Introduktion till MSB:s metodstöd

Daniel Bosk och Carina Bengtsson[1]

Avdelningen för informations- och kommunikationssytem (IKS),
Mittuniversitetet, Sundsvall.

msbintro.tex 2193 2015-02-10 15:38:56Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

1. MSB:s metodstöd
   - MSB
   - Metodstödet
2. Förbereda
   - Introduktion
   - Ledningens engagemang
   - Projektplanering
3. Analysera
   - Verksamhetsanalys
   - Riskanalys
4. Examinationsuppgifter

Översikt

MSB

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

Varför behöver samhället detta?

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

Tietohaveriet I

[Lin12] ger följande sammanfattning:

Fredag e.m.	Tieto 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.	Tieto 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.

Tietohaveriet 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.

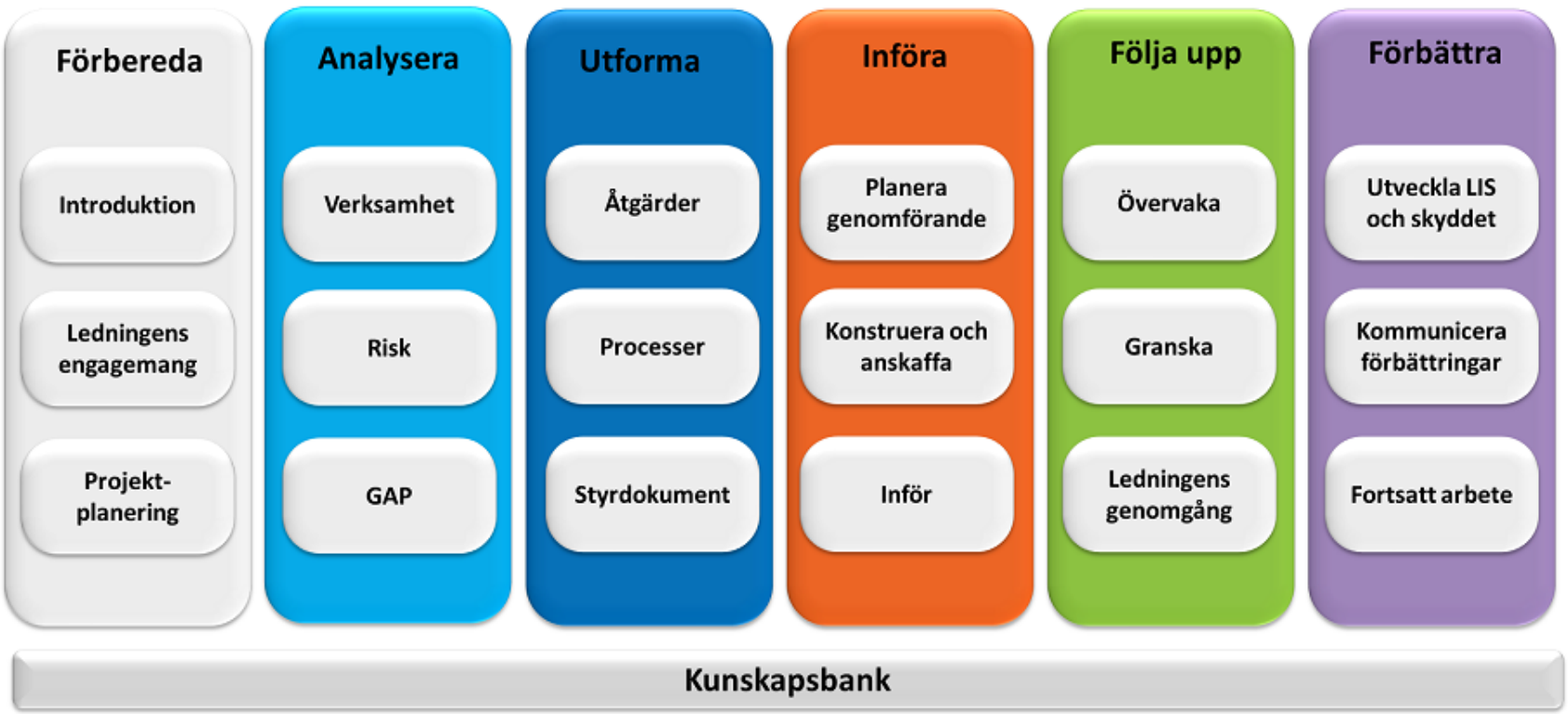
Informationssäkerhet.se

- 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 Tieto—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?

