Introduktion till Informationssäkerhet och MSB:s metodstöd

Daniel Bosk, Carina Bengtsson och Lennart Franked [1]

Avdelningen för informationssystem och teknologi (IST),
Mittuniversitetet, Sundsvall.

17 januari 2019

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

1. Informationssäkerhet
   - MSB Metodstöd för Informationssäkerhet
2. Förbereda
   - Introduktion
3. Analysera
   - Verksamhetsanalys
   - Riskanalys

Översikt

Varför behöver samhället detta?

- Information är centralt i dagens samhälle.
- Tillgodoser behov för både individ och samhälle.
- Behöver undvika störningar av våra informationssystem.

Exempel på driftstörning I

Fredag e.m.	Ett större företag som driftar IT-system för många organisationer uppmärksammar en driftstörning. 350 Apoteket-butiker tappar kontakt med sina IT-system. Många andra större organisationer drabbas också, bland andra ett större logistikföretag.
Söndag e.m.	Företaget rapporterar maskinvarufel och påbörjar åtgärder.
Måndag f.m.	Logistikföretag kan inte sköta sin verksamhet och inte nå sina anställda. Bilprovningen har totalstopp i IT-systemet – dessa hanterar 20 000 fordon om dagen – resulterar i körförbud då Transportstyrelsen ej får in godkända kontrollbesiktningar. Nacka kommun övergår till Facebook och Twitter för kommunikation.

Exempel på driftstörning II

Måndag e.m.	Socialkontoren i Nacka och Sollentuna kan ej betala ut försörjningsstöd. Stockholm stads frånvarorapporteringssytem för skolorna ligger nere.
Onsdag lunch	Samtliga Apotek har fått tillbaka sina IT-system.
11 dagar	Logistikföretaget får tillbaka sitt IT-system. Verksamheten är fortfarande inte återställd två månader efter haveritet.

MSB

- Myndigheten för samhällsskydd och beredskap.
- ”MSB utvecklar, tillsammans med andra, individens och samhällets förmåga att förebygga, hantera och lära av olyckor och kriser.”

