Administrativ säkerhet

1DV425 Nätverkssäkerhet

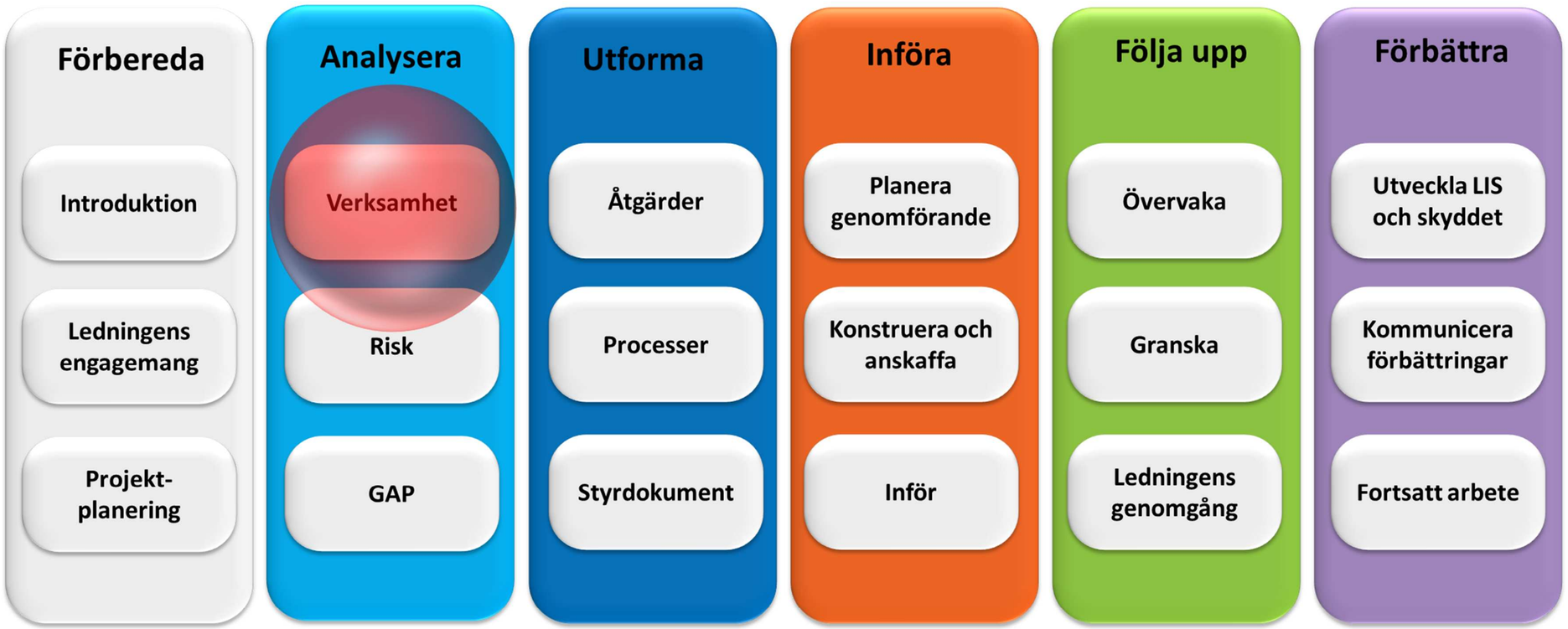
Linnéuniversitetet

Dagens Agenda

- **Informationshantering**
  - Hur vi handhar vår information
  - Varför vi bör klassificera information
- **Riskanalys**
  - Förarbete till ett säkerhetstänkande
- **Säkerhetspolicy**
  - Mål och ansvar

