Informationsklassning

Arbetsmaterial vid workshop - Informationsklassning

Senast uppdaterad: 2020-05-28

OM WORKSHOPEN - INFORMATIONSKLASSNING

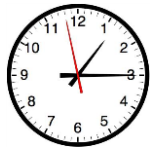
- Kort presentation om informationssäkerhet och informationsklassning
- Genomförande av workshop
- Sammanfattning och nästa steg

VAD ÄR INFORMATIONSSÄKERHET?

- Informationssäkerhet avser de åtgärder (*organisatoriska och IT-tekniska*) som genomförs för att minska hot och störningar i organisationens informationsförsörjning
  - Åtgärderna är främst baserade på verksamhetens identifierade risker, interna och externa krav och informationstillgångarnas skyddsvärde
  - Informationssäkerhets grundläggande egenskaper är *konfidentialitet*, *riktighet och tillgänglighet*. *Spårbarhet* är en stödjande del för egenskaperna ovan

Konfidentialitet

Riktighet



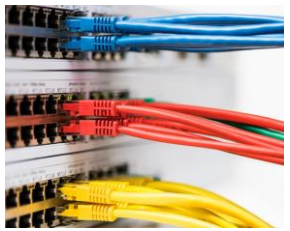
Tillgänglighet

Spårbarhet

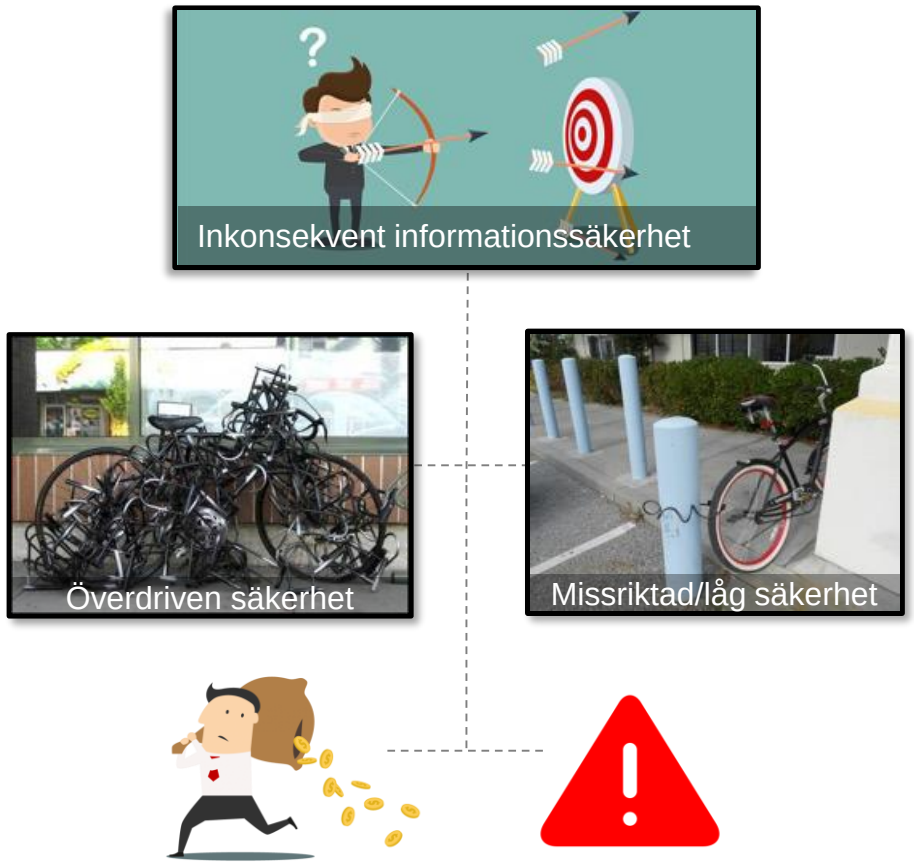
VAD ÄR INFORMATIONSSÄKERHET?