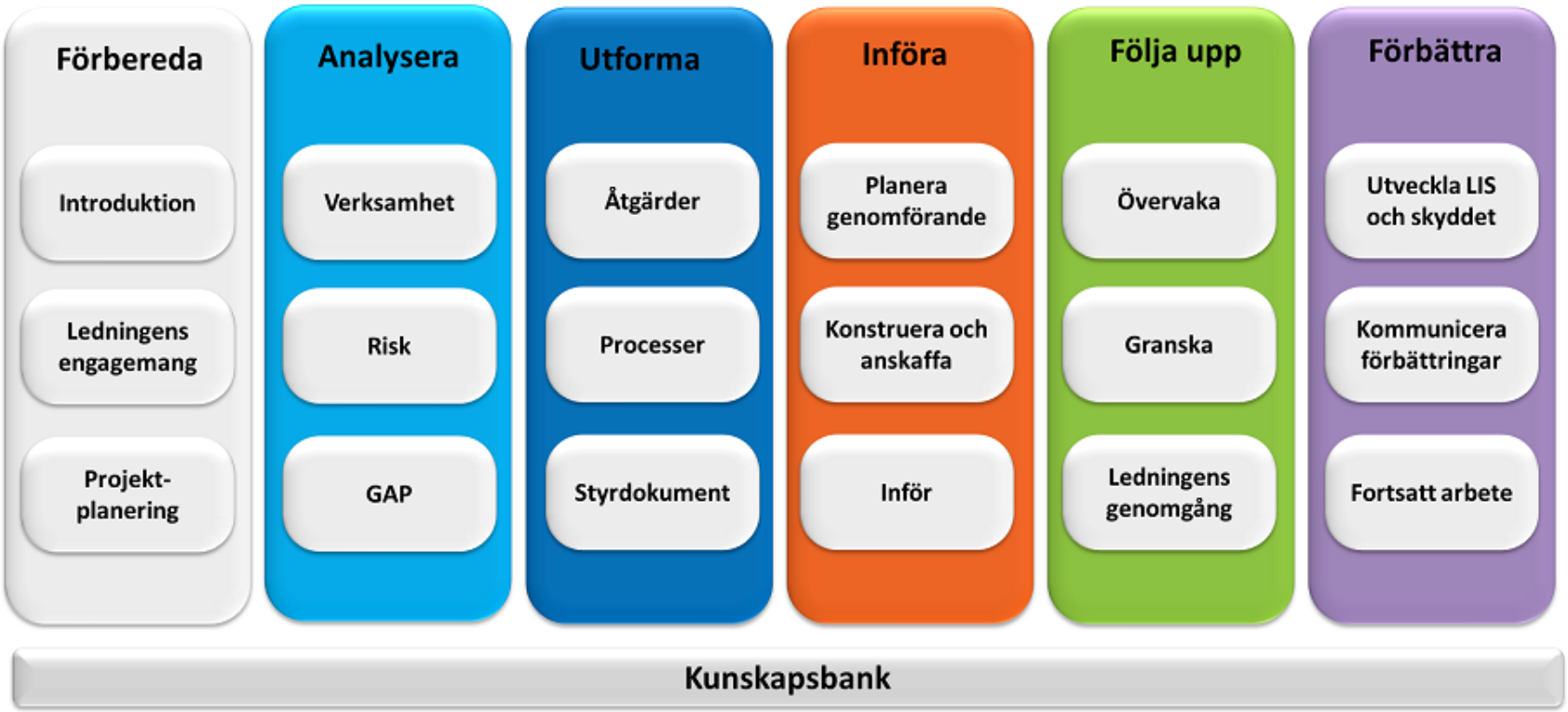
Informationssäkerhet.se

- MSB drev projektet SVISA: Stöd för Verksamheters InformationsSäkerhetsArbete.
- Resulterade i `informationssäkerhet.se`.
- Ska ge praktiskt stöd för systematiskt informationssäkerhetsarbete.

Metodstödet

- Stöd för att bedriva informationssäkerhetsarbete i en organisation.
- Förklarar hur man bygger ett ledningssystem för informationssäkerhet.
- Bör ses som ett ”smörgåsbord”:
  - Ta de delar som är aktuella för verksamheten.
  - Tillämpa dem i den ordning som är lämpligt.
- Informationssäkerhet är komplext:
  - Krävs att den integreras i *hela* organisationen: allt från högsta ledningsnivå till lägsta operativa nivån.

Metodstödet



Figur: Översikt av metodstödet.

Översikt

Vad är informationssäkerhet?

- Uppstår tillsammans med andra processer och verksamheter.
- Informationssäkerheten i en verksamhet har inget egenvärde måste integreras för att kunna skydda verksamheten.

Vad är informationssäkerhet?

- Förmågan att bevara de krav och förväntningar som finns på informationen i verksamheten.
- Bland annat att skydda från haverier likt exemplet som gavs tidigare — om det finns sådana krav!

Krav och förväntningar på informationen

Konfidentialitet Informationen ska endast vara tillgänglig för behörig.

