UMEÅ UNIVERSITET

# VÄGLEDNING-RISK OCH SÅRBARHETSANALYS

UMEÅ UNIVERSITET

# Innehåll

UMEÅ UNIVERSITET

# 1. Beskrivning

Det här dokumentet beskriver hur en riskanalys går till. Utgångspunkten är det metodstöd som MSB - Myndigheten för samhällsskydd och beredskap tagit fram samt den internationella standarden för informationssäkerhet, SS-EN ISO/IEC 27001/27002/27005 samt ISO 31000.

Metoden går att använda vid en organisationsövergripande riskanalys eller vid en riskanalys av ett enskilt analysobjekt, till exempel en process eller ett IT-system.

Innan riskanalysen påbörjas bör analysobjekt ha identifierats och den informationstillgång som ingår bör ha värderats genom att en klassificering utifrån säkerhetsaspekterna Konfidentialitet, Riktighet och Tillgänglighet är genomförd, Bilaga (MS-Excel) för dokumentation återfinns i Aurora under Informationssäkerhet och rubriken Styrande dokument.

# 2. Bakgrund

I riskanalysen identifieras de hot och oönskade händelser som kan påverka informationssäkerheten i organisationen. En riskanalys går ut på att besvara de tre frågorna; *Vad kan hända? Hur sannolikt är det? och Vad blir konsekvenserna?*

Syftet är att ge ett underlag för beslut om vilka säkerhetsåtgärder som ska införas men också att höja medvetenheten om hot, sårbarheter och risker hos de som deltar i analysen.

För att uppfylla Dataskyddsförordningen och ISO-standarden SS-EN ISO/IEC 27001 krävs:

- Att personuppgifts- och informationssäkerhetsrelaterade risker analyseras,
- Att riskanalysens resultat ligger till grund för val och utformning av säkerhetsåtgärder och det systematiska informationssäkerhetsarbetet.

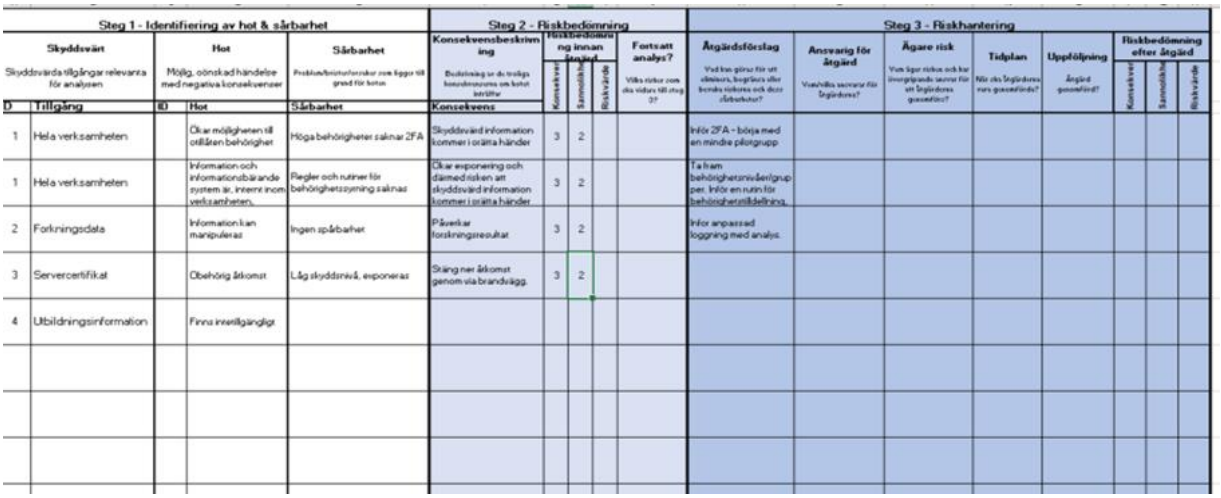
# 3. Användningsområden

Riskanalysens användningsområde är stort och kan genomföras på olika nivåer och situationer. Några exempel på analysobjekt:

- Verksamheten som helhet
- Vid nyanskaffning it-system/tjänst
- Ett forskningsprojekt
- En specifik informationsmängd
- En specifik applikation
- En serverhall
- En verksamhetsprocess
- En organisationsförändring

Nedanstående exempel på mall innefattar själva riskanalysen och ger även stöd för fortsatt arbete med hantering av de identifierade riskerna. Mallen finns tillgänglig på Aurora.

