl är samlad genomförs analysen med hjälp av arbetsuppgifterna i figur 1. I avsnitt 3 nedan beskrivs varje moment mer ingående.

Figur 1. Arbetsuppgifter som ska utföras under en riskanalys



Ibland kan det vara nödvändigt att dela upp riskanalysen på flera tillfällen med olika deltagare. Man kanske väljer att göra en riskanalys för en informationstillgång per tillfälle, eller att göra de olika arbetsmomenten vid olika tillfällen. Ibland kan det vara bra att välja olika deltagare till de olika arbetsmomenten: till exempel ”Ta fram åtgärdsförslag” görs kanske bättre av andra än dem som gjorde ”Riskbedömning”. Det är dock viktigt att en eller två av deltagarna finns med vid samtliga tillfällen för att behålla en ”röd tråd” genom hela arbetet.

1.4 Mallar

Första gången är alltid svårast. För att slippa uppfinna hjulet finns det ett antal mallar att utgå ifrån för att strukturera arbetet med att identifiera risker. Det enklaste är naturligtvis att titta på vilka risker som andra organisationer har identifierat. I slutet av det här dokumentet finns ett antal mallar att använda för att komma igång.

2. Förberedelser inför analysen

Det här avsnittet innehåller goda råd till analysledaren inför en riskanalys. Analysledarens huvuduppgift är att förbereda och leda riskanalysen, vilket förutsätter att han eller hon har goda kunskaper om riskanalysmetoden.

Goda råd till analysledaren

- I längden tjänar man på att låta det inledande momentet ta tid och förvissa sig om att analysgruppen har rätt sammansättning och att arbetsuppgiften är avgränsad. Alla deltagare måste också förstå vad de ska göra.
- Gruppmedlemmarna måste vara medvetna om värdet av deras deltagande. Försök uppmuntra dem till att våga vara aktiva.
- Om förutsättningarna är otydliga kan man behöva gå tillbaka till beställaren för ytterligare information.

2.1 Analysgruppens sammansättning

Det är viktigt att analysgruppen innehåller ett urval personer med tillräckligt bred kompetens. I arbetet bör följande roller finnas med:

- **Beställaren** är den person som initierar en riskanalys. Många gånger är beställaren också mottagare av analysens resultat, till exempel analysledaren.
- **Analysledaren** måste veta
 - hur verksamheten och analysobjektet fungerar på ett övergripande plan
 - hur metoden fungerar
 - hur en analysgrupp ska sättas samman
 - vilket underlag som behövs för analysen
 - vilket resultat som förväntas
 - hur man bör leda en analysgrupp
- **Experter** av olika slag behövs i gruppen. Beroende på typen av analys kan det exempelvis vara IT-tekniker, säkerhetssamordnare och jurister.
- **Objektsägaren** är den person som ansvarar för informationstillgången som ska analyseras. Objektsägaren bör vara med vid riskanalysen.

- **Medarbetare**, det vill säga de som har kunskap om det analysobjekt som analyseras.
- **Dokumentationsansvarig** är den som håller i pennan eller IT-stödet, och som måste kunna metoden och de hjälpmedel som används vid analysen.

Storleken på analysgruppen varierar beroende på vilken typ av riskanalys det gäller. En grupp med fler än tio deltagare brukar dock vara svår att hantera. Vid riskanalyser är det viktigt att gruppen består av rätt personer och att analysledaren har rätt kompetens, att gruppen har tillräckliga resurser och att de administrativa stöd som behövs finns på plats.

2.2 Information inför analysen

Inför en riskanalys är det viktigt att ha tillgång till den information som behövs för att lösa uppgiften. Analysledarens uppgift är att se till att medlemmarna i analysgruppen har förberett sig för detta och har tagit reda på alla nödvändiga fakta. Med stöd av beställaren ska analysledaren även se till att

- varje deltagare ska få tid för deltagande i analysen och känna att uppgiften är viktig och prioriterad
- deltagarna ska få tillräckligt med information för att förstå nyttan med att delta i gruppen

Nödvändig information inför riskanalysen är

- författningskrav, föreskrifter och andra styrande dokument som direkt kan påverka riskanalysen
- statistik som underlättar analysgruppens bedömning
- liknande riskanalyser som kan vara av stort värde för arbetet
- allmänna hotbilder som kan vara till stöd och hjälp för att identifiera hot
- dokument som beskriver dagens lösningar när det exempelvis gäller lokaler, nätverkstopologi och serverdokumentation.