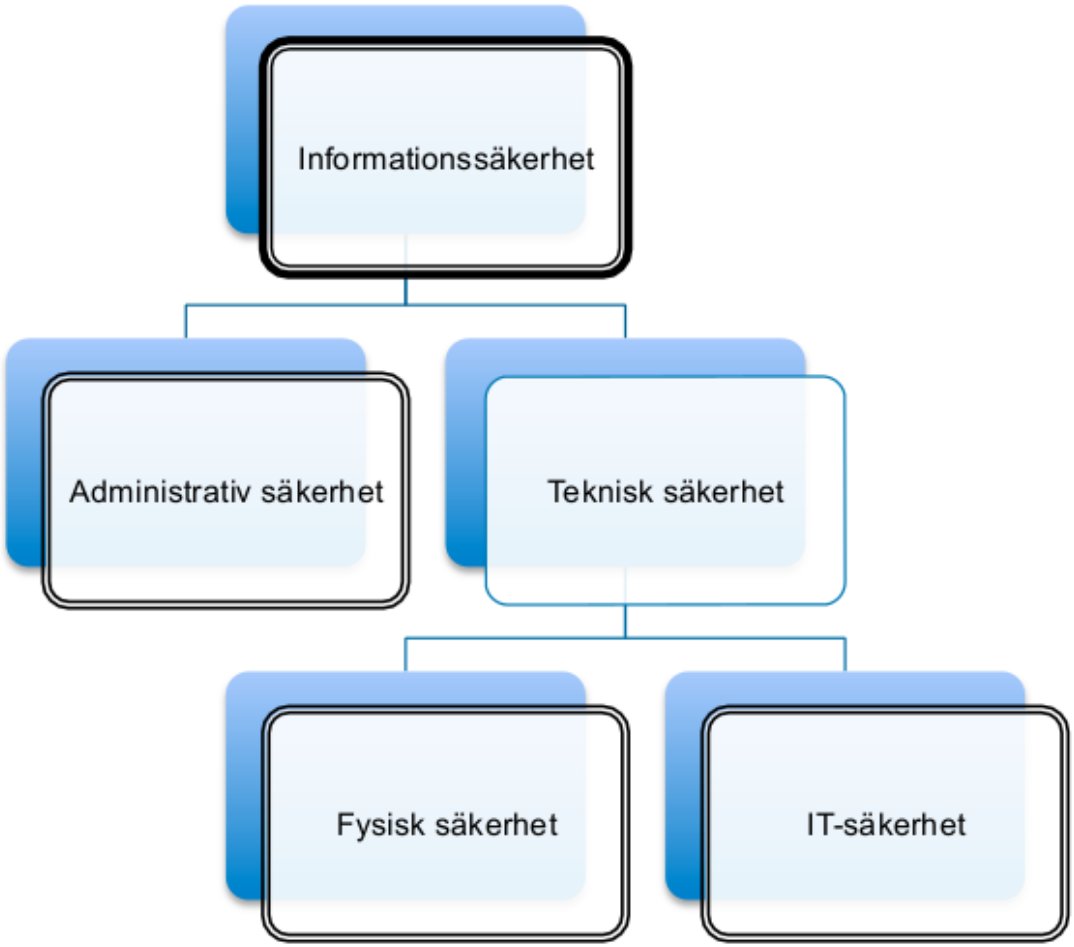
Oavvislighet Det ska inte gå att förneka en handling.

Autentisering Fastställa en entitets identitet.

Auktorisation Att ge en autentiserad entitet vissa rättigheter.

Återkommer till dessa senare i kursen.

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 Tietohaveriet;

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.

MSBFS 2009:10

- På grund av ökat elektroniskt informationsutbyte i samhället ställs nu krav på myndigheters informationssäkerhetsarbete.
- Författningen trädde i kraft 1 februari 2010.

MSBFS 2009:10

1 § Denna författning innehåller bestämmelser om myndigheternas arbete med informationssäkerhet och deras tillämpning av standarder i sådant arbete.

MSBFS 2009:10

4 § En myndighet ska i sitt arbete med att upprätthålla säkerhet i sin informationshantering tillämpa ett ledningssystem för informationssäkerhet. Det innebär att myndigheten ska

1. upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet,
2. utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet,
3. klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet,
4. utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt besl uta om åtgärder för myndighetens informationssäkerhet,
5. dokumentera granskningar och säkerh etsåtgärder av större betydelse som har vidtagits.

MSBFS 2009:10

5 § Myndighetens ledning ska löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på myndigheten.

MSBFS 2009:10

6 § En myndighets arbete enligt 4 och 5 §§ ska bedrivas i former enligt följande etablerade svenska standarder för informationssäkerhet;

- Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001:2006 fastställd 2006-01-19), och
- Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005 fastställd 2005-08-12).

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, . . .

Ledningssystem för informationssäkerhet (LIS)

- Bör integreras med övriga ledningssystemet!
- Syftar till att ordna informationssäkerhetsarbetet.
- Även hur man håller ordning: exempelvis arbetssätt, metoder.
- Styrdokument har en viktig roll i ett LIS.