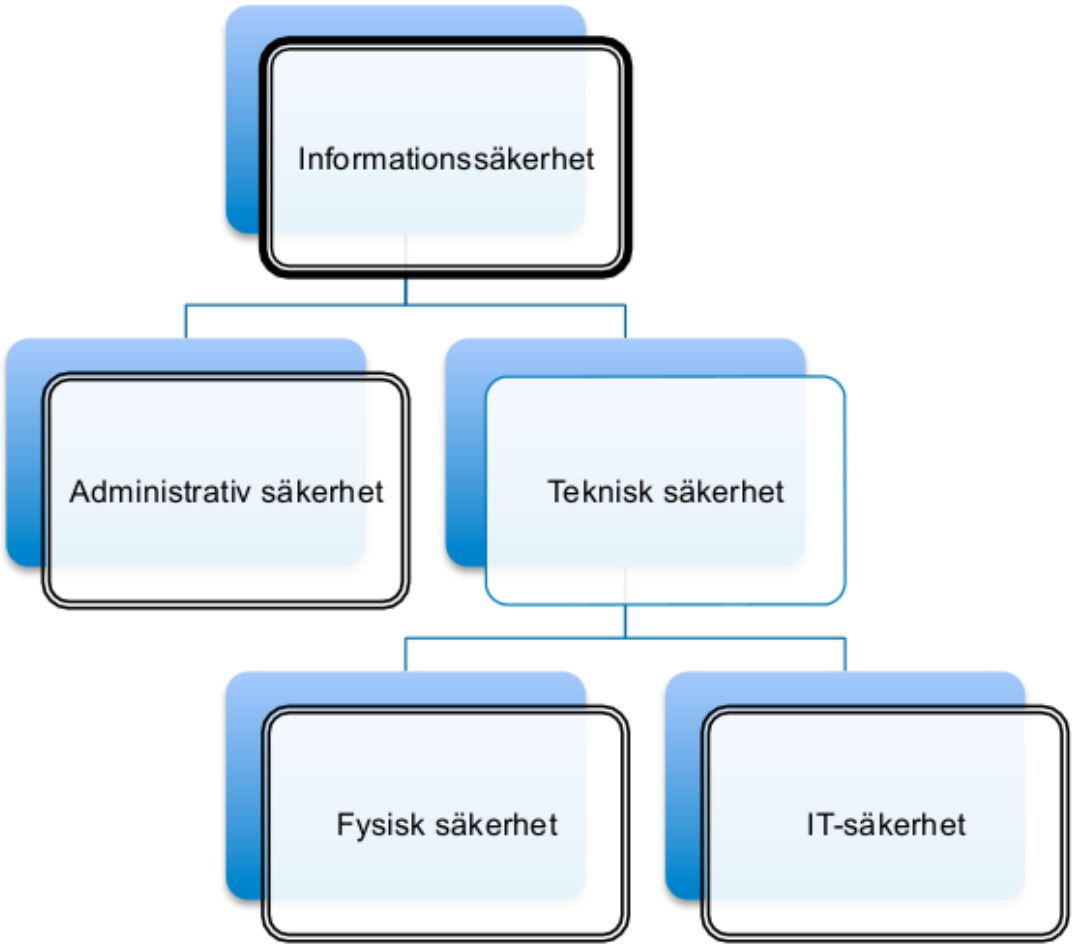
Tillgänglighet Informationen är användbar och finns till hands när den behövs.

Riktighet Informationen är exakt och fullständig.

Krav och förväntningar på informationen

Spårbarhet	Vem har tagit del av eller förändrat information?
Oavvislighet	Det ska inte gå att förneka en handling.
Autentisering	Fastställa en entitets identitet.
Auktorisation	Att ge en autentiserad entitet vissa rättigheter.

Vad är informationssäkerhet?



Figur: Informationssäkerhetens struktur.

Struktur

Figur: Att arbeta med informationssäkerhet.

Säkerheten är inte starkare än den svagaste länken

- Svårgissat lösenord på post-it bredvid datorn.
- Oknäckbart kodlås på glasdörr.
- Det måste finnas förutsättningar för att arbeta säkert.

Varför skydda information?

Frivilligt

Bra för verksamhetens

rykte: vem låter ett företag hantera ens information om de är kända för att göra det vårdslöst;

ekonomi: gott rykte är bättre för ekonomin och kostnader för säkerhetsincidenter minskar;

intern effektivitet: inga förluster av information eller uppehåll i arbetet, jämför med exemplet av en driftstörning som gavs tidigare;

kvalitet: följd blir att kvalietet på arbetet man utför ökar.

Varför skydda information?

Obligatoriskt

PUL 1998:204 säger att personuppgifter inte får hanteras och lämna en verksamhet hur som helst;

Offentlighets- och sekretesslagen 2009:40 säger att viss information *ska* finnas tillgänglig för allmänheten medan annan information *inte* ska det.

Arkivlagen 1990:782 säger att myndigheter måste diarieföra alla allmänna handlingar.