2.3 Lokal och utrustning

Risken analysen ställer krav på lokalen och dess utrustning. Det måste finnas möjlighet att använda skrivtavla, blädderblock eller liknande för att visualisera de olika stegen i analysen. Den framtagna informationen måste hela tiden vara synlig för deltagarna i analysgruppen så att tillbakablickar bli möjliga. eftersom den dokumentationsansvarige ofta sammanställer resultatet i efterhand.

Att tänka på när man planerar lokalen:

- Se till att det finns en skrivtavla och/eller blädderblock.
- Utnyttja gärna övriga ytor i lokalen, exempelvis väggarna.
- Lokalen bör kunna låsas under pauser.
- Om ni behöver något datorstöd, se till att det finns OH-duk, projektor och förlängningsladdar och testa att utrustningen fungerar.
- Välj gärna en lokal som ligger en bit från den normala arbetsmiljön för att undvika spring.
- Ha bra ventilation.
- Tryck upp eller skriv upp begrepp och definitioner synligt i lokalen.
- Tryck upp eller rita matrisen i en lämplig storlek.
- Se till att det finns pennor, tejp och post-it-lappar.

2.4 Tidsplanering

Analysledaren ska ta fram en realistisk tidsplan inför analysarbetet. Vissa delar kan visa sig ta längre tid än beräknat, men det är ändå viktigt att ha ett ”grundschema” att falla tillbaka på för att säkert bli klar i tid. Avsätt tid för flera korta pauser men se till att deltagarna inte springer iväg och jobbar med annat under pauserna. Analysgruppens fokusering är helt avgörande för resultatet.

Ett exempel på tidsschema för analysen

- Inledning med presentation av deltagarna 5–20 minuter.
- Beskrivning av metoden 5–10 minuter.
- Val och beskrivning av analysobjekten 10–40 minuter.
- Vad kan hända? Hotframtagning 30–90 minuter.
- Sammanställning och gruppering av hot 30–60 minuter.
- Riskbedömning – konsekvens och sannolikhet 20–60 minuter.
- Eventuell framtagning av åtgärdsförslag 60–240 minuter.
- Sammanställning av rapport 2–16 timmar.

2.5 Att inleda en riskanalys

Det är bra om beställaren till analysen kan delta under inledningen för att hälsa alla välkomna, berätta om syftet och svara på eventuella frågor. Analysledaren går sedan igenom agendan och hur riskanalysen är tänkt att genomföras. Beskrivningen måste anpassas till deltagarnas tidigare erfarenhet. I detta skede får även deltagarna presentera sig. Efter denna inledning ska deltagarna veta hur riskanalysen går till och vad som förväntas av dem. Dessutom är det viktigt att redan från början lösa praktiska frågor om till exempel tider, måltider och pauser.

Frågor att besvara i gruppen

- Målet med mötet – vilka förväntningar har vi?
- Vilka är här och vilken kompetens har vi?
- Hur lång tid har vi till vårt förfogande?
- Finns alla deltagare tillgängliga under hela tiden?
- Behöver vi gå igenom själva metoden?
- Vem är mottagare av analysens dokumentation och vad kommer mottagaren att göra med resultatet?
- Vilken information och vilka dokument behöver vi gå igenom (se avsnitt ”information inför analysen” ovan)?

3. Riskanalysens arbetsuppgifter

Det här kapitlet innehåller en detaljerad beskrivning av de arbetsmoment som illustreras i figur 1.

3.1 Välj och beskriv analysobjektet

Analysobjekten väljs ut med hjälp av listan på informationstillgångar från den tidigare verksamhetsanalysen. Sedan ska de aktuella informationstillgångarna beskrivas så ingående att alla deltagare är överens om vad som ingår i analysen och vad som ligger utanför. Oftast går det inte att analysera samtliga informationstillgångar, utan man väljer dem som är centrala och kritiska för verksamheten eller som av någon annan anledning är extra intressanta att analysera. Det kan också vara så att analysobjektet redan är givet, ifall man ska göra en analys för exempelvis ett visst IT-system. I så fall beskriver man det objektet. Det kan vara praktiskt att analysledaren och beställaren förbereder det här steget innan analysgruppen träffas.