Tillämpa LIS

Inte bara upprätta, utan även

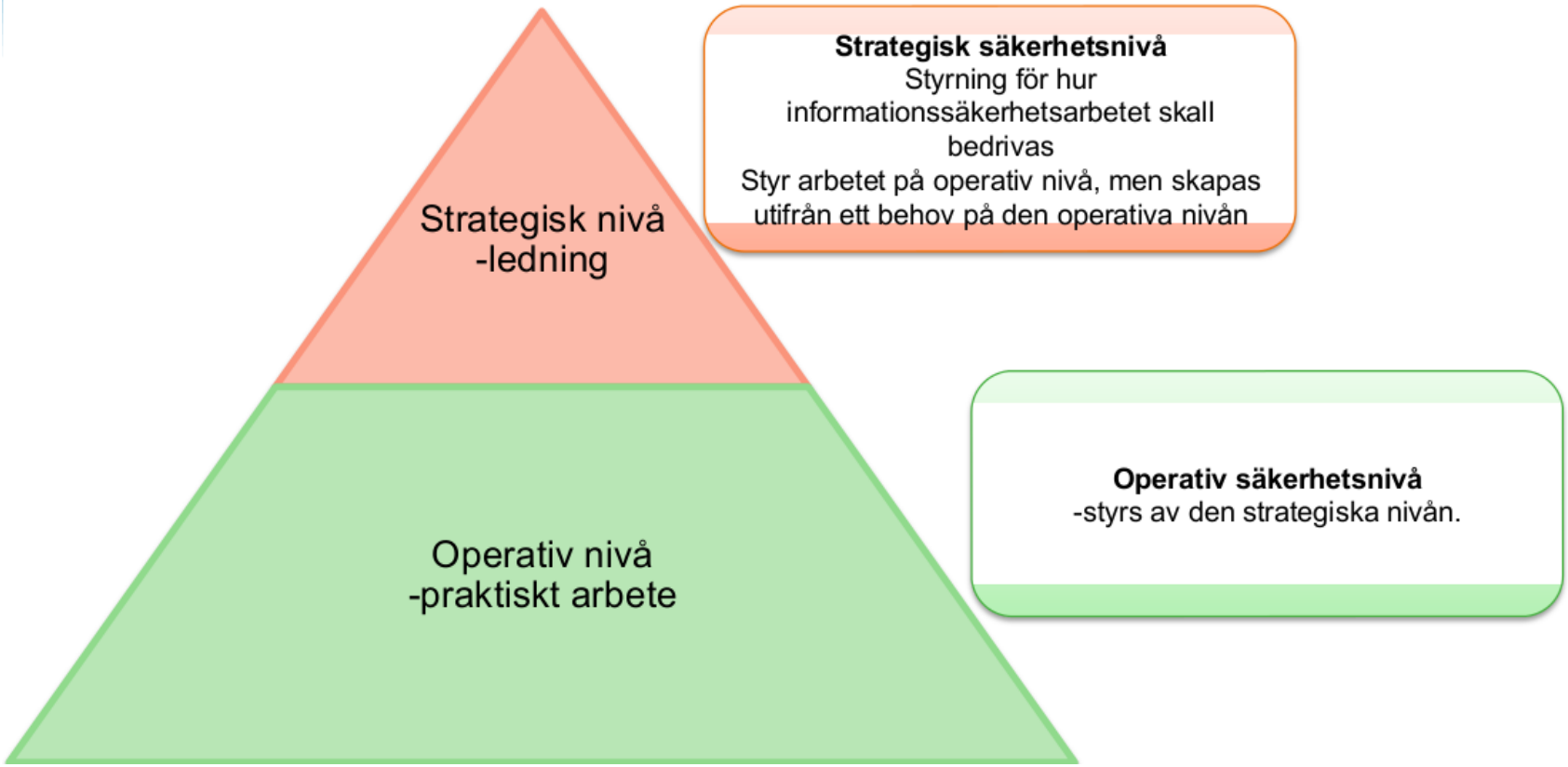
- införa,
- driva,
- övervaka,
- granska,
- underhålla och förbättra

LIS inom ramen för verksamheten och riskerna.

Styrdokument

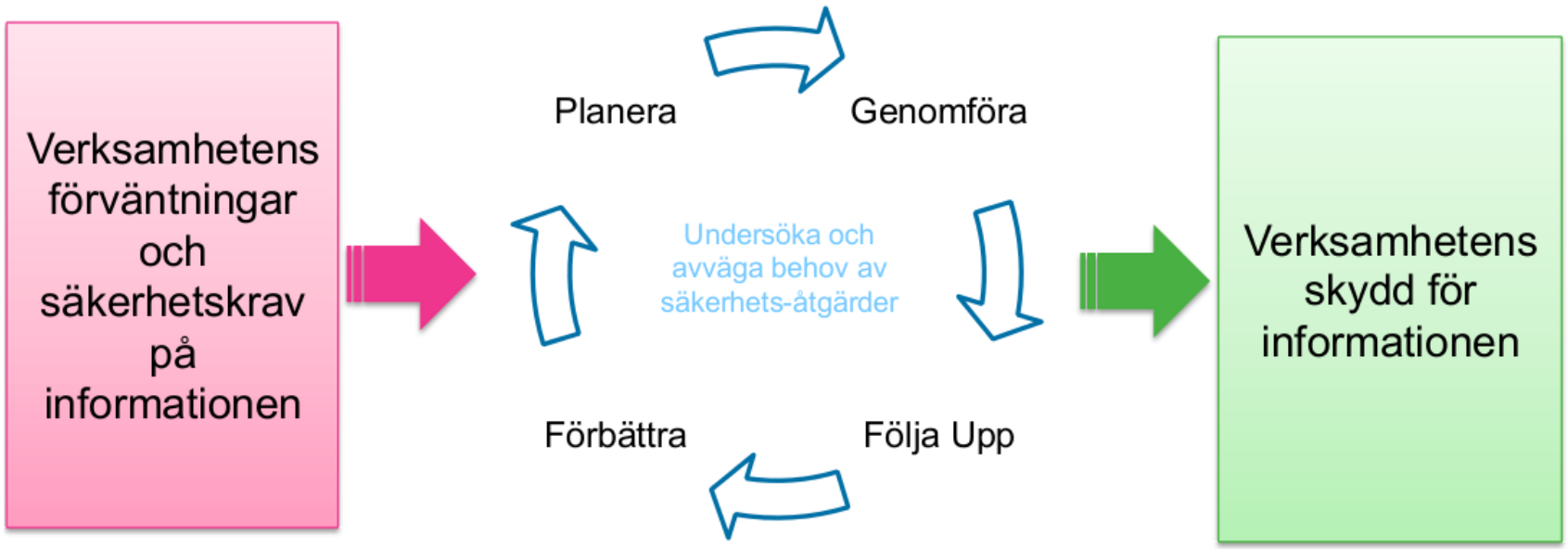
- Handlingsplaner, policyer, riktlinjer, . . .
- Policy: vad vill vi uppnå? En stor eller många små.
- I övrigt bör styrdokumenten integreras i verksamhetens nuvarande struktur.