UMEÅ UNIVERSITET



| Steg 1 - Identifiering av hot & sårbarhet | | | | | Steg 2 - Riskbedömning | | | | | Steg 3 - Riskhantering | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Skyddsvärt | | Hot | | Sårbarhet | Konsekvensbeskrivning | Riskbedömning innan åtgärd | | | Fortsatt analys? | Åtgärdsförslag | Ansvarig för åtgärd | Ägare risk | Tidplan | Uppföljning | Riskbedömning efter åtgärd | | |
| Skyddsvärda tillgångar relevanta för analysen | | Möjlig, oönskad händelse med negativa konsekvenser | | Problem/brister/svagheter som ligger till grund för hotet | Beskrivning av de tänkta konsekvenserna om hotet inträffar | Konsekvens | Sannolikhet | Riskvärde | Vilka risker som ska vidare till steg 3? | Vid vilka åtgärder för att eliminera, begränsa eller bemöta riskerna och deras sårbarheter? | Vem/vilka ansvarar för åtgärderna? | Vem äger risken och har övergripande ansvar för att åtgärderna genomförs? | När ska åtgärderna vara genomförda? | Åtgärd genomförd? | Konsekvens | Sannolikhet | Riskvärde |
| ID | Tillgång | ID | Hot | Sårbarhet | Konsekvens | | | | | | | | | | | | |
| 1 | Hela verksamheten | | Ökar möjligheten till otillåten behörighet | Höga behörigheter saknar 2FA | Skyddsvärd information kommer i orätta händer | 3 | 2 | | | Inför 2FA - börja med en mindre pilotgrupp | | | | | | | |
| 1 | Hela verksamheten | | Information och informationsbärande system är, internt inom verksamheten, | Regler och rutiner för behörighetstyrning saknas | Ökar exponering och därmed risken att skyddsvärd information kommer i orätta händer | 3 | 2 | | | Ta ham behörighetsnivåer/grupper. Inför en rutin för behörighetstilldelning. | | | | | | | |
| 2 | Forkningsdata | | Information kan manipuleras | Ingen spårbarhet | Påverkar forskningsresultat | 3 | 2 | | | Inför anpassad loggning med analys. | | | | | | | |
| 3 | Servercertifikat | | Obehörig åtkomst | Låg skyddsnivå, exponeras | Stäng ner åtkomst genom via brandvägg. | 3 | 2 | | | | | | | | | | |
| 4 | Utbildningsinformation | | Finns inetillgänglig | | | | | | | | | | | | | | |

# Genomföra riskanalysen

**1 Utse analysledare**

**2 Bjud in till en workshop** – beskriv syfte och vilken information som ska analyseras. Lämpliga deltagare kan exempelvis vara systemägare, systemförvaltare, informationsägare, IT-systemadministratör.

**3 Förbered** så mycket som möjligt när det gäller beskrivning av tillgången. Finns ett resultat från en klassificering bör den finnas som en grund för den fortsatta riskanalysen. Finns systembeskrivningar över befintlig IT-miljö? Ta reda på vilka lagar och krav som kan påverka. Hotbilder?

3.1 Bestäm avgränsningar

3.2 Identifiera eventuella externa och interna krav

3.3 Beskriv informationstillgången **(hämta från informationsklassningen)** finns det särskild skyddsvärd data?
GDPR: Finns personuppgifter, integritetskänsliga personuppgifter eller känsliga personuppgifter?