Flera analysobjekt

Om analysen gäller flera analysobjekt, exempelvis flera informationstillgångar, ska *varje* objekt beskrivas så väl att analysgruppen är överens om objektet och dess avgränsningar. Den tid som är avsatt för riskanalysen kommer att begränsa antalet analysobjekt som kan analyseras vid ett och samma tillfälle. Man får alltså tänka på att anpassa antalet objekt så att tiden räcker för alla. Det tar ofta längre tid än man tror att analysera ett objekt och det är rimligt att hinna 3–5 objekt vid ett och samma tillfälle.

Resultat av arbetsuppgiften

Arbetsuppgiften är klar när

- analysobjekten är valda och beskrivna
- avgränsningarna är tydligt dokumenterade
- alla i gruppen är överens om vad som ska analyseras.

3.2 Identifiera hot

Nästa moment är att identifiera de hot som finns mot analysobjekten. Deltagarna tar fram, diskuterar och dokumenterar alla hot de ser mot respektive analysobjekt genom att besvara frågorna:

- Vilka är hoten mot informationstillgångarna?
- Vad kan inträffa?

För att alla deltagare ska få möjlighet att ta fram hot bör gruppen använda sig av "brainstorming". Varje deltagare kan till exempel på en lapp skriva ner hot som kan inträffa eller saker som redan har hänt. Alla hot samlas sedan in och går igenom.

Det är viktigt att analysdeltagarna verkligen försöker beskriva hoten så att alla förstår. I stället för att skriva "hacker" som ett hot bör man till exempel skriva "en extern angripare hackar sig in i systemet x för att ta del av uppgifterna y". Det blir då lättare att bedöma risken i kommande steg. Alla måste förstå och vara överens om innebörden i hoten.

Att tänka på i gruppdiskussionen:

- Lyssna extra noga på de personer som arbetar aktivt med den berörda verksamheten.
- Vad kan hända?
- Vad har hänt som kan hända igen?
- Fokusera på hoten – undvik att tänka i lösningar!
- Undvik för långa diskussioner om det befintliga skyddet.
- Låt alla komma till tals.
- Experter måste tänka på att tala så att alla förstår.

Goda råd till analysledaren:

- Den dokumenterade bilden av analysobjektet ska alltid finnas tillgänglig och det är viktigt att gruppen stämmer av mot den hela tiden för att inte avvika från ämnet.
- Ett bra sätt är att deltagarna använder sin kunskap och sin fantasi för att lista vad som kan hända i de olika hotsituationerna. Till exempel kan varje deltagare beskriva tre relevanta hot. Se till att uppmuntra och inspirera deltagare som har svårt att komma igång.
- Det kan vara bra att ha tidigare analyser och hotkataloger "i bakfickan". Du som analysledare kan använda dem som inspiration.
- Gå igenom hoten med gruppen och sammanställ dem på en skrivtavla eller i en dator. Beskriv varje hot tydligt och se till att alla i gruppen förstår.

Resultat av arbetsuppgiften

Arbetsuppgiften är klar när

- alla tänkbara hot mot varje valt analysobjekt är dokumenterade
- varje hot är tydligt dokumenterat och satt i sitt sammanhang.

3.3 Sammanställ och gruppera hot

I nästa moment ska dubletter tas bort, hoten sorteras efter grupp, och de hot som bedöms ligga utanför avgränsningen tas bort. Eventuellt måste vissa hot förtydligas.

Gruppering av hot

Med hjälp av analysledaren ska gruppen försöka beskriva hoten på ett strukturerat sätt. Målet är att gruppera liknande hot med varandra, ta bort dubletter och förtydliga vissa hot om det behövs.

Använd post-it-lapparna och gruppera hoten så att de är lättare att hantera. Situationen styr hur man väljer att gruppera hoten i olika kategorier men ofta brukar det falla sig naturligt när man börjar flytta runt lapparna och ser ett mönster.

Tänk på att vissa hot riktar sig mot flera informationstillgångar. Det kan därför vara bra att göra en grupp för varje informationstillgång.