Informationssäkerhet på olika nivåer



Figur: De olika nivåerna där informationssäkerhetsarbete kan bedrivas.

Syftet med LIS



Figur: Att omvandla krav till aktivt skydd.

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.

PDCA

Plan	Förbereda, analysera, utforma.
Do	Införa.
Check	Följa upp.
Act	Förbättra.

Därefter åter till steget analysera.

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.

ISO 27002 – vad ska göras?

Allt detta täcks av olika kapitel i ISO 27002, dessa återkommer vi till under nästa föreläsning.

Ledningens engagemang

- Hur lyckas man? Det krävs stöd från ledningen.
- Då informationssäkerhetsarbetet ska genomsyra hela organisationen måste ledningen vara engagerad.
- De som driver arbetet måste få mandat att utföra det.

Skapa engagemang

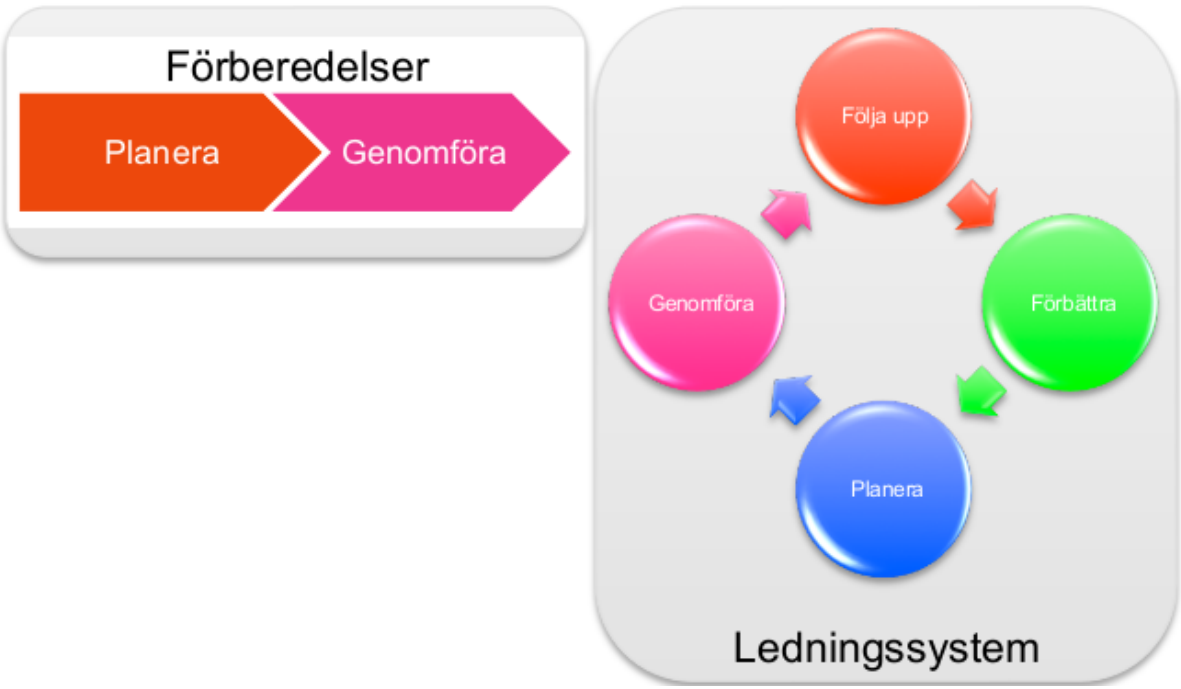
- Ledningen har det övergripande ansvaret för organisationen—detta innefattar informationssäkerheten och säkerhetsincidenter.
- Få ledningen att förstå vikten av informationssäkerhet.

Motivation

- Vilka positiva effekter följer av god informationssäkerhet?
- Vad kan det kosta att inte skydda informationen?
  - Företagshemligheter som läcker.
  - Infrastruktur som är otillgänglig under längre tid.
- Visa incidenter.
- Lagar och andra regleringar?

Projektplanering

- Metodstödet rekommenderar att ett LIS etableras i projektform . . .
- . . . för att sedan övergå till en process.



Figur: Införande och genomförande av LIS.

Projektplan

- Utgör projektets grund.
- Definierar omfattningen och gränserna för LIS.
- Ett avtal som är bra för både projektledare och ledning.
- Kan innehålla:
  - Bakgrund och behov,
  - syftet med projektet,
  - mål,
  - omfattning och avgränsning,
  - kopplingar och kontaktytor,
  - tidsplan, och
  - budget.