Finns forskningsdata? Eventuell data/information som senare kan leda till patentansökan? Finns ett syfte? Informationsmängd? Ta hänsyn till informationstillgångens livscykel.

3.4 Hotbild – använd generella och aktuella beskrivningar av hotbilder i exempelvis trend och årsrapporter (internationella, nationella och sektorsspecifika). Finns tidigare incidentsammanställningar inom organisationen att ta del av?

UMEÅ UNIVERSITET

## 4 Steg 1 – Identifiering av hot och sårbarheter. Vad kan hända?

Vilka hot och vilka sårbarheter har identifierats som kan medföra att en oönskad händelse kan inträffa och ge negativa konsekvenser?

## 5 Steg 2 – Riskbedömning. Lista riskerna – numrera

Riskbedöm genom att titta på sannolikhet och konsekvens för varje risk.

| Konsekvens | | Sannolikhet | Intervall sannolikhet |
|---|---|---|---|
| **(1) Försumbar** | | **(1) Osannolikt** eller **mycket sällan** | < 0,05 ggr/år |
| **(2) Måttlig** | | **(2) Liten sannolikt** eller **sällan** | 0,05-0,5 ggr/år |
| **(3) Betydande** | | **(3) Stor sannolikhet** eller **regelbundet** | 0,5–1 ggr/år |
| **(4) Allvarligt** | | **(4) Mycket stor sannolikhet eller ofta** | 1–10 ggr/år |

**Konsekvens.** Ta del av exempel på specifika konsekvensnivåer i riskanalysens mall för värdering och beskriv konsekvensen kortfattat.

Tänk på att Dataskyddsförordningen ställer krav på att en specifik konsekvensbedömning ska göras om riskanalysen visar att en viss personuppgiftsbehandling bedöms leda till en hög risk för fysiska personers rättigheter och friheter. I sådana fall ska Dataskyddsombudet vid Umeå universitet kontaktas. Detta utesluter inte att i andra fall göra en generell konsekvensbedömning utifrån ett verksamhets-, ekonomiskt-, förtroende- och individperspektiv.

**Sannolikhet** är ett mått som beskriver hur ofta man skattar att en händelse kommer att inträffa. Det finns flera olika sätt att svara på frågan hur troligt ett specifikt riskscenario är. Ett vanligt sätt är att använda sannolikheter eller frekvenser.

5.1 För in värdet för sannolikhet och konsekvens i riskbedömningen.

5.2 Bestäm vilka risker som ska vidare till steg 3.

## 6 Steg 3 - Riskhantering.

6.1 Bedöm vilken säkerhetsåtgärd som kan införas för att eliminera eller reducera risken. Beakta eventuella nuvarande skydd. Ta stöd i ISO 27001 tabell A för att hitta lämpliga tekniska och organisatoriska säkerhetsåtgärder.

6.2 Prioritera och tilldela en riskägare samt vem som är ansvarig för att säkerhetsåtgärden realiseras.

6.3 Sätt tidplan och följ upp.

UMEÅ UNIVERSITET

6.4 Ange riskbedömning efter att åtgärden är införd.

# Riskmatris

Riskernas bedömning – både före och efter att säkerhetsåtgärder har införts kan (valfritt) riskerna visualiseras i riskanalysmallen under fliken Riskmatris i dokumentationsmallen.

# Kompletterande information och slutsats

Om relevant, komplettera i riskanalysmallen, under fliken Komplettering, frågeställningarna nedan.
Kommer bakgrundskunskap att föras in i projektet? Föreligger immaterialrätter kopplade till sådan kunskap?
Hur ska resultat hanteras i projektet – finns krav på nyttjande- eller äganderätter till resultat?

Behöver upphandling av system eller tjänster genomföras av systemet/projektet (observera krav ur GDPR och arkivperspektiv på sådan)?

Ange eventuella slutsatser.