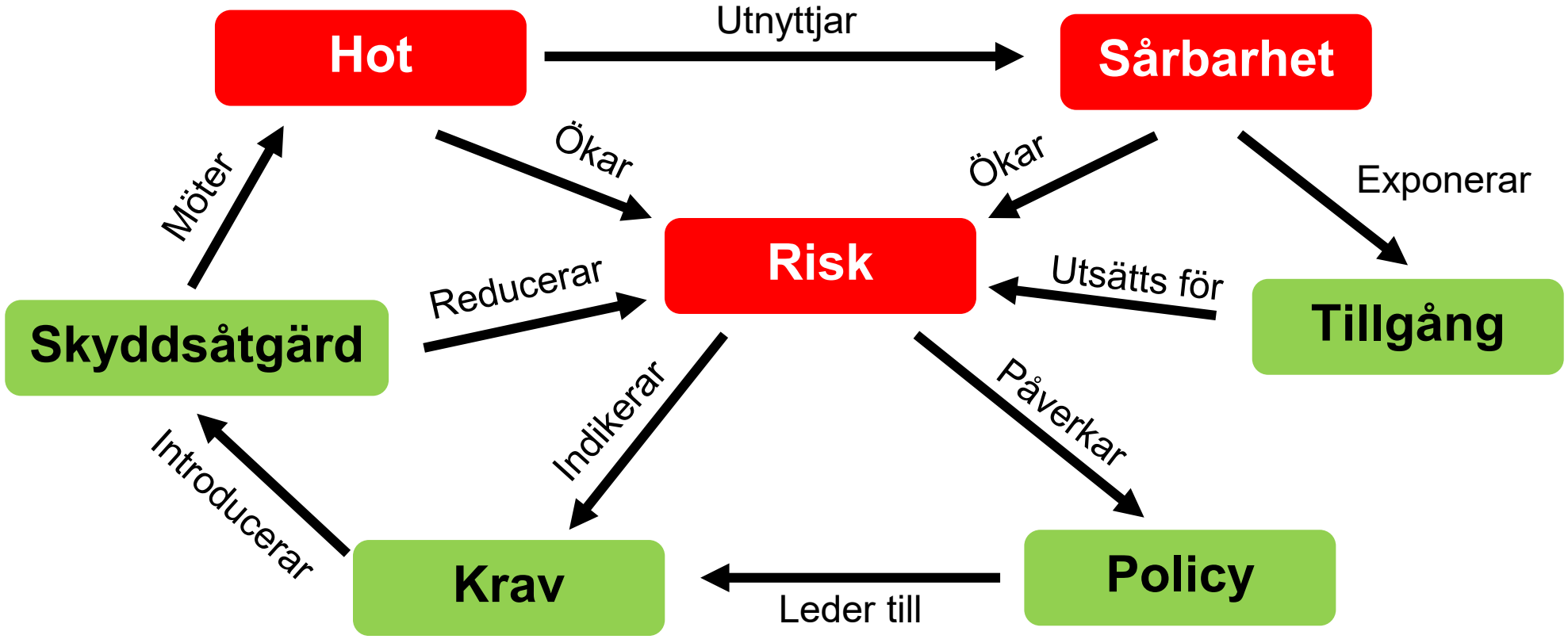
Riskanalys

Vad är en riskanalys?

- Riskanalysen besvarar tre frågor:
  - Vilka sårbarheter har vi?
  - Vad är sannolikheten för en incident?
  - Vad blir konsekvenserna?
- Krav i ISO-standarden SS-EN ISO/IEC 27001:
  - Risker analyseras
  - Riskanalysen ligger till grund för säkerhetsåtgärder

Hur hänger allt ihop?