Projektorganisation

- Viktigt med bredd: att representera hela organisationen.
- Viktigt med rätt kompetens: projektledning och informationssäkerhet.
- Viktigt med mandat!
- Organisationen bör vara aktiv och engagerad för att inte kompetensen ska försvinna efter projektets slut.

En kort checklista

- Har ledningen fattat beslut om att arbeta för att implementera LIS?
- Har ledningen utsett någon som samordnar organisationens informationssäkerhet?
- Har ledningen sett till att det finns en strategi för att kommunicera LIS-arbetet internt?
- Har ledningen fattat beslut gällande resurser?

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.

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.

MSB:s förslag på klassificeringsmodell

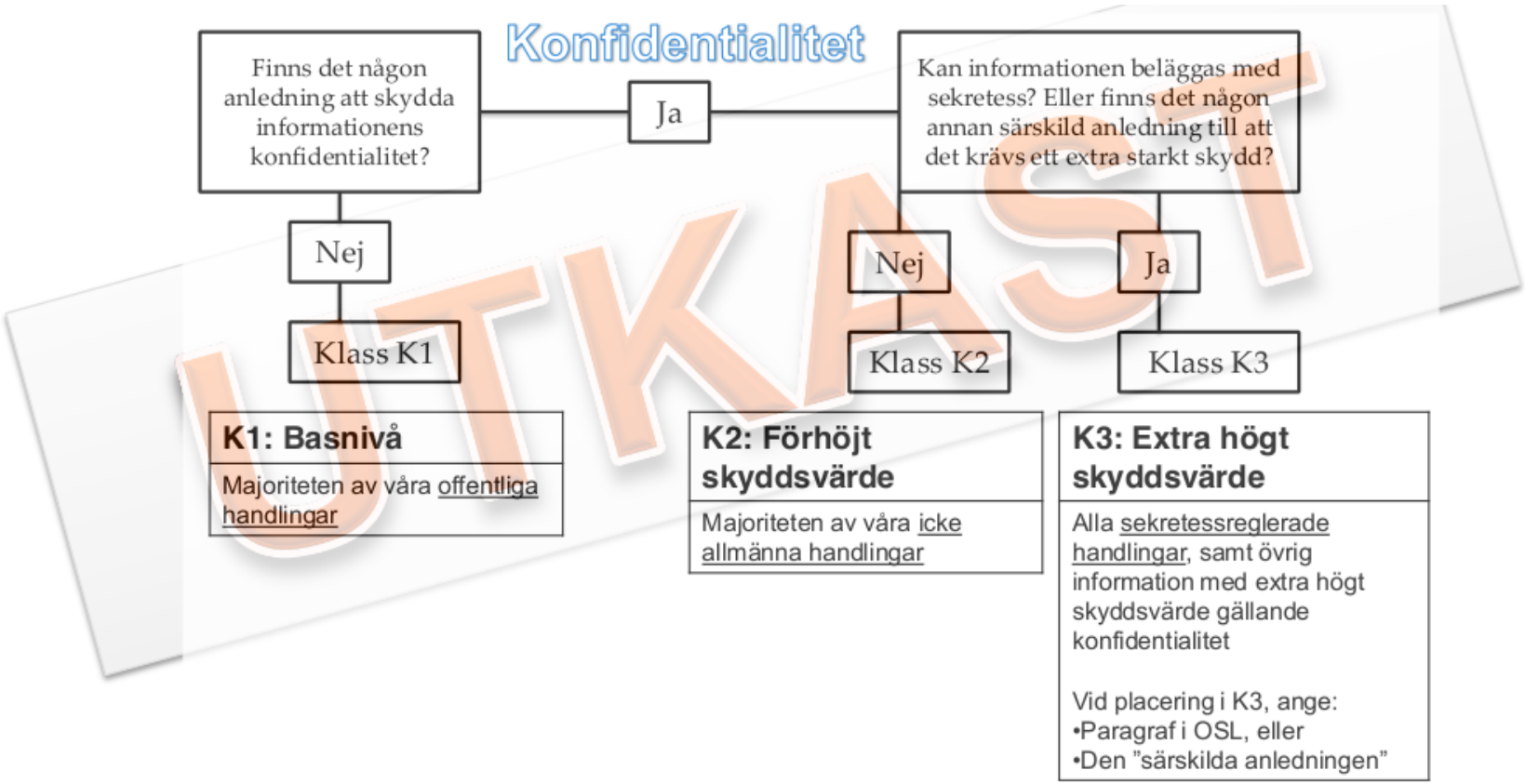
Säkerhetsaspekt / Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **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