När de huvudsakliga hoten är tydliga ska de dokumenteras. I det här dokumentet finns en mall som kan användas.

Att tänka på i gruppdiskussionen:

- Finns det flera hot som egentligen är ett och samma och som kan slås ihop?
- Finns det hot som är relevanta för mer än det aktuella analysobjektet?
- Behöver något hot kompletteras eller tas bort?

Goda råd till analysledaren:

- Här är det viktigt analysledaren hittar ett sätt att gruppera hoten så att de blir hanterbara.
- Fundera över vem som är lämpligast att göra grupperingen; analysledaren eller hela gruppen.

Resultat av arbetsuppgiften

Arbetsuppgiften är klar när

- gruppen har en hanterbar mängd hot som är numrerade och tydligt beskrivna
- hoten finns nedskrivna och tillgängliga för deltagarna, till exempel på en skrivtavla eller i ett datorframställt dokument.

3.4 Bedöm risken – konsekvens och sannolikhet

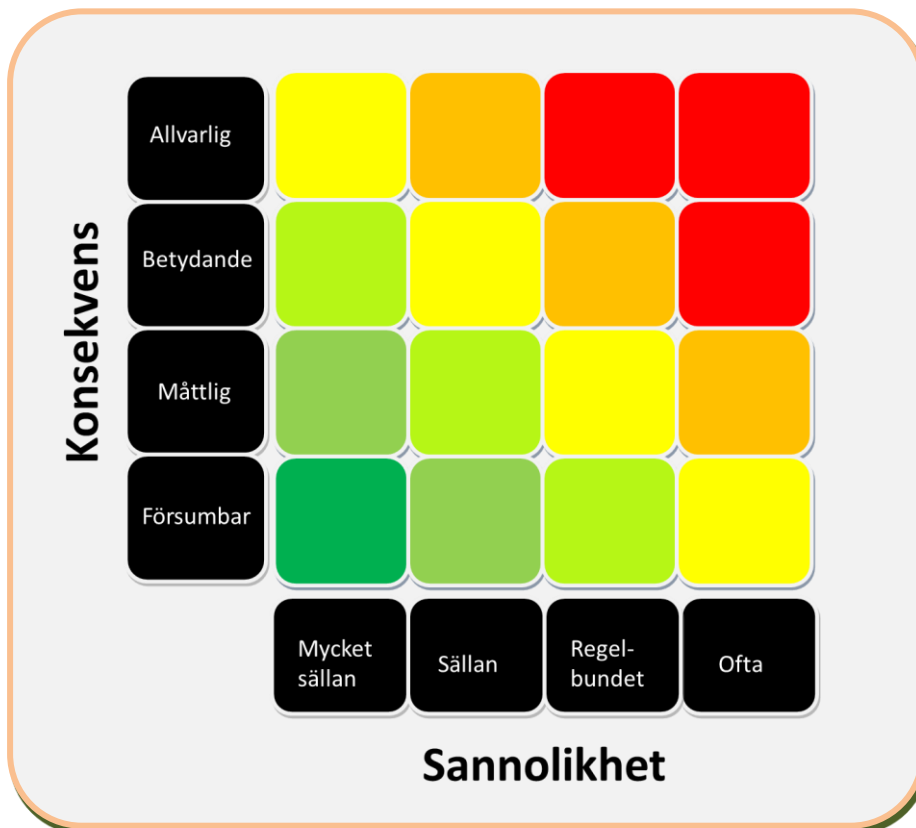
Efter grupperingen är det dags att bedöma vilka konsekvenserna blir om hotet inträffar och hur sannolikt det är.

Inplacering av hoten i en matris

Varje enskilt hot ska bedömas av gruppen och sättas in på sin plats i en konsekvens- och sannolikhetsmatris (figur 2). Med matrisens hjälp kan analysgruppen bedöma risken (konsekvensen och sannolikheten) för ett hot. Det är viktigt att alla förstår matrisen och att gruppen är överens om hur de ska bedöma konsekvens och sannolikhet. Därför kan man börja med att diskutera klassificeringsmodellen och vad den innebär och också komma överens om vilken betydelse varje kategori ska ha. Matrisens resultat kommer senare att ligga till grund för bland annat prioriteringen av olika åtgärder.