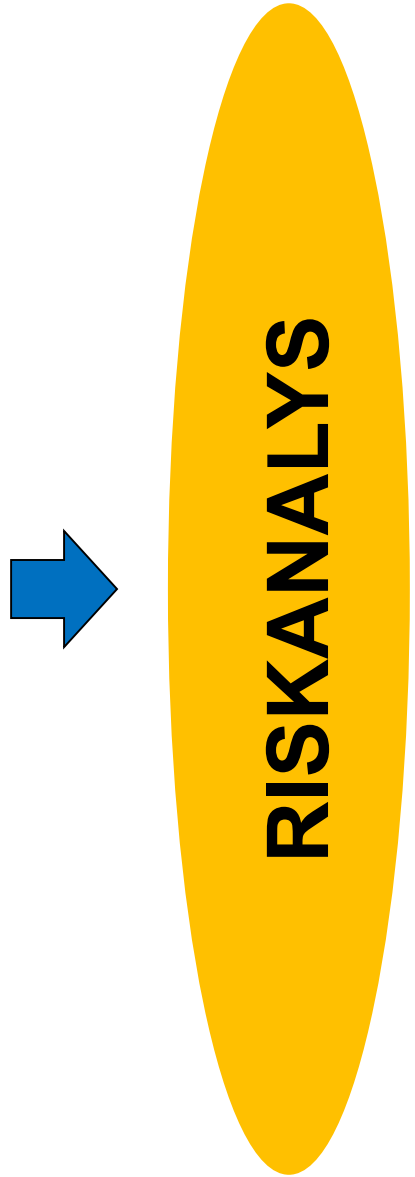
Omvärldsanalys och verksamhetsanalys

Omvärldsanalys

- **Politiska läget**
- **Rättsliga faktorer**, lagar, förordningar och föreskrifter
- Relationer med **externa intressenter**, deras mål och förväntningar – Media, Kunder
- **Ägarförhållanden –** Aktieägare, Moderbolag, Kommunen, Staten
- **Konkurrenter**
- **Avtalsbundna relationer och åtaganden -** kunder, leverantörer
- **Hotbild**

Verksamhetsanalys

- **Organisationen**
- **Ansvariga -** processansvarig, objektsansvarig, systemägare, Informationsägare
- **Interna intressenter:** Medarbetare, konsulter, beslutsfattare, avdelningar och enheter
- **Tillgångar:** Information, tjänster
- **Geografiskt läge**
- **Informationssäkerhet:** hur är den hanterad/organiserad



Interna förutsättningar för informationssäkerhet

- Visioner, **mål**, värderingar och organisationens kultur
- **Organisation** för informationssäkerhet
- Riktlinjer, **processer** och arbetsmetodik
- Rätt **resurser**: kapital, tid, personal
- **Infrastruktur:** datalagring, informationssystem, nätverk och teknik av alla de slag
- Ledningens **engagemang**

- Process för riskanalys
- Process för riskhantering
- Kriterier för konsekvensbedömning
- Kriterier för sannolikhetsbedömning
- Kriterier för riskacceptans

Vad kan man ha för målsättning?

- Hantera alla kritiska risker det första året
- Hantera alla höga risker under år 2 och 3.
- Göra en komplett systeminventering (HW/SW)
- Segmentera nätverken
- Begränsa internetåtkomst beroende på applikation
- Genomföra MSB’s top-10 lista

När gör man en riskanalys?

- Är ett kontinuerligt arbete och bör göras vid förändringar
- Vid anskaffning av nya system och molntjänster
- I samband med uppgraderingar
- När drift ska läggas ut (outsourcing)
- Vid organisationsförändringar
- Vid nya uppdrag/tjänster
- Periodvis återkommande, mer eller mindre kontinuerligt

Hur gör man en riskanalys?

Workshop med intressenter

- De som har **kunskap om objektet** som ska analyseras
- **Avgränsningar** för riskanalysen (objektet)
- Alla känner till **processen och metoder**
- Alla vet hur **resultatet** ska användas
- Dokumenterad **sannolikhetsbedömning** och **konsekvensskala**

Gör följande

- **Beskriver** analysobjektet
- **Identifierar** potentiella hot mot analysobjektet
- **Analyserar** riskerna, sannolikhet och konsekvens för de olika hoten
- **Dokumenterar**
- **Kommunicerar**

Konsekvensbedömning

Konsekvens	Ekonomisk förlust	Minskat förtroende	Avbrott i verksamheten
Allvarlig	2 miljoner kronor och uppåt eller avvikelse på över 20% av budget	Ihållande drev i rikstäckande medier, eller av organiserade grupperingar i sociala medier. Ej endast enskilda personer pekas ut, utan även organisationens grundläggande kultur.	Avbrott i en eller flera kritiska verksamheter som är längre än godtagbart. Omfattande omprioriteringar av verksamheten.
Betydande	500 000 – 2 miljoner kronor eller avvikelse på 10-20% av budget	Nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier. Missnöjet är dock begränsat till enskilda händelser eller enskilda personers agerande.	Avbrott i en kritisk verksamhet som är längre än godtagbart. Stora omprioriteringar av verksamheten.
Måttlig	…	…	…
Försumbar	…	…	…