MSBFS 2009:10 gäller myndigheters arbete med informationssäkerhet.

ISO 27000

- Inte bara myndigheter som kan ha nytta av detta.
- Finns möjlighet för certifiering av ISO 27000 för alla organisationer.
- MSB:s metodstöd är alltså anpassat efter dessa internationella standarder.

Ledningssystem

- Alla har ett ”system” för att leda verksamheten.

  *”Ett formaliserat system som används för att göra arbetet mer effektivt med avseende på uppställda mål. Det ska innehålla rutiner och ansvarsfördelningar i hur verksamheten leds och bedrivs, finnas uppsatta mål och riktlinjer för hur de ska uppnås.” [**lis**]*

- Omfattar exempelvis organisationsstruktur, styrdokument, . . .

ISO 27001

- Metodstödet beskriver hur man bygger upp ett LIS utifrån kraven i ISO 27001.
- ISO 27001 är en ständigt pågående systematisk process som strävar mot ständiga förbättringar av arbetssätt och säkerhetslösningar i informationssäkerhetsarbetet.
- Det är viktigt att anpassa detta efter den egna verksamheten – men det innebär inte att man kan hoppa över delar efter eget godtycke.

ISO 27002 – vad ska göras?

- Säkerhetspolicy.
- Organisation av informationssäkerheten.
- Hantering av tillgångar.
- Personalresurser och säkerhet.
- Fysisk och miljörelaterad säkerhet.
- Styrning av kommunikation och drift.
- Styrning av åtkomst.
- Anskaffning, utveckling och underhåll av informationssystem.
- Hantering av informationssäkerhetsincidenter.
- Kontinuitetsplanering för verksamheten.
- Efterlevnad.

Projektorganisation

- Viktigt med bredd: att representera hela organisationen.
- Viktigt med rätt kompetens: projektledning och informationssäkerhet.

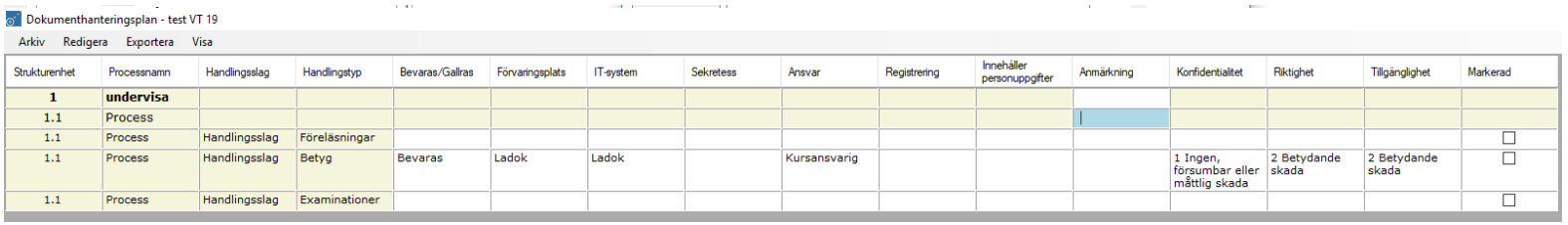
Översikt

Vad ska skyddas?

- Vilka informationstillgångar har vi och hur skyddsvärda är de?
- Vad menas med att skydda dem?

Verksamhetsanalys

- Verksamhetsanalysen syftar till att identifiera informationstillgångar, samt
- hur skyddsvärda de är.
- Ska leda till en strukturerad förteckning över
  - vilka informationstillgångar som finns,
  - vilka krav och förväntningar som finns på dessa, samt
  - vilket värde respektive tillgång har.