För att minska ”grupptricket” kan det vara bra om varje deltagare börjar med att på egen hand placera in riskerna i matrisen. Analysledaren kan sedan sammanställa de enskilda bedömningarna och använda detta som utgångspunkt för en fortsatt diskussion i gruppen.

Figur 2. Exempel på konsekvens- och sannolikhetsmatris



Sannolikheten anger hur troligt det är att hotet kommer att inträffa enligt följande kategorier:

- mycket sällan – en gång på 100 år
- sällan – en gång på 10 år
- regelbundet - årligen
- ofta – mer än en gång per år.

Konsekvensen är ett mått på hur mycket verksamheten skadas om hotet blir verklighet. Påverkan kan exempelvis vara direkt eller indirekt, ekonomisk eller medmänsklig. Modellen innehåller följande fyra nivåer:

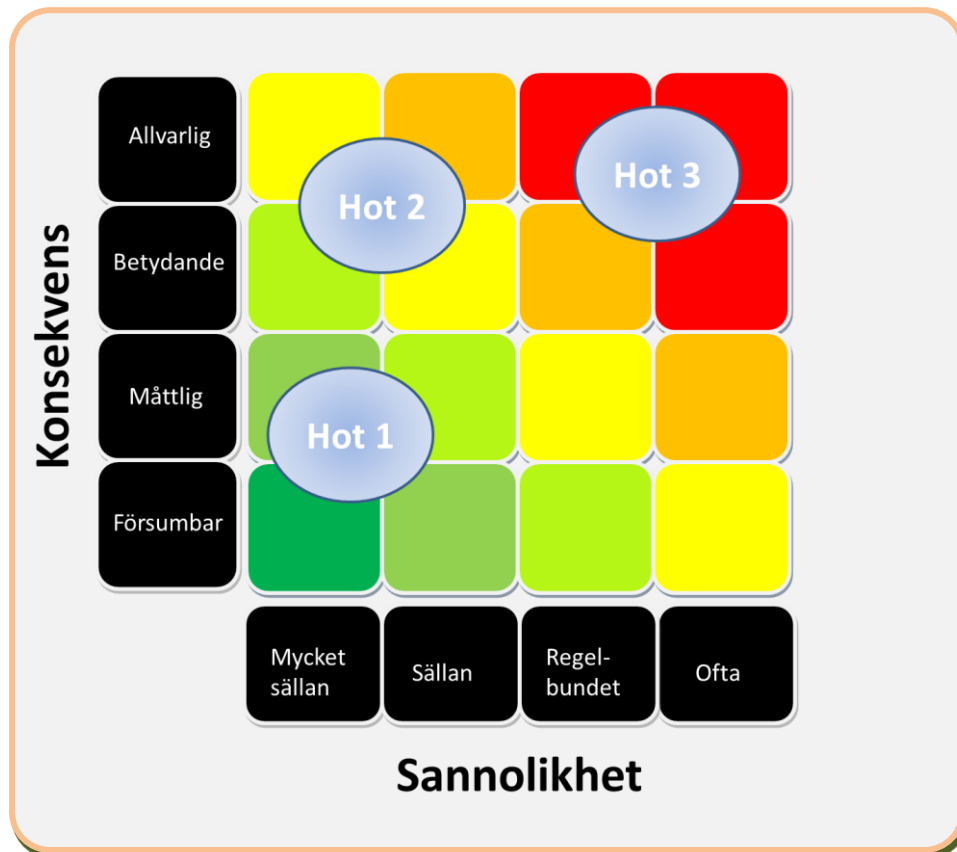
- försumbar skada
- måttlig skada
- betydande skada
- allvarlig skada

Definitionerna av konsekvens och sannolikhet är ett riktmärke och kan förändras, och det är viktigt att gruppen går igenom definitionerna och ändrar det som behövs. Eventuella förändringar ska dokumenteras och tas med i

slutrapporten. Konsekvenserna kan dokumenteras i samma mall som användes för att dokumentera hotet.

När alla sannolikheter och konsekvenser är bestämda kan varje hot placeras in i matrisen (figur 3).