Linnéuniversitetet

Metodstöd



Källa:MSB, www.informationssäkerhet.se

Linnéuniversitetet

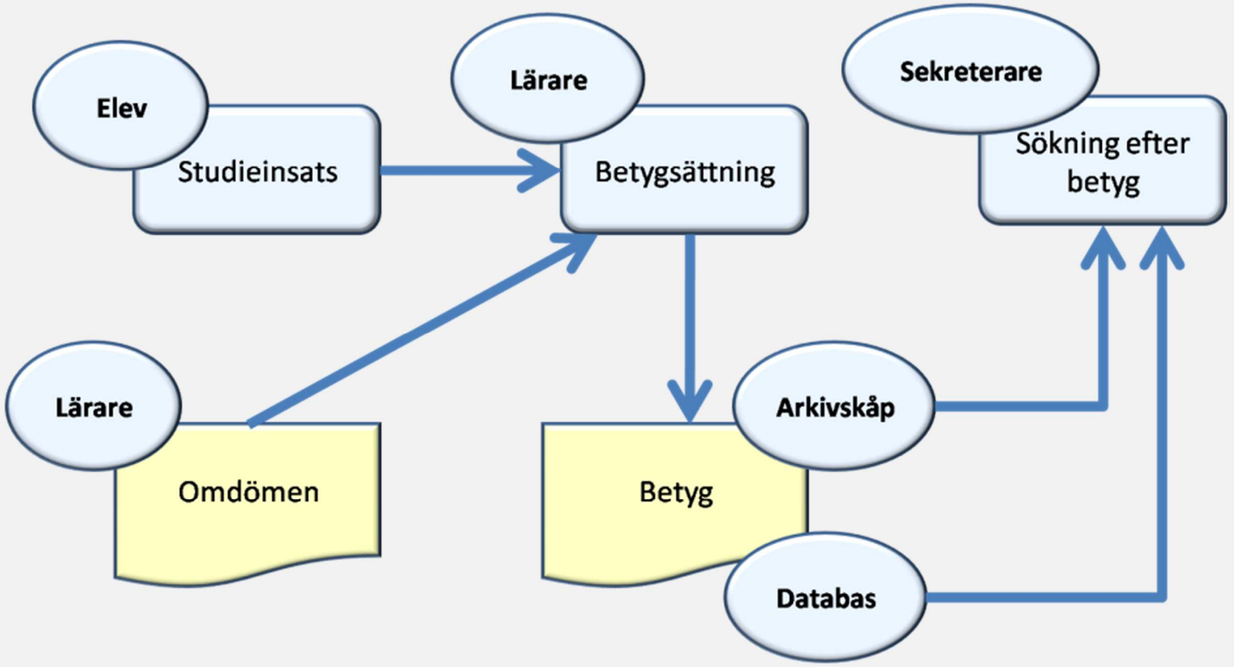
Risker & hot

- Sannolikhetskalkyler i vår vardag
- Användningen av informationsteknik och risker
  - Konkreta risker
  - Abstrakta risker
- Hjälpmedlet kan vara att finna processer

Linnéuniversitetet

Verksamhetsprocesser

Exempel på process – betygsättning



Källa: MSB, www.informationssäkerhet.se

Linnéuniversitetet

Riskbedömning - misstag

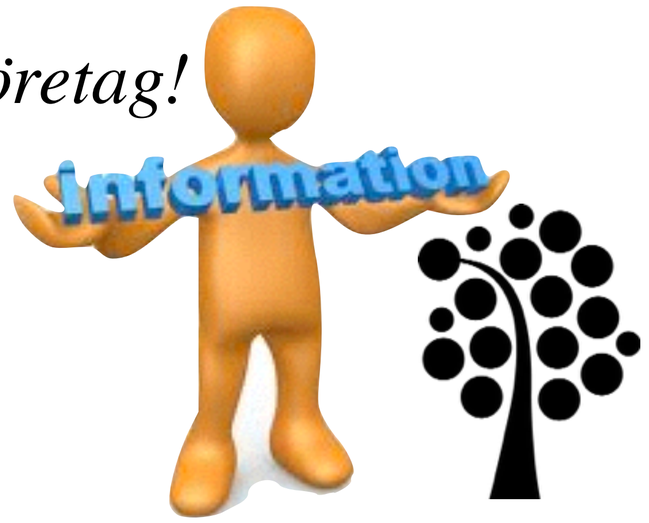
- Ett datum när bedömningen måste omprövas
- Underskattning
- Betonar risker på fel sätt
- Ibland kan det vara bättre att utbilda

Linnéuniversitetet

Riskvärdering

- Handlar alltid om någon tillgång eller resurs som vi försöker skydda
- Vad är då föremålet när vi sysslar med informationssäkerhet?

Vi kan inte genomföra en riskvärdering som gäller alla företag!



Exempel på tillgångar

- ☑ Kund och medlemsregister
- ☑ Ekonomiska data
- ☑ PM, rapporter och forskningsartiklar
- ☑ Webbplatsen
- ☑ Programkod, musik, film
- ☑ Personer
- ☑ Rykte, varumärke och förtroende

Linnéuniversitetet

Informationstillgångar

Information

Databaser
Datafiler
Avtal och överenskommelser
Systemdokumentation
Forskningsinformation
Användarmanualer
Drift- och stödrutiner
Organisationens kontinuitetsplaner
Nödrutiner
Revisionsspår
Arkiverad information

Programvarutillgångar

Tillämpningsprogram
Systemprogram
Utvecklingsverktyg
Stödprogram

Tjänster

Data- och kommunikationstjänster
Försörjningssystem (värme etc.)
Ljus, elkraft och luftkonditionering

Immateriella

Rykte och profil

Medarbetare

Kvalifikationer
Talanger
Erfarenhet

Fysiska tillgångar

Datorutrustning
Kommunikationsutrustning
Flyttbara datamedia och annan utrustning