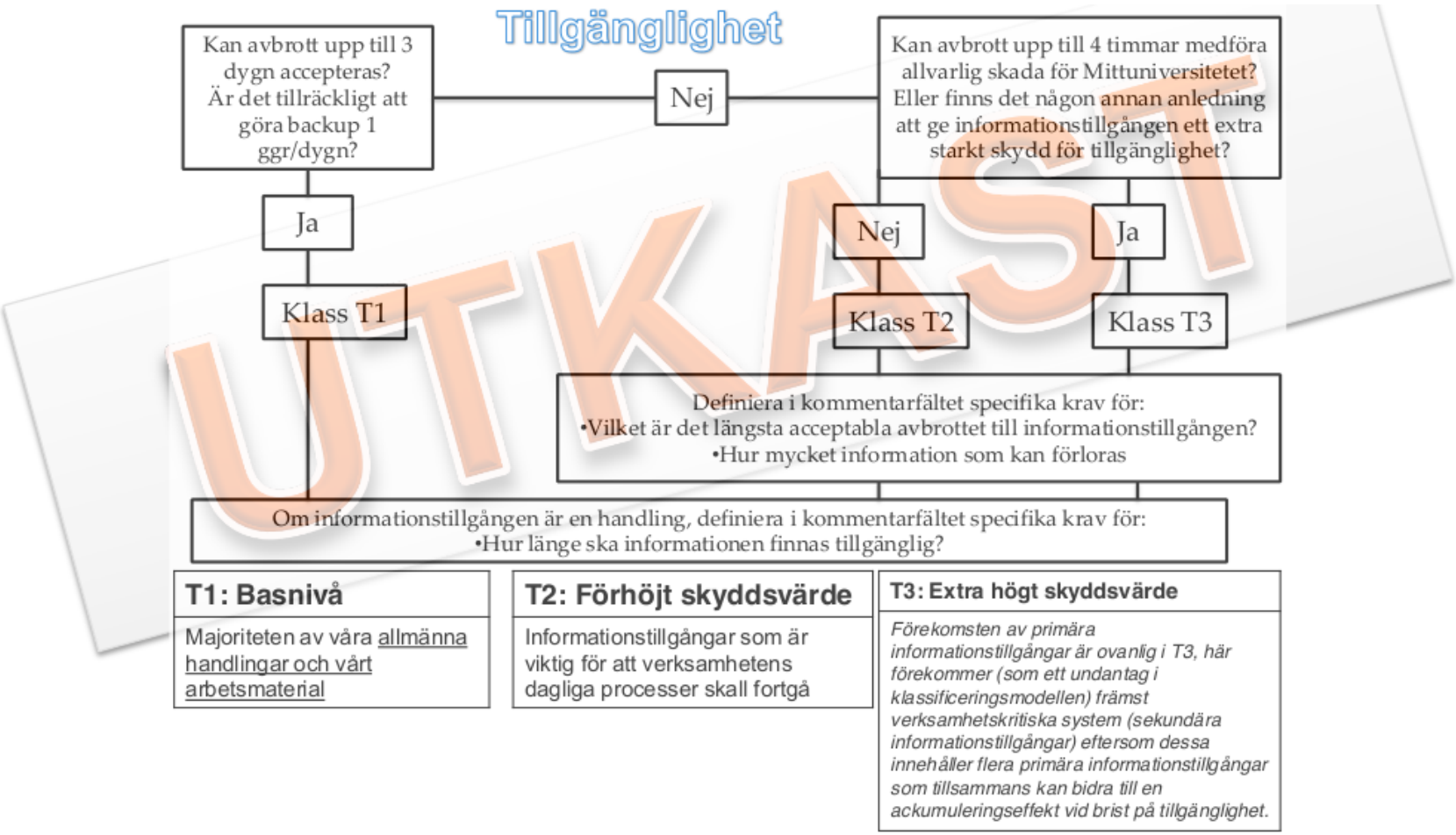
- Alla tillgångar klassificeras mot alla identifierade krav ur alla perspektiv.
- Informationsägaren klassificerar.
- Anpassa gärna modellen efter verksamheten.