- Informationssäkerhet omfattar skydd av alla typer av informationsmedia
  - Pappersinformation
  - Digital information
  - Samtal mellan kollegor och med andra aktörer






VARFÖR ARBETA MED INFORMATIONSSÄKERHET?



INFORMATION HAR OLIKA SKYDDSBEHOV

- Information har olika skyddsbehov. Exempelvis beroende på lagstiftning och/eller hur kritisk informationen är för verksamheten

Personuppgifter

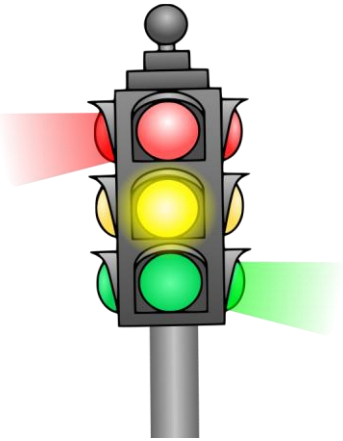
Känsliga personuppgifter

Publicerad forskningsresultat

Forskningsdata

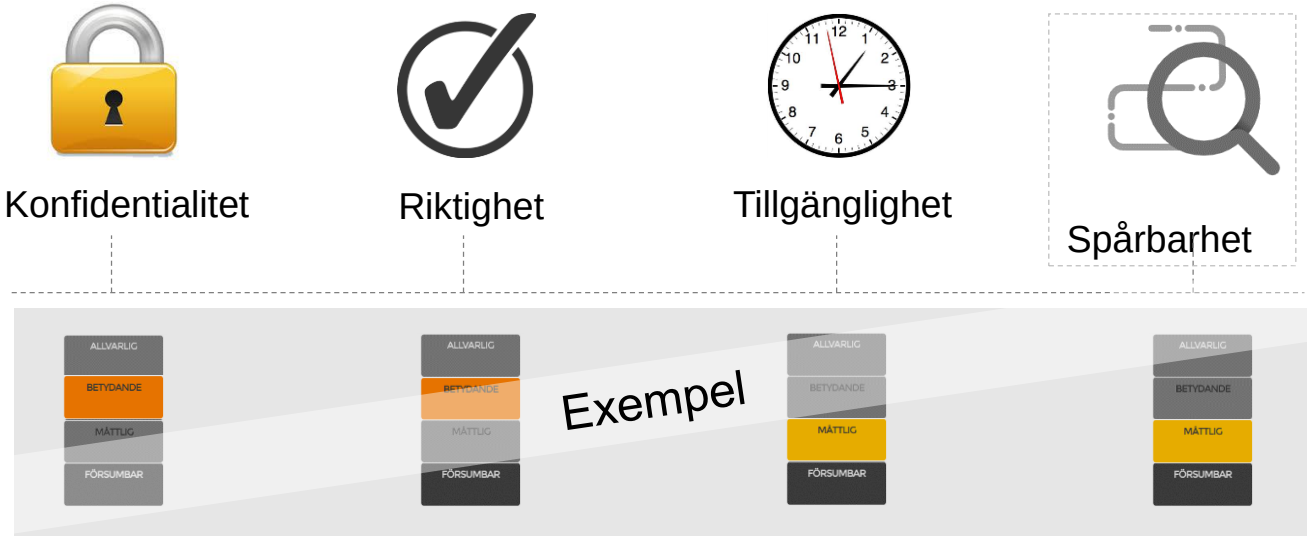
Kontouppgifter

Information på externwebben



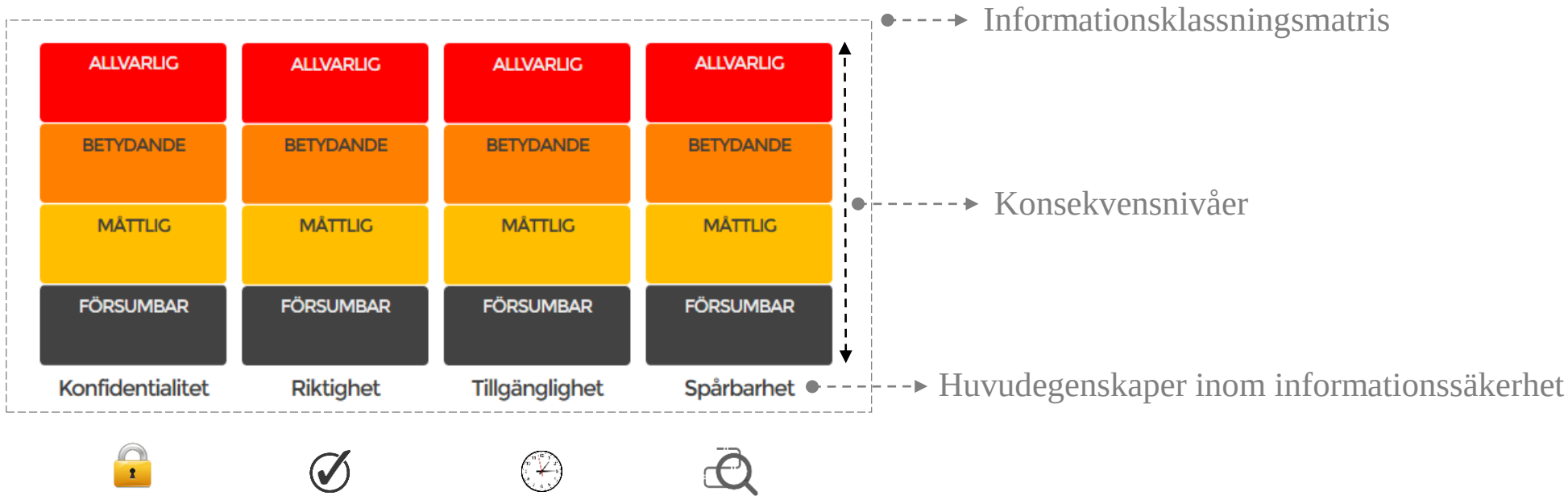
OM INFORMATIONSKLASSNING