Källa: MSB, www.informationssäkerhet.se

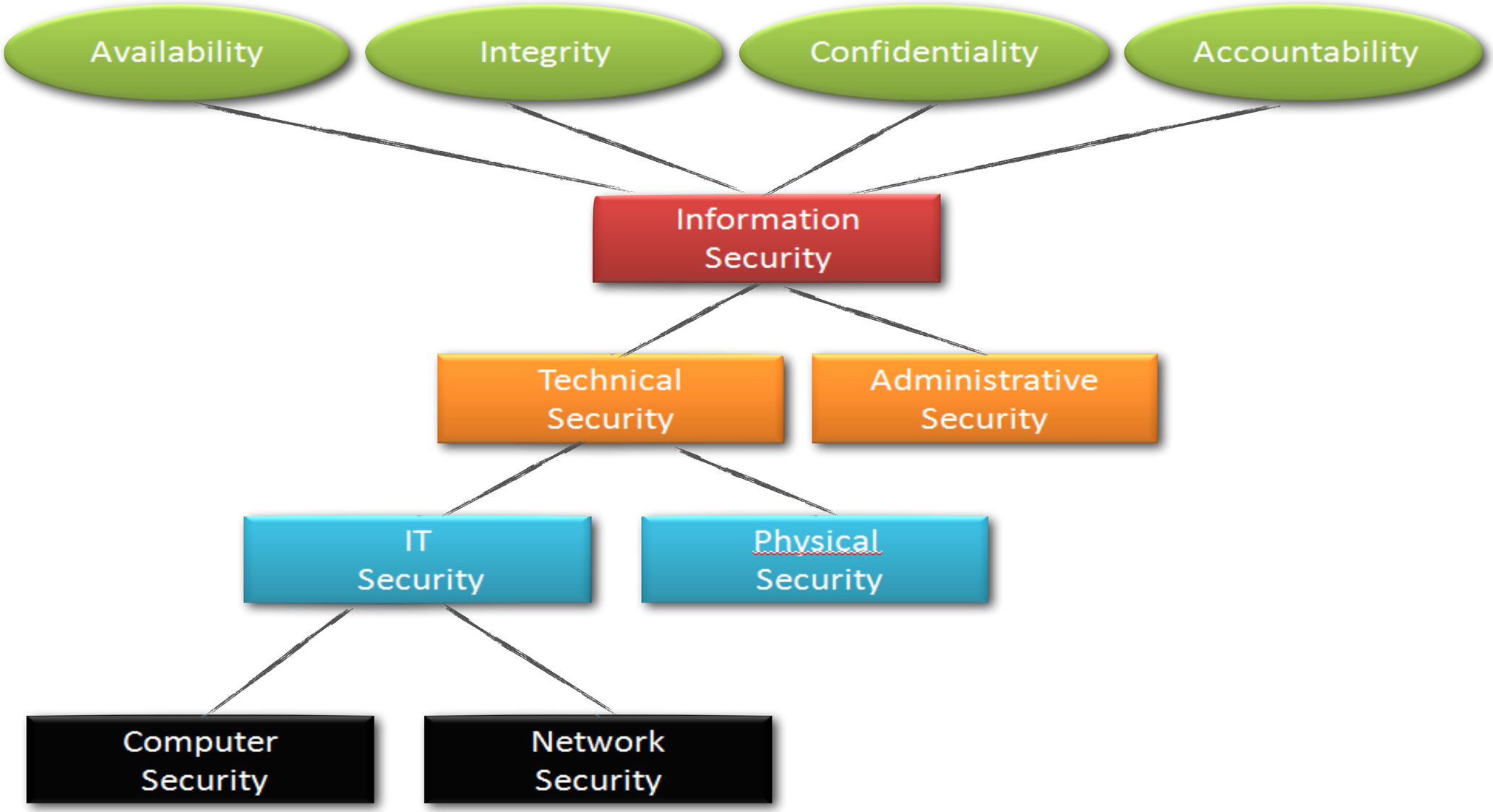
Linnéuniversitetet

Informationssäkerhet

Innebär att man genom olika åtgärder minskar sannolikheten för oönskade händelser eller att man mildrar konsekvenserna av dem

- Vad betyder säkerhet?
- Vad betyder informationssäkerhet?
  - Informationen ska vara tillgänglig, spårbar och riktig så att företaget, dess medarbetare, kunder samt leverantörer och andra intressenter ska kunna vara säkra