Figur 3. Exempel på ifylld matris



Att tänka på i gruppdiskussionen:

- Alla i gruppen ska förstå hur matrisen fungerar och vad konsekvens och sannolikhet innebär.
- Om begreppen känns oklara eller inte riktigt passar in i analysen är det viktigt att gruppen tillsammans bestämmer sig för en tolkning.
- Man kan behöva flera matriser om man har flera analysobjekt.

Goda råd till analysledaren:

- Detta är den svåraste delen i analysen för deltagarna. Se till att ta paus när deltagarna blir trötta.
- Börja med att ta fram konsekvenserna och sedan sannolikheten.
- För att kunna använda matrisen på ett korrekt sätt måste alla begrepp i tabellen vara enhetligt definierade och alla deltagare förstå deras innebörd. Sätt gärna upp begreppen på tavlan så att alla kan läsa dem.
- Om deltagarna inte är överens är det viktigt att alla tillsammans bestämmer sig för en tolkning och även dokumenterar denna tolkning.
- Om för mycket tid går åt att bedöma konsekvenser och sannolikhet bör analysledaren bryta diskussionen och försöka komma till konsensus.

Resultat av arbetsuppgiften

Arbetsuppgiften är klar när

- det går att överblicka vilka risker som finns, vilka konsekvenserna blir om de blir verklighet och hur sannolikt det är att de inträffar
- resultatet finns visualiserat i en konsekvens- och sannolikhetsmatris.

3.5 Ta fram åtgärdsförslag

Sedan ska deltagarna gå igenom de identifierade riskerna och ta fram förslag på hur de kan hanteras. Detta kan gruppen dokumentera i samma mall som användes i de föregående stegen (bilaga A). Det finns två sätt att arbeta med åtgärderna.

Alternativ 1: Riskerna ska hanteras senare

Ett alternativ är att riskerna inte ska mötas med några åtgärder ännu. Det gäller om riskanalysen är en del i ett större arbete för att införa ett ledningssystem för verksamhetens informationssäkerhet enligt den processmodell som MSB föreslår på informationssäkerhet.se. I så fall kommer åtgärderna i senare steg, men om deltagarna har bra förslag på åtgärder kan man ändå dokumentera dem.

Risker med stor sannolikhet och stora konsekvenser kanske inte kan vänta eftersom de innebär en allvarlig risk för verksamheten. De riskerna ska i så fall åtgärdas direkt enligt alternativ 2 nedan.

Alternativ 2: Riskerna ska hanteras nu

Det andra alternativet går ut på att ta hand om riskerna på en gång. Den framtagna matrisen visar vilka hot som är allvarligast – de med högst sannolikhet och störst konsekvenser. Med den informationen som utgångspunkt är det sedan dags att diskutera eventuella åtgärdsförslag och prioriteringsordningen för dem. Analysgruppen tar fram ett förslag på lämpliga åtgärder och anger i vilken ordning de bör hanteras.

Att tänka på i gruppdiskussionen:

- Gruppen ska försöka hitta förslag på åtgärder och förbättringar för att eliminera, reducera eller acceptera riskerna.
- Diskutera behovet av sekretess – riskanalysen är troligtvis känslig.

Goda råd till analysledaren:

- Se till att det finns godis, dricka, frukt, kaffebröd eller liknande att bjuda deltagarna på för att få upp blodsockret.
- Gå tillbaka till ursprungsuppgiften och se över den en gång till. Har ni tagit med alla aspekter, kan ni ha glömt något och har alla fått säga sin mening?

Resultat av arbetsuppgiften

Arbetsuppgiften är klar när det finns ett förslag till åtgärder och rekommendationer som mottagaren kan ta ställning till

4. Sammanställning och rapport

Resultatet tas sedan om hand av analysledaren som sammanställer en slutgiltig rapport. Förutom själva analysresultatet är det viktigt att rapporten innehåller all tänkbar information, alla avsteg som gruppen har gjort från analysobjektet och eventuella nya definitioner. Rapporten kan också omfatta annan viktig information, till exempel styrdokument, produktbeskrivningar och ritningar som är värdefulla för resultatet.

Det är viktigt att skriva en bra och kortfattad sammanfattning som på ett enkelt sätt beskriver de risker som analysgruppen funnit, gärna med hjälp av matrisen för att illustrera riskanalysens resultat. Sammanställningen bör även innehålla eventuella förslag till åtgärder och rekommendationer till den som ska fatta beslutet.