Dokumenthanteringsplan - test VT 19

Arkiv Redigera Exportera Visa

Strukturenhet	Processnamn	Handlingsslag	Handlingstyp	Bevaras/Gallras	Förvaringsplats	IT-system	Sekretess	Ansvar	Registrering	Innehåller personuppgifter	Anmärkning	Konfidentialitet	Riktighet	Tillgänglighet	Markerad
1	**undervisa**														
1.1	Process														
1.1	Process	Handlingsslag	Föreläsningar												☐
1.1	Process	Handlingsslag	Betyg	Bevaras	Ladok	Ladok		Kursansvarig				1 Ingen, försumbar eller måttlig skada	2 Betydande skada	2 Betydande skada	☐
1.1	Process	Handlingsslag	Examinationer												☐

Figur: Dokumenthanteringsplan

Exempel på informationstillgångar

- Medarbetare: kvalifikationer, erfarenheter.
- Data: databaser, avtal, dokumentation, prover, rutiner.
- Programvarutillgångar: tillämpningsprogram, systemprogram, utvecklingsprogram.
- Tjänster: data- och kommunikationssystem, försörjningssystem.
- Immateriella: rykte, profil.
- Fysiska: datorutrustning, flyttbar datamedia.

Uppdelning av informationstillgångar

Primära	Avser den huvudsakliga informationen; exempelvis ritning, logg och avtal.
Sekundära	Avser resurser som krävs för att hantera de primära informationstillgångarna.

Vad händer när du inte längre har kvar programmet som kan läsa det proprietära slutna formatet som informationen finns lagrad i?

Hitta informationstillgångarna

- Tidigare kartläggningar?
- Avdelningsvis?
- IT-system?
- Projekt?
- Processer?
- Funktionsvis?

Krav på informationstillgångarna

- För att kunna klassificera behövs kraven kännas till.
- Behöver objektivt sätt att mäta vikten av skydd.
  - Min information är viktigast!
- Vilken information är viktig för att verksamheten ska gå att bedriva?

Legala krav

Avtal lagar och förordningar.

- PUL,
- Arkivlagen,
- Offentlighets- och sekretesslagen,
- MSBFS 2009:10,
- Säkerhetsskyddslagen.

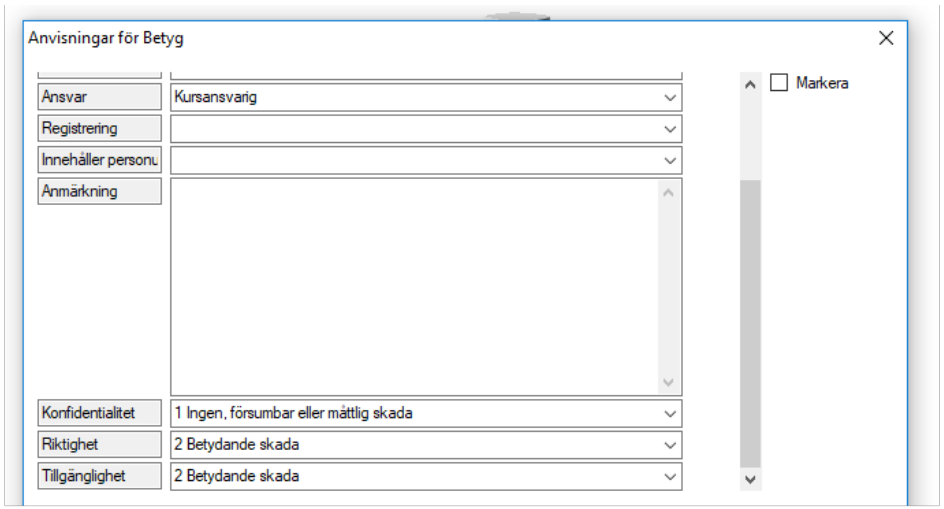
Interna krav

Krav som verksamheten ställer upp för att nå sina mål. Exempelvis:

- Vision,
- affärsidé,
- policyer,
- värdegrund.

Informationsklassificering

- Metod för att värdera hur skyddsvärd en informationstillgång är.
- För att kunna skapa ett lämpligt skydd.
- Värderar respektive tillgång utifrån:
  - tillgänglighet,
  - riktighet,
  - konfidentialitet.
- Varje perspektiv har ett antal skyddsklasser.