- Metoden informationsklassning har i syfte att bedöma vilken nivå av *konfidentialitet*, *riktighet*, *tillgänglighet* (och i vissa fall *spårbarhet)* som är lämplig för att minska hot mot de aktuella informationstillgångarna
  - Bedömning görs genom att värdera vilka *konsekvenser* som kan uppkomma vid förlorad förmåga av egenskaperna nedan. *Exempelvis förlorad förmåga gällande konfidentialitet*



INFORMATIONSKLASSNING - MATRIS

- För att bedöma informationens skyddsbehov, används en s.k. informationsklassningsmatris. Denna består av fyra konsekvensnivåer
  - *Allvarlig, betydande, måttlig och försumbar*



INFORMATIONSKLASSNING – ENDAST VÄGLEDANDE

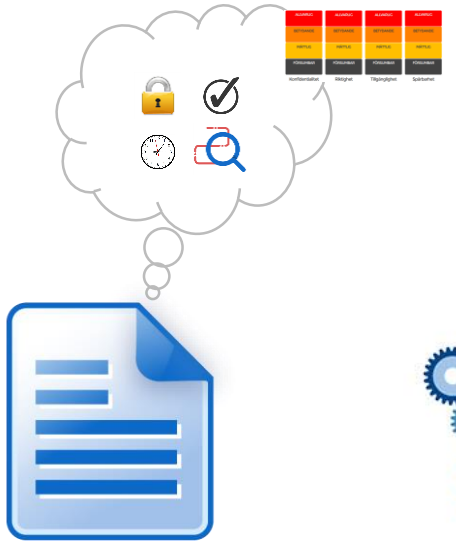
- Metoden att genomföra informationsklassning är ingen exakthet. Snarare en ”kompassriktning” vad informationstillgångar har för skyddsbehov