Goda råd till analysledaren:

- Anpassa resultatet till mottagaren.
- Beskriv alla rekommendationer tydligt.
- Resultatet ska vara ett tydligt och konkret beslutsunderlag för eventuella föreslagna åtgärder.
- Fundera över behovet av sekretess – riskanalysen är troligtvis känslig.

5. Nästa steg

Den färdiga slutrapporten ska ut på "remiss" till deltagarna som får möjlighet att ge sina synpunkter. Efter det lämnas den till mottagaren för vidare åtgärd. Analysledaren eller någon annan person bör även ge en muntlig framställning av resultatet när mottagaren får slutrapporten

Nu ska mottagaren bedöma hur resultatet ska hanteras, det vill säga se till att ta fram en handlingsplan, avdela resurser och åtgärda de hot som behöver åtgärdas. Handlingsplanen bör ange vilken åtgärd det gäller och vem som är ansvarig för att den utförs, men det bör också stå när den ansvarige tog emot uppdraget. På detta sätt kan man undvika att vissa åtgärder faller mellan stolarna och blir liggande utan någon åtgärd.

Bilaga A: Mall för dokumentation av hot

Benämning	
Beskrivning	

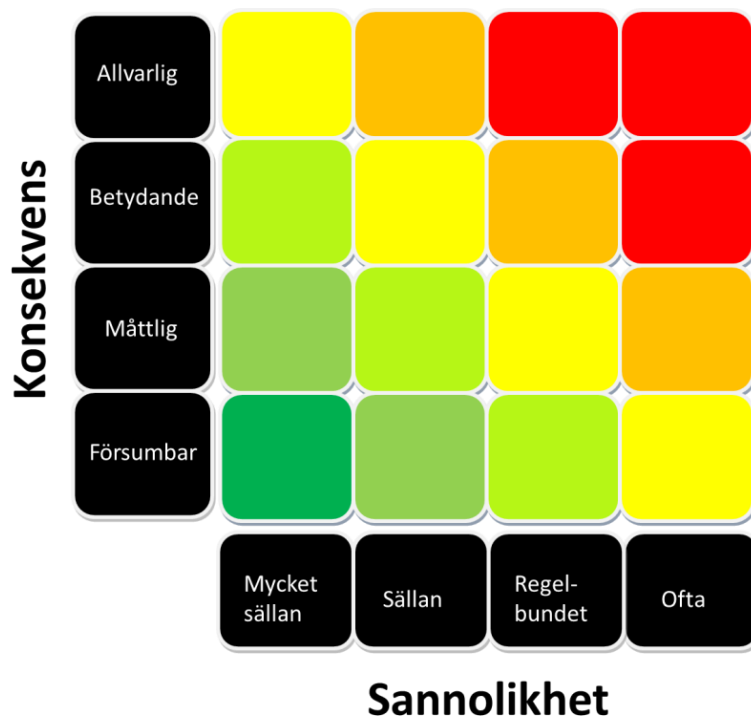
Konsekvenser

Konsekvenser kan exempelvis vara verksamhetskonsekvenser, goodwillkonsekvenser och ekonomiska konsekvenser.

Konsekvenser av det inträffade

Riskbedömning

Markera den bedömda risken i matrisen.



Åtgärder

Nuvarande skydd

Bedömning av nuvarande skydd

Nivå	Bedömning
Det nuvarande skyddet bedöms vara tillräckligt.	Ja/Nej
Det nuvarande skyddet bedöms inte vara tillräckligt men verksamheten accepterar de kvarvarande riskerna.	Ja/Nej
Det nuvarande skyddet bedöms inte vara tillräckligt och det behövs ytterligare åtgärder.	Ja/Nej

Ytterligare skydd som behövs

Bilaga B: Dokumentation för handlingsplan

Prioriterad handlingsplan

Prioritet	Åtgärd	Ansvarig	Datum	Mottaget	Utfört
1				<input type="checkbox"/>	<input type="checkbox"/>
2				<input type="checkbox"/>	<input type="checkbox"/>
3				<input type="checkbox"/>	<input type="checkbox"/>
4				<input type="checkbox"/>	<input type="checkbox"/>
5				<input type="checkbox"/>	<input type="checkbox"/>