Linnéuniversitetet



Linnéuniversitetet

Ledningssystem

- Ledningssystem för informationssäkerhet
- SS-ISO/IEC 27001, SS-ISO/IEC 27002
- Kravstandard
- Modell för ledningssystem för informationssäkerhet
  - Upprätta policy, mål, processer och rutiner som är relevanta för riskhantering och förbättring av informationssäkerhet.
    - Införa och driva policy, åtgärder och rutiner
    - Följa upp, övervaka och granska
    - Underhålla och ständigt förbättra

Linnéuniversitetet

SS-ISO/IEC 27002

- Riktlinjer för styrning av informationssäkerhet
- Standarden anger riktlinjer och allmänna principer för:
  - initiera
  - införa
  - bibehålla
  - förbättra styrningen

Linnéuniversitetet

Organisation och säkerhet

- En organisations sammantagna säkerhet skapas genom en kombination av:
  - Tekniska
  - Administrativa skyddsåtgärder

- Informationssäkerhet som begrepp omfattar **skydd av information** både när den hanteras **manuellt** av människor och när den behandlas **med hjälp av IT**

Linnéuniversitetet

Hur?

- **Vad ska man göra?**
  - Upprätta informationssäkerhetspolicy och andra styrande dokument
  - Organisation, roller och ansvarsförhållanden
  - Personalens medverkan
  - Risk- och sårbarhetsanalyser
  - Informationsklassificering

HUR?

- **Skyddsåtgärder**
  - Fysiskt skydd
  - Skydd av drift och datakommunikation
  - Åtkomst- och behörighetsstyrning
  - Systemutveckling, systemanskaffning och systemavveckling
  - Kontinuitetsplanering
  - Incidentrapportering och incidenthantering
  - Granskning och uppföljning

Informationsklassning

Linnéuniversitetet

Klassning

Informationsklassning

- Kategoriserar information efter hur känslig eller hemlig den är

Klassningsmodell

- Vi vill eftersträva att använda samma klassningsmodell för hela organisationen
- All information behandlas på samma sätt vart den än befinner sig
- Samma utbildning över hela organisationen.
- Modellen testas på samtliga avdelningar/verksamheter inom organisationen

Linnéuniversitetet

Klassning

Olika typer av informationsklasser

- Information avsedd för internt bruk.

  Interna telefonlistor, prislistor, framtida planer och motsvarande.
- Företagshemlig information

  Avtal, *produktutveckling*, *brister i en verksamhet*.
- Kvalificerat företagshemlig information

  Anbud, *krislägen*, *företagsköp*, *finansiell information*
- Öppen information

Linnéuniversitetet

Krav

- **Legala krav:** avtal, lagar och förordningar
- **Interna krav:** krav från verksamheten för att uppnå uppsatta mål

Interna krav

- Aspekter
  - Nyttan i för hållande till målen
  - Konsekvens vid förlust av konfidentialitet
  - Konsekvens vid bortfall av riktighet
  - Konsekvens vid bortfall av tillgänglighet

Riskanalys

Linnéuniversitetet

Olika typer

- Quantitative Risk Analysis
- Qualitative Risk Analysis

Linnéuniversitetet

Riskanalys

- Grund för säkerhetsarbetet
  - Analys av risker
  - Bra metoder
  - Realisera resultaten
  - Riskanalysarbetet är omfattande
- Risker
  - Hotet från ”attackerarna”
  - Översvämmande flod

Linnéuniversitetet

Viktiga begrepp

- **Hot**

  Alla oönskade händelser eller situationer som kan störa verksamheten

- **Risk**

  Sannolikheten för att en störning som medför skada eller förlust ska inträffa

  (risken = sannolikheten x konsekvensen)

- **Brist**

  En eller flera svagheter i exempelvis verksamheten, dess rutiner, programvaror eller utrustning

Viktiga begrepp

- **Sårbarhet**

  Risken för oförutsedda och förutsebara händelser som medför att verksamheten skadas eller drabbas av oönskade konsekvenser

- **Säkerhet**

  Innebär att man genom olika åtgärder minskar sannolikheten för oönskade händelser eller att man mildrar konsekvenserna av dem

Riskanalys

Riskanalys

- Definiera risker och hot
- Hittar brister och sårbarheter i organisationen
- Företagshemlighet
- Aktuella säkerhetsnivån
- Hur hög säkerhetsnivå bör vi ha.
- Grund till handlingsplaner och motsvarande
- Omfattningen av en riskanalys varierar

Linnéuniversitetet

Riskanalys

Tidsåtgång

- Drar ut på tiden
- Maximalt ett par dagar
- Minimera risken för ändringar
- Minimera störmoment
- Snabbt ut i organisationen

Tid är pengar!