Figur: Klassificering av informationstillgång i VisAlpha

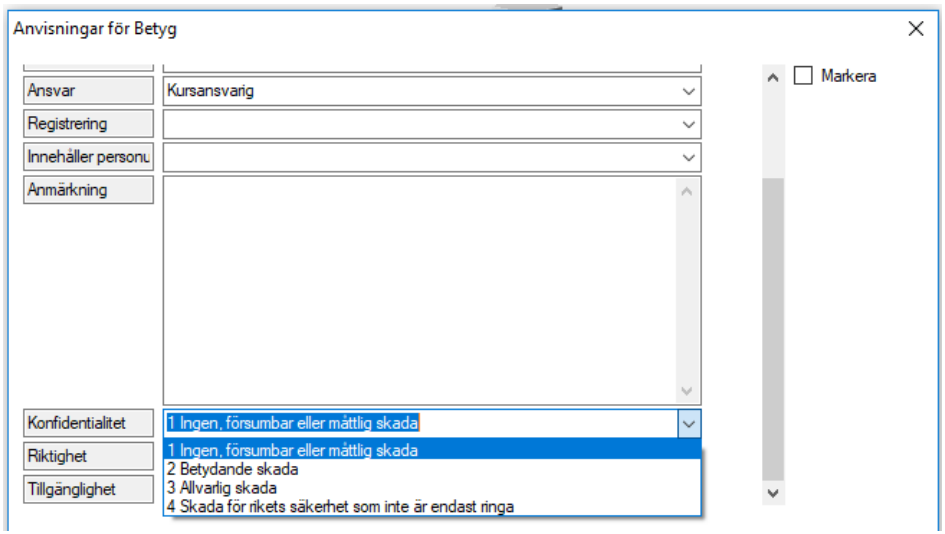
MSB:s förslag på klassificeringsmodell

Säkerhetsaspekt / Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande	Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig	Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ingen eller försumbar*	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. **	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild. **

Figur: MSB:s förslag på klassificeringsmodell.

Informationsklassificering

- Alla tillgångar klassificeras mot alla identifierade krav ur alla perspektiv.
- Informationsägaren klassificerar.
- Anpassa gärna modellen efter verksamheten.



Figur: Klassificeringsnivåer i VisAlpha

Riskanalys

Måste göra avgränsningar:

- Vilka informationstillgångar vill man göra riskanalys på?
- Vilka tillgångar är inte tillräckligt kritiska för en riskanalys?