Universitetets förslag på klassificeringsmodell



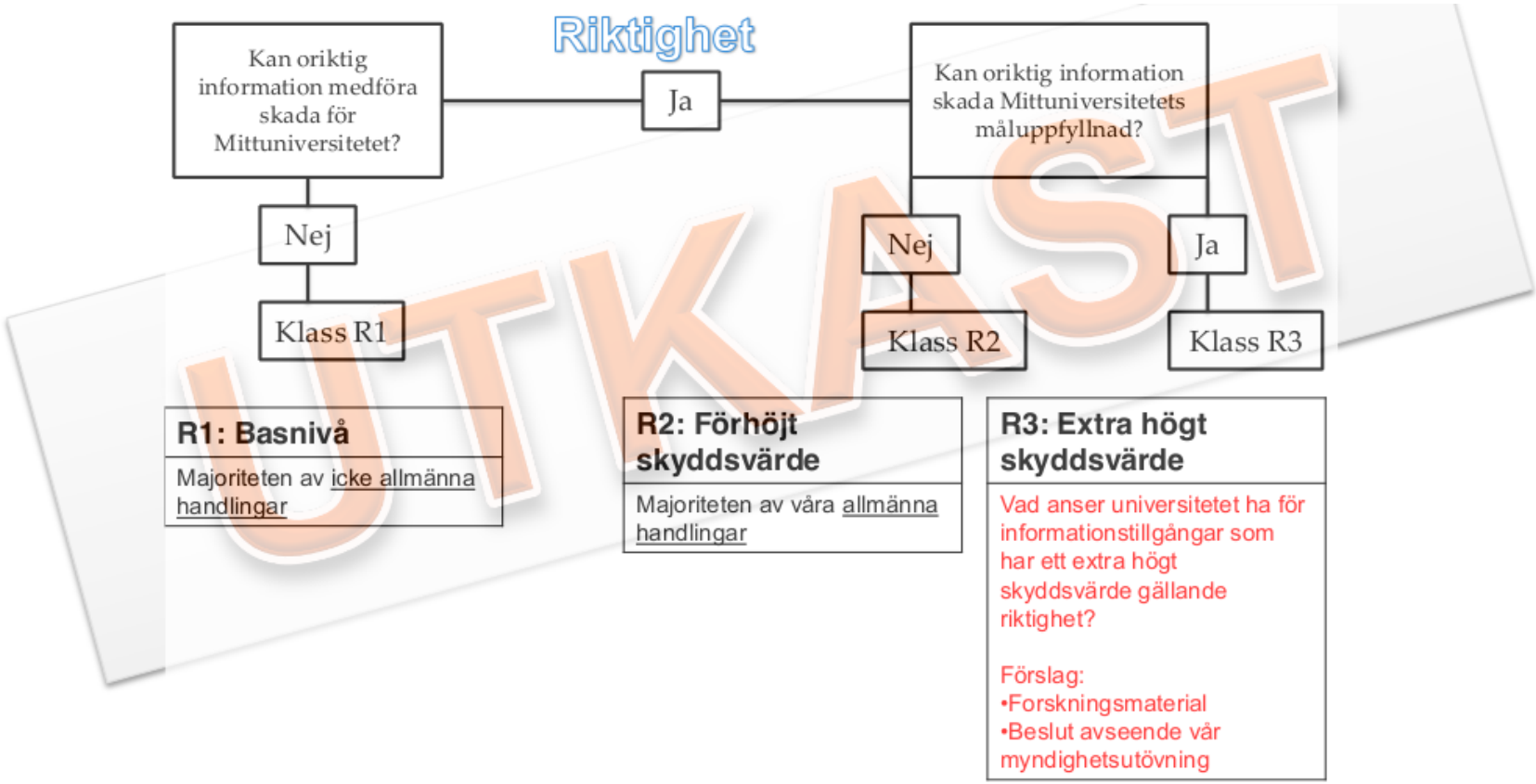
Figur: Universitetets förslag på klassificeringsmodell för konfidentialitet.

Universitetets förslag på klassificeringsmodell



Figur: Universitetets förslag på klassificeringsmodell för tillgänglighet.

Universitetets förslag på klassificeringsmodell



Figur: Universitetets förslag på klassificeringsmodell för riktighet.

Exempel på resultat från universitetet

Mittuniversitetet
MID SWEDEN UNIVERSITY

Primära informationstillgångar
(Information och data)

1a Informations-tillgång	1b Identifierade krav och förväntningar (legala, interna)	1c Säkerhets-klassificering (Värde: 1-3)	1d Sammanvägd säkerhetsklassi-ficering	Eventuella kommentarer
1. Avvikelse-rapporter	MSBFS 2009:10, OSL, AL Skyddskommittéens förväntningar, förväntan på skyndsam hantering	Konfidentialitet:2 Riktighet: 2 Tillgänglighet: 2		
2. Polis-anmälningar & beslut	OSL, AL	Konfidentialitet:1 Riktighet: 2 Tillgänglighet: 1		
3. Brandskydds-dokumentation	LSO, OSL, AL, Boverkets byggregler	Konfidentialitet:1 Riktighet: 2 Tillgänglighet: 2		Tillgängligheten bedöms ej vara en trea på grund av att dokumentationen i sig ej räddar liv i ett akut läge. Utrymningsplaner bör läsas innan det börjar brinna

Figur: Del av universitetets resultat.

Riskanalys

Måste göra avgränsningar:

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

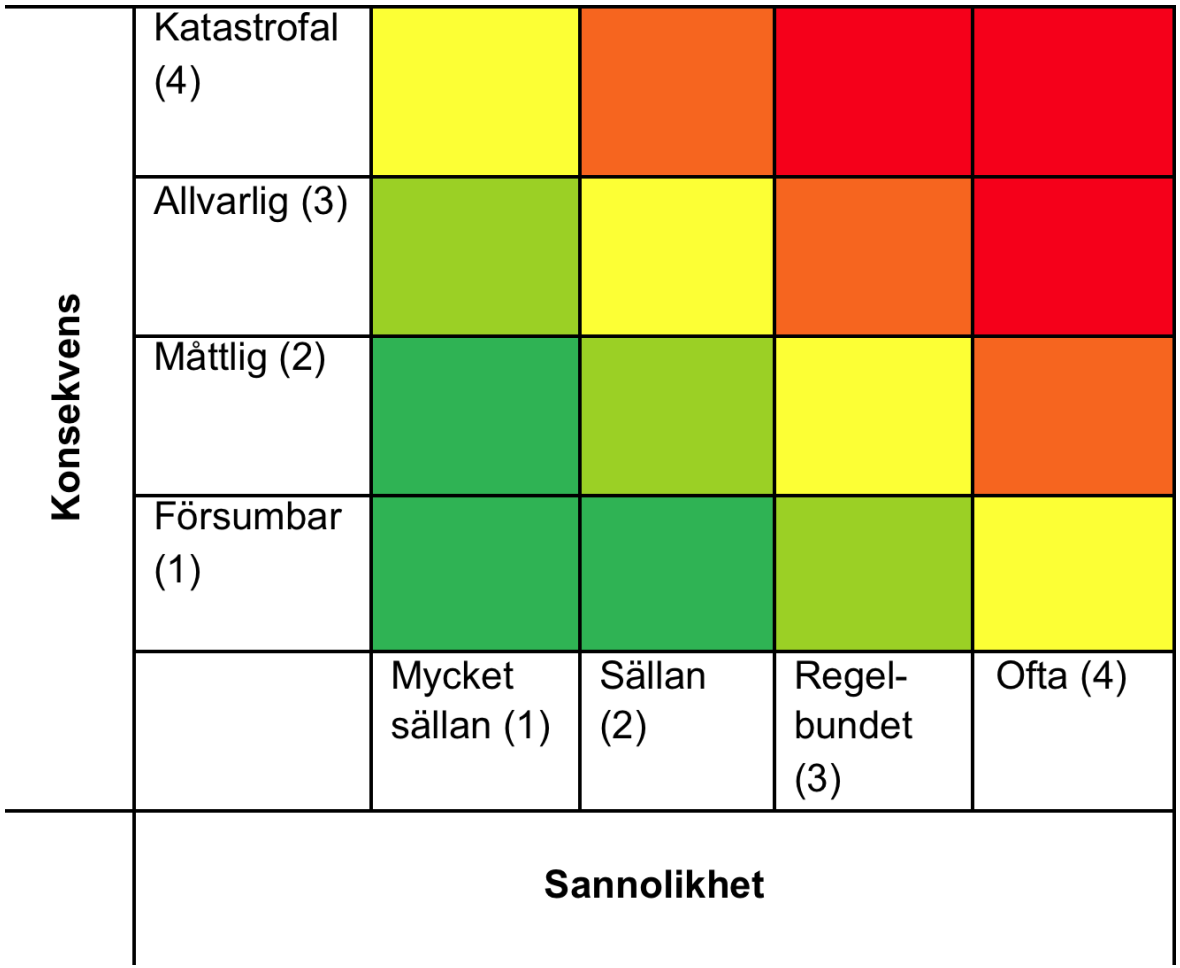
Riskanalys

- 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

- Bedöm sannolikhet och konsekvens av varje enskilt hot och placera dem i matrisen.
- Fokus för konsekvenser är konsekvenser för verksamheten.
- Ger visualiserat resultat, lättöverskådlig grund för prioritering av säkerhetsåtgärder.

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

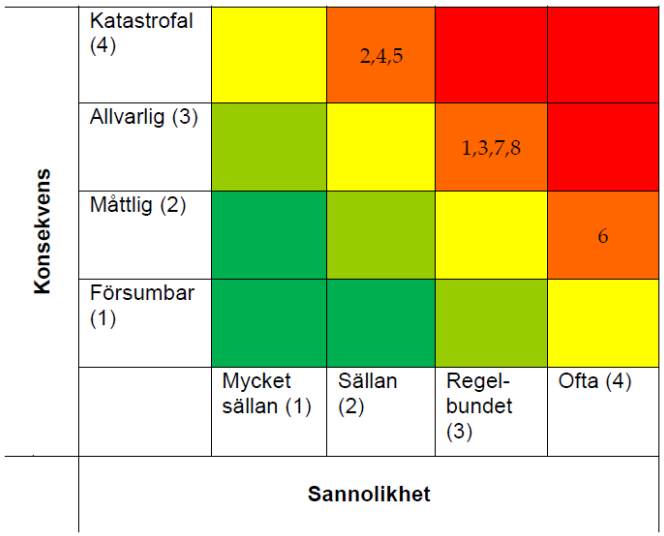
- Administrativ säkerhet:
  - Styrdokument,
  - kunskapshöjande åtgärder.
- Fysisk säkerhet:
  - Tillträdeskontroll,
  - låsta arkivskåp.
- IT-säkerhet:
  - Bradväggar,
  - kryptering,
  - fler under kursens gång.

Exempel från universitetet

Hemligt forskningsmaterial med stort affärsintresse: K3, R2, T2.

Nr:	Hot:
1.	Oavsiktlig informationsläcka från person
2.	Avsiktligt industrispionage
3.	Oavsiktlig informationsläcka från teknik
4.	Stöld av information/fysisk informationstillgång
5.	Åtkomst till backup
6.	Förlust av informationssresurs (borttappad)
7.	Stöld av informationsresurs
8.	Läckage från partner

(a) Hotbild



(b) Risker

Figur: Hotbild och bedömd risk.

Exempel från universitetet

Hot nr: 7 - Stöld av informationsresurs ☐ Acceptera risken ☐ Eliminera risken ☐ Överföra risken ☒ Behandla risken
Om annat än *Acceptera risken* är valt, lämna förslag på åtgärd/åtgärder: Kryptering. Fjärr-radering. Pin-kod. Inlog. Medvetenhet om lagring på bärbar dator (t.ex. att saker sparas i cash-minnet). Krav på att använda teminalserver. Skalskydd, eventuellt förstärkt skalskydd. Utbildning.

Figur: Åtgärder för att bemöta hotet.

Slutligen—när ska analyserna göras?

- Årligen.
- Vid förändrad verksamhet.
- Vid planering av ny verksamhet.

Översikt

Examinationsuppgifter

- M1 Ledningssystem för informationssäkerhet.
- M2 Verksamhets- och riskanalys.
- S3 Verksamhets- och riskanalys.

Referenser I

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