Linnéuniversitetet

Riskanalys

Genomförande

- Förberedelser
  - Rätt personal
    - Konsulter?
    - Egna anställda i företaget?
  - Avgränsa

Linnéuniversitetet

Genomförande

Genomförande

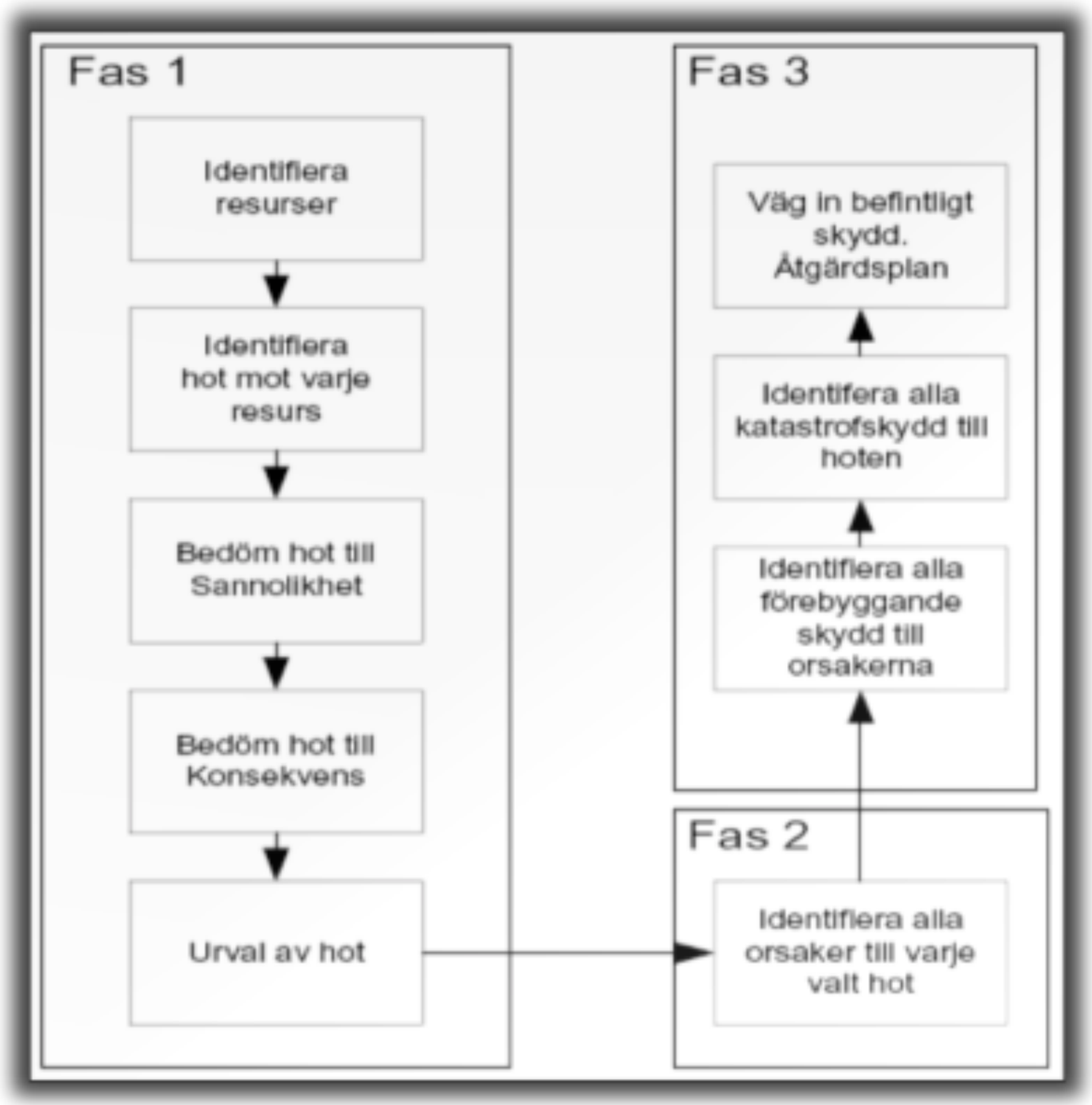
- Analyser
- Bedömning av risker
- Acceptera en del risker

Frågeställningar

- Vilka resurser måste vi skydda?
- Vem eller vad behöver de skyddas mot?
- Hur stor blir kostnaden vid en eventuell förlust?
- Hur stor är kostnaden för att skydda resurserna?
- Hur stor är sannolikheten för en förlust?
- Det som skyddas måste vara i rimlig (pris)nivå med skyddet i sig själv

Linnéuniversitetet

Process



Linnéuniversitetet

Identifiering av resurser

R-nr	Resurs	H-nr	Hot
R1	Personal	H1	Våld eller hot om våld
		H2	Olycka
R2	Datorer	H3	Obehörig tillskansar sig konfidentiell information
		H4	Stöld
R3	Ekonomisystem	H5	Inte tillgängligt
		H6	Falska utbetalningar
		H7	Manipulation av informationen
R4	Nätverk	H8	Inte tillgängligt
		H9	Avlyssning
R5	Personaladministrativt system	H10	Inte tillgängligt
		H11	Obehörig får del av konfidentiell information
R6	Betalningsrutiner	H12	Inte tillgängligt
		H13	Manipulation av information

Linnéuniversitetet

Sannolikhet & konsekvens

Sannolikhet (S)	Konsekvens (K)
Nivå 0 = Osannolik, inträffar om 30 år.	**Nivå 0** = Betydelselös.
Nivå 3 = Mindre sannolik, inträffar om 5 år.	**Nivå 3** = Låg, kan påverka trovärdighet, viss ekonomisk påverkan, gränslandet för vad som är lagligt (ej gråzon), lite påverkan på människor (liv och hälsa).
Nivå 5 = Möjlig, kan inträffa under året.	**Nivå 5** = Hög, är avgörande för trovärdighet, har stor ekonomisk påverkan, gråzonen för vad som är lagligt, stor påverkan på människor (liv och hälsa, flertal skadade).
Nivå 8 = Sannolik, inträffar flera gånger per år.	**Nivå 8** = Mycket hög, kan hota företagets trovärdighet, mycket stor ekonomisk påverkan, är olagligt, mycket stor påverkan på människor (liv och hälsa, flertal döda eller svårt skadade).

Linnéuniversitetet

Sannolikhet- och konsekvensbedömning

R-nr	Resurs	H-nr	Hot	S	K
R1	Personal	H1	Våld eller hot om våld	7	8
		H2	Olycka	4	8
R2	Datorer	H3	Obehörig tillskansar sig konfidentiell information	3	9
		H4	Stöld	6	3
R3	Ekonomisystem	H5	Inte tillgängligt	6	7
		H6	Falska utbetalningar	4	7
		H7	Manipulation av informationen	3	8
R4	Nätverk	H8	Inte tillgängligt	1	4
		H9	Avlyssning	2	4
R5	Personaladmini-strativt system	H10	Inte tillgängligt	1	4
		H11	Obehörig får del av konfidentiell information	3	3
R6	Betalningsrutiner	H12	Inte tillgängligt	1	4
		H13	Manipulation av information	1	4

Linnéuniversitetet

Hittar orsaker

R-nr	Resurs	H-nr	Hot	S	K	Orsak
R1	Personal	H1	Våld eller hot om våld	7	8	Försöksdjurs-verksamhet
						Utsläpp av gift i närmiljö
						Industrispionage
		H2	Olycka	4	8	Trafikolycka – säljpersonal
						Otillräckliga arbetarskydd
R2	Datorer	H3	Obehörig tillskansar sig konfidentiell information	3	9	Lättillgänglig dator (ej fysiskt skyddad)
						Dator lämnad oövervakad och inloggad
						Fientligt program installerat som kopierar ut information
		H4	Stöld	6	3	Bärbar dator förvaras i bil

Linnéuniversitetet

Skydd mot hot

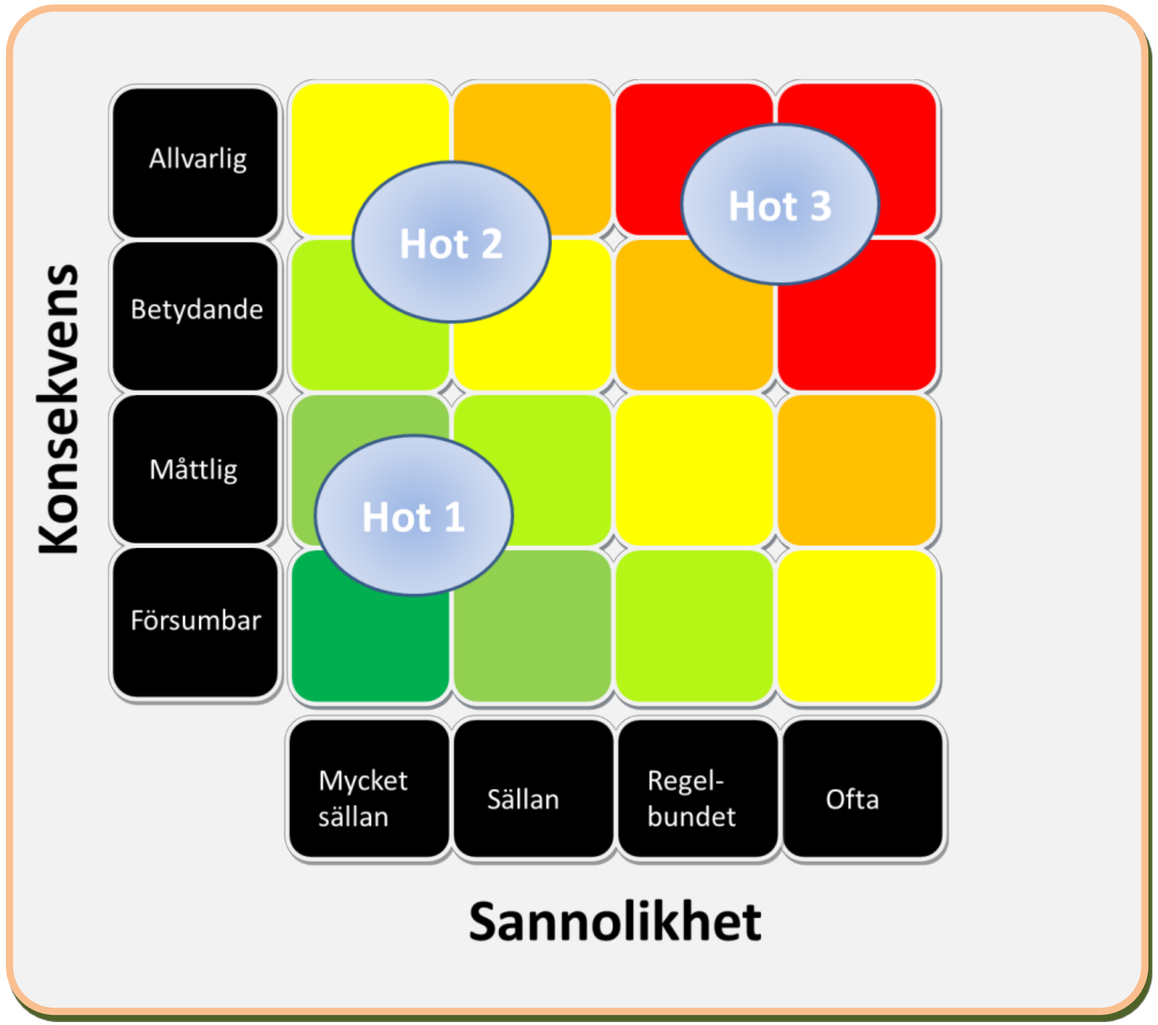
Nr	Resurs	H-nr	Hot	S	K	Orsak	Förebyggande skydd (mot orsak)	Katastrofskydd (mot hot)
							bilen	
						Datorn står lättillgänglig	Flytta datorn till en plats som inte är lättillgänglig	
							Lås fast datorn	
						Industrispionage	Kryptera informationen	
							Spara ingen information på pc	
R3	Ekonomisystem	H5	Inte tillgängligt	6	7	Nätverks-komponent har gått sönder	Reservutrustning för nätverks-komponent som kan gå sönder	Manuella rutiner
						Strömlöst	Reservkraft	Kontinuitetsplan
						Systemet fungerar inte	Regelbundet underhåll	

Linnéuniversitetet

Beslut

Sannolikhet	Konsekvens	Risknivå
1= Mycket låg	1= Mycket liten	1-4 = Kan accepteras
2= Låg	2= Liten	5-14= Bör åtgärdas
3= Medelstor	3= Medelstor	15-25= Åtgärdas snarast
4= Stor	4= Stor	
5= Mycket stor	5= Mycket stor	