INFORMATIONSKLASSNING - KONTEXT

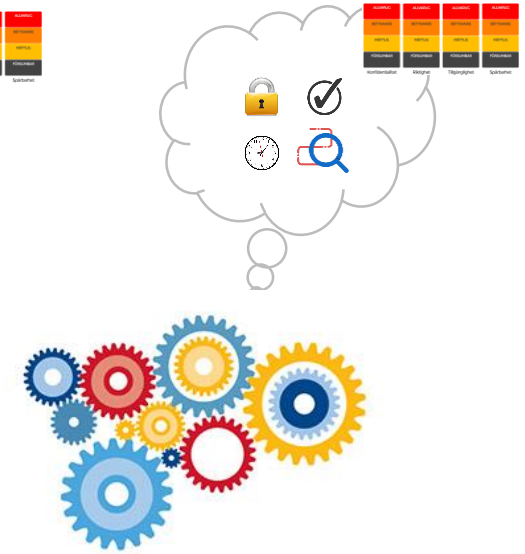
- Informationsklassning kan utföras utifrån olika perspektiv och syften

För IT-system och dess information

För informationsmängder och personuppgifts-behandlingar



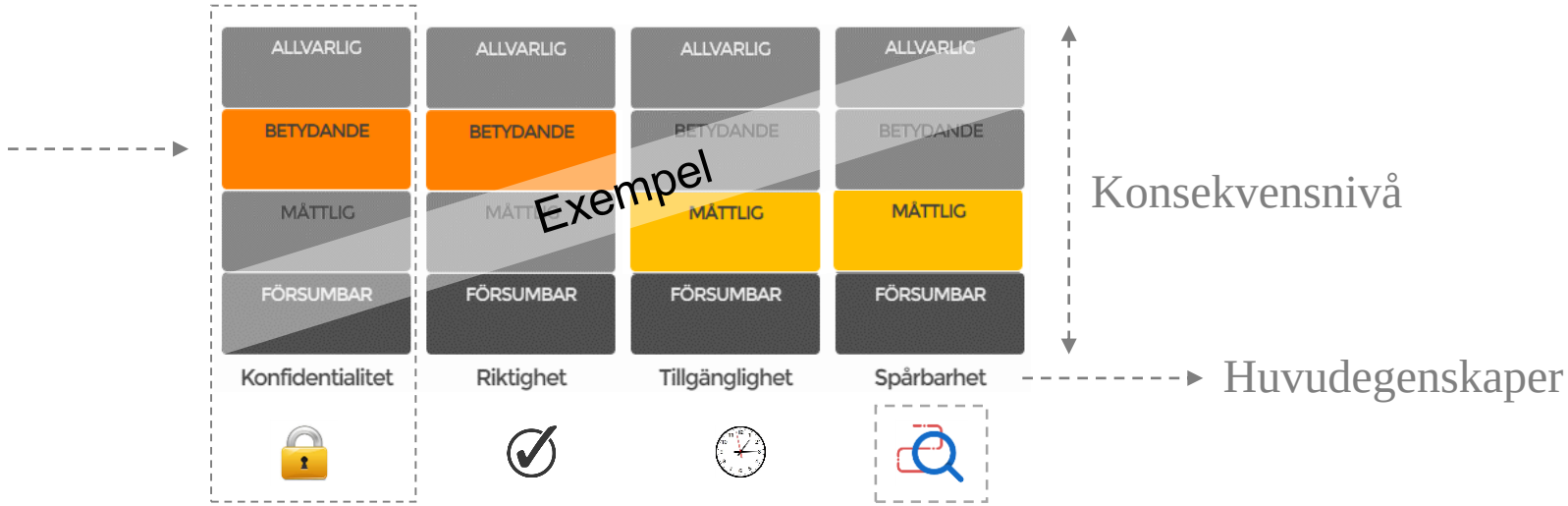
För enskilda informationsobjekt



För verksamhetsprocesser