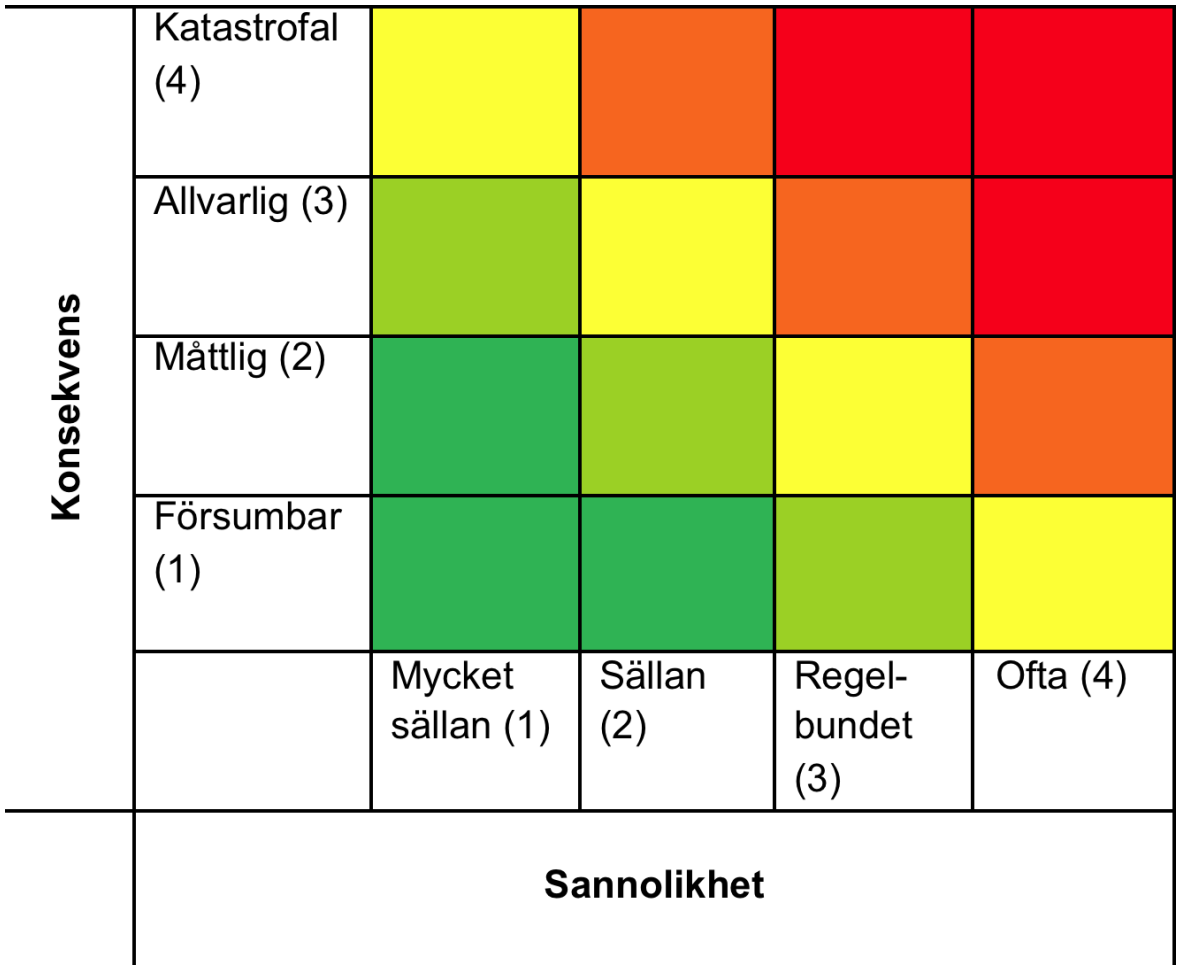
Riskanalys

- Används för att anpassa skyddet efter verksamhetens tillgångar.
- Genererar en förteckning över
  - befintliga hot,
  - hotens skadeverkningar, och
  - förslag på riskhantering.

Identifiera hot

- Använd brainstorming för att ta fram förslag på hot.
- Ta med alla förslag!
- Var specifik: avsiktligt eller oavsiktligt informationsläckage.
- Exempel:
  - Medarbetare avsiktligt saboterar ett system.
  - Medarbetare snubblar i nätverkskablarna som är dragna på golvet.
  - Buggar i programvara.
  - Brand, översvämning.

Riskmatris



Figur: En riskmatris.

Riskmatris

Konsekvenser

- Hur allvarlig blir konsekvensen för verksamheten om hotet blir verklighet?
- Klargör för *vem* det blir en konsekvens: verksamheten genom bieffekt av konsekvenser för samhället?
- Underlättar att ange exempel för de olika nivåerna, exempelvis: kostnader, försämrat rykte, ...

Allvarlig – Betydande – Måttlig – Försumbar

Riskmatris
Sannolikhet

- Hur troligt är det att hotet inträffar?
- Underlättar med exempel för nivåerna: år, veckor, dagar?

Mycket sällan – Sällan – Regelbundet – Ofta

Riskbehandling

- Besluta om de identifierade hoten ska åtgärdas eller accepteras:
  - Acceptera,
  - eliminera,
  - överföra,
  - behandla.
- Vilka åtgärder ska vidtas?

Möjliga åtgärder

- Administrativ säkerhet:
  - Styrdokument,
  - kunskapshöjande åtgärder.
- Fysisk säkerhet:
  - Tillträdeskontroll,
  - låsta arkivskåp.
- IT-säkerhet:
  - Bradväggar,
  - kryptering,
  - fler under kursens gång.

Referenser I

[Lin12] Ida Lindkvist. *Tietohaveriet – dag för dag*. Febr. 2012. URL: https://computersweden.idg.se/2.2683/1.434018/tietohaveriet---dag-for-dag.