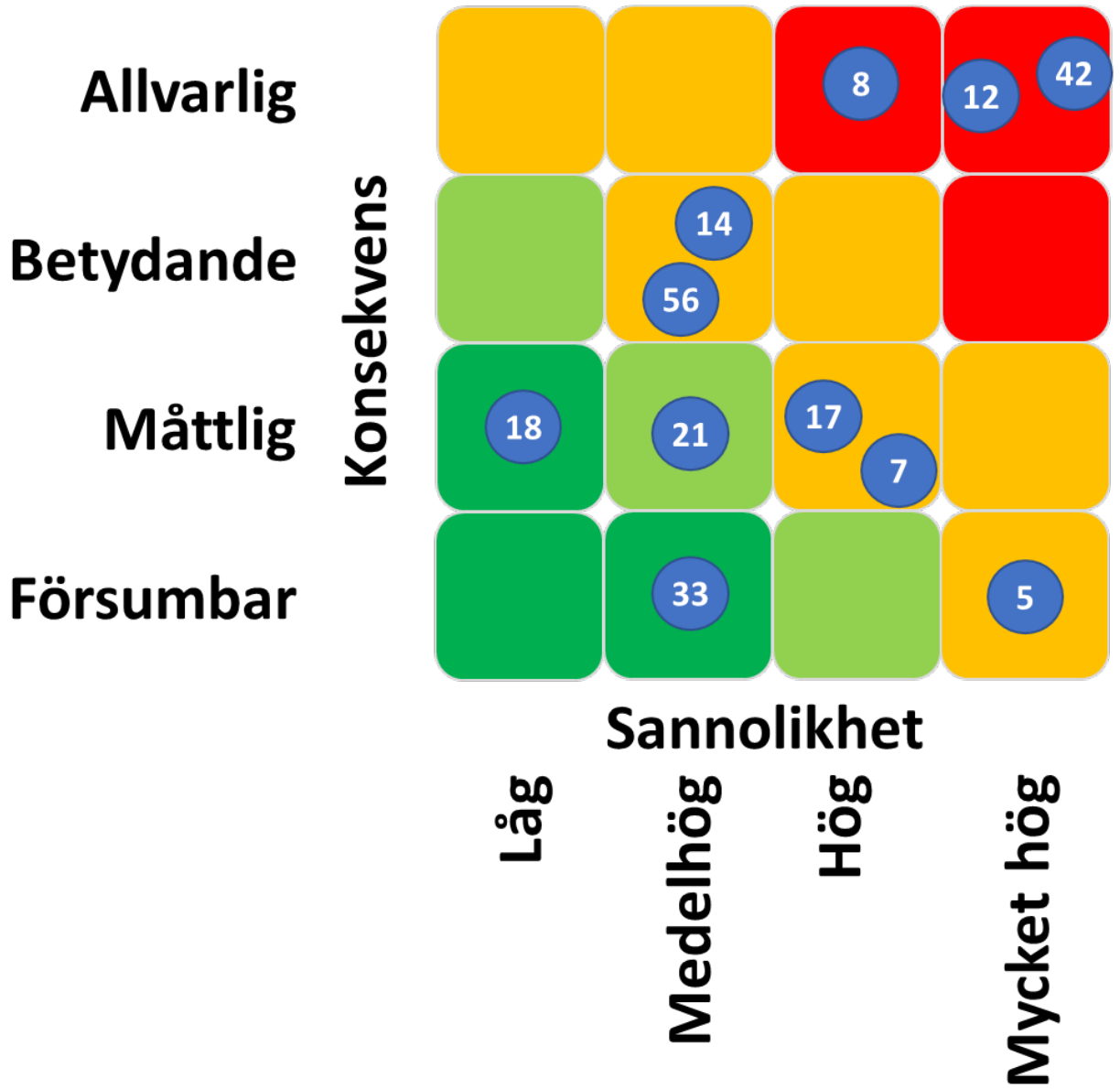
Sannolikhetsbedömning

Hur ska man veta sannolikheten?

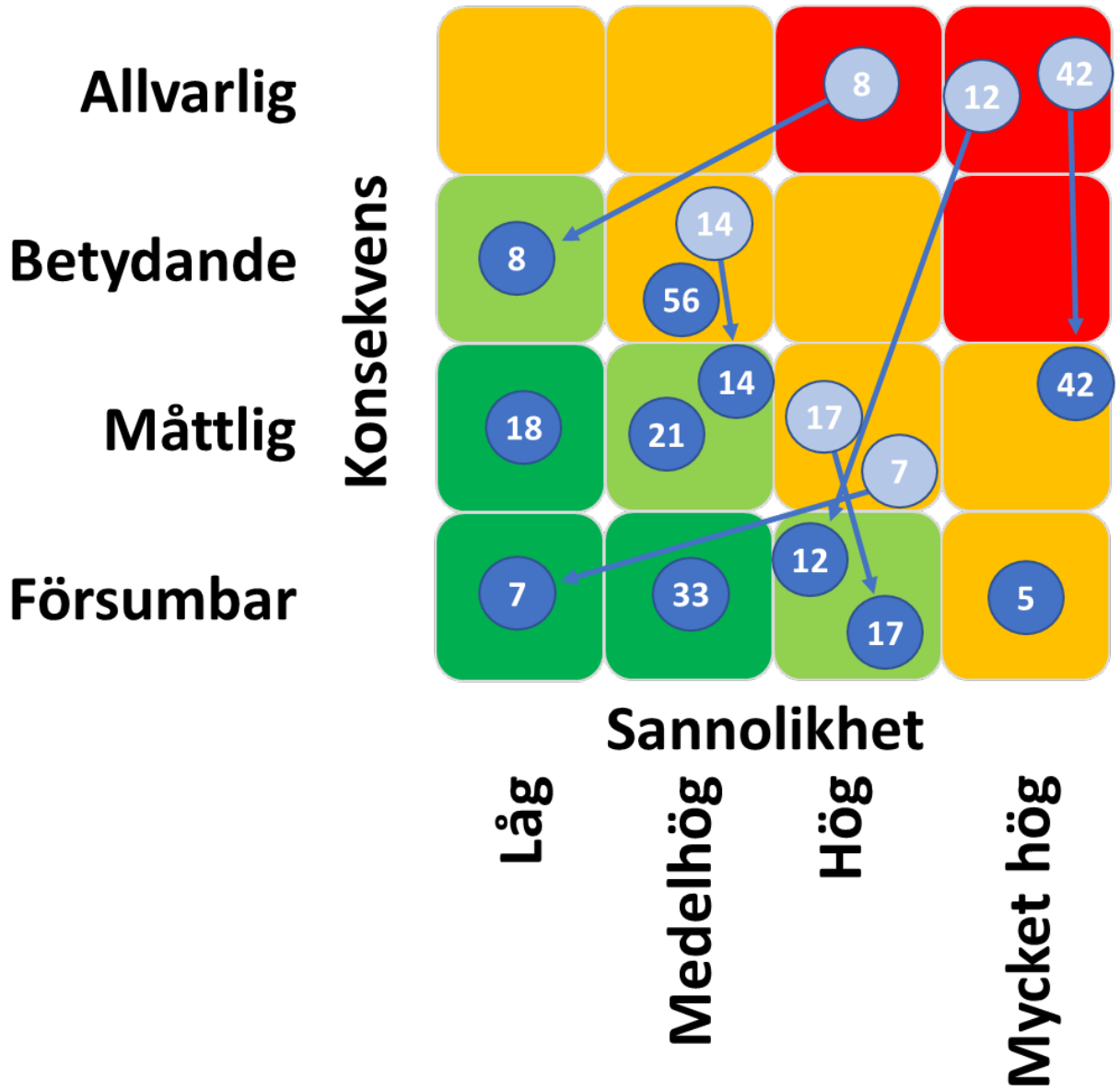
- Utgå från tidigare händelser och erfarenheter
  - Egna och andras
  - Inom samma sektor och rent generellt
  - Liknande system och miljöer
- Kvalificerade uppskattningar
  - Visst det finns vetenskapliga modeller, men att spå i framtiden är osäkert

Begrepp	Intervall
Mycket hög sannolikhet	1-10 ggr/år
Hög sannolikhet	0,5-1 ggr/år
Medelhög sannolikhet	0,05-0,5 ggr/år (mellan en gång vartannat till en gång per 20 år)
Låg sannolikhet	< 0,05 ggr/år (mindre än en gång per 20 år)

Riskmatris


Allvarlig
Betydande
Måttlig
Försumbar
Konsekvens
8
12
42
14
56
18
21
17
7
33
5
Sannolikhet
Låg
Medelhög
Hög
Mycket hög

Riskmatris


Allvarlig
Betydande
Måttlig
Försumbar
Konsekvens
8
12
42
8
14
56
14
18
21
17
7
42
7
33
12
17
5
Sannolikhet
Låg
Medelhög
Hög
Mycket hög

Både för stort och smått

- Riskanalysen kan göras både för stora organisationsövergripande processer och mindre enskilda system och tjänster
  - Verksamheten som helhet
  - Process
  - Specifik funktion eller verksamhetsområde

Riskanalysens resultat

- En dokumenterad lista över:
  - Risker
  - Riskbedömning
  - Ansvarig
- Att bli medvetna om hoten
- Beslutsunderlag för val av säkerhetsåtgärder
- Resultatet är skyddsvärd information