Beslut



Källa: MSB, www.informationssakerhet.se

Linnéuniversitetet

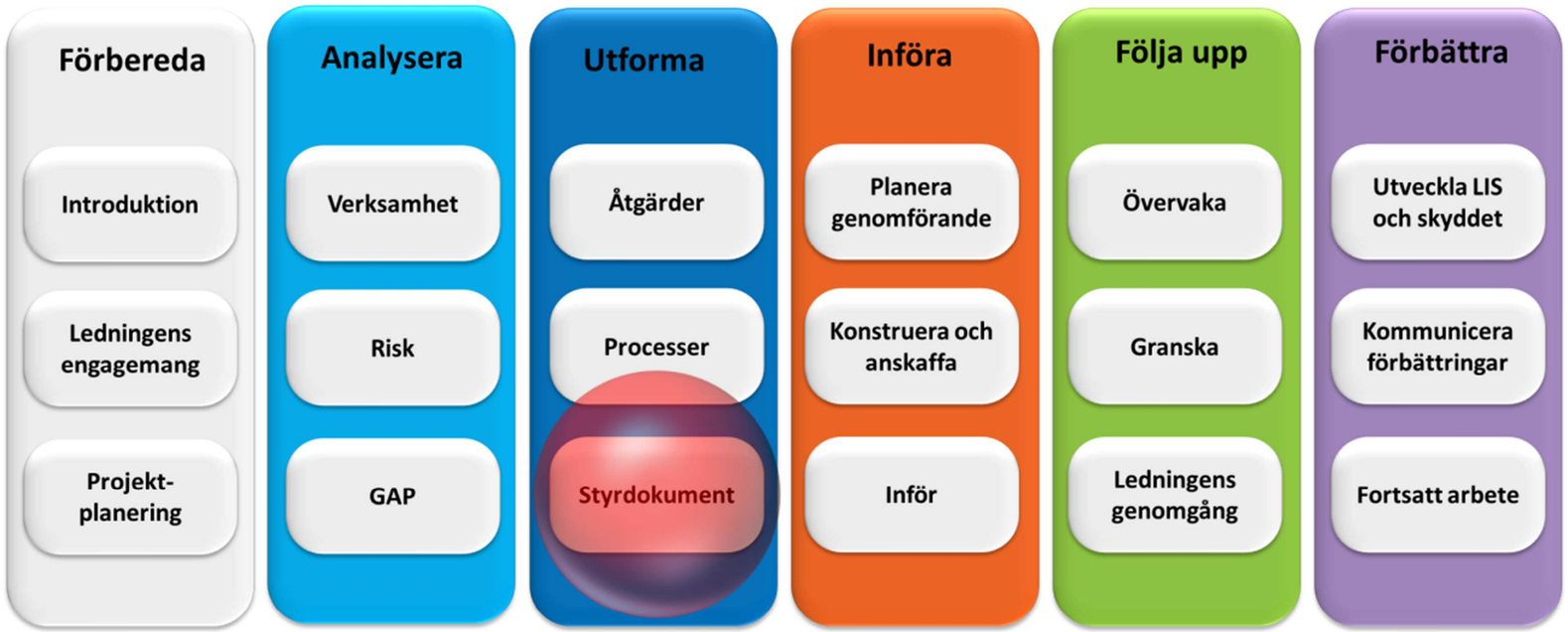
Genomförande

När ska vi göra en riskanalys?

- Vid utveckling och anpassning
- I organisationer med system som är av stor betydelse
- Vid verksamhetsförändringar
- Vid ändrad lagstiftning

Linnéuniversitetet

Styrdokument



Källa: MSB, www.informationssäkerhet.se

Styrdokument

- Policy, interna förskrifter, riktlinjer osv.
- Styrdokumenten kan ha olika benämningar
- Dock viktigt att de följer en given hierarki

Styrdokumentshierarki

Policyer	Ledningens övergripande viljeinriktning Säkerhetspolicy
Interna föreskrifter	Bindande regler, så kallade ”ska-regler”
Riktlinjer	Om det inte behövs bindande regler Tillåter alternativa handlingssätt
Vägledningar	För att kunna följa föreskrifterna och riktlinjerna på rätt sätt eventuella regler, praxis, bra arbetssätt
Rutiner	Anger hur arbetet ska bedrivas på detaljnivå säkerhetskopior, övervakning, händelseloggar

Linnéuniversitetet

Styrdokument

- Styrdokumenten bör inte nämna teknik
- ...särskilt inte dokumenten högt upp i hierarkin
- Fokusera istället på vilket skydd man vill uppnå
- Gäller inte rutinbeskrivningar eller instruktioner

Linnéuniversitetet

Säkerhetspolicy

Säkerhetspolicyn bör innehålla:

- Ledningens viljeinriktning (varför?)
- Kort beskrivning av hur viljeinriktningen ska uppnås
- en kort beskrivning av ansvarsförhållandena
- en förklaring av viktiga begrepp
- en redogörelse för vem som ansvarar för policyn samt hur den ses över och revideras

Linnéuniversitetet

Säkerhetspolicy

- Identifiera befintliga dokument
- Uppdatera
- Många säkerhetsåtgärder kräver ändringar i flera dokument
- Upphäv regler som inte gäller
- Arbeta strukturerat
- Spårbarhet i arbetet är viktigt!

Säkerhetspolicy

Skrivtips

- Tänk igenom innan...
- Styreffekt (”ska-regler”, ”bör-regler” eller praxis)
- Börja med att motivera säkerhetsåtgärden
- Processen som får/krävs
- Identifiera målgrupp (för vem skriver vi?)

Linnéuniversitetet

Säkerhetspolicy

Goda råd för att skriva tydliga styrdokument

- Skriv enkelt och använd inga komplicerade termer
- Använd konkreta exempel
- Använd gärna bilder

Linnéuniversitetet

Seminarium

- Läs instruktionerna **noga** på kurshemsidan
- Förberedelseanteckningar
- Case

Linnéuniversitetet

Det var allt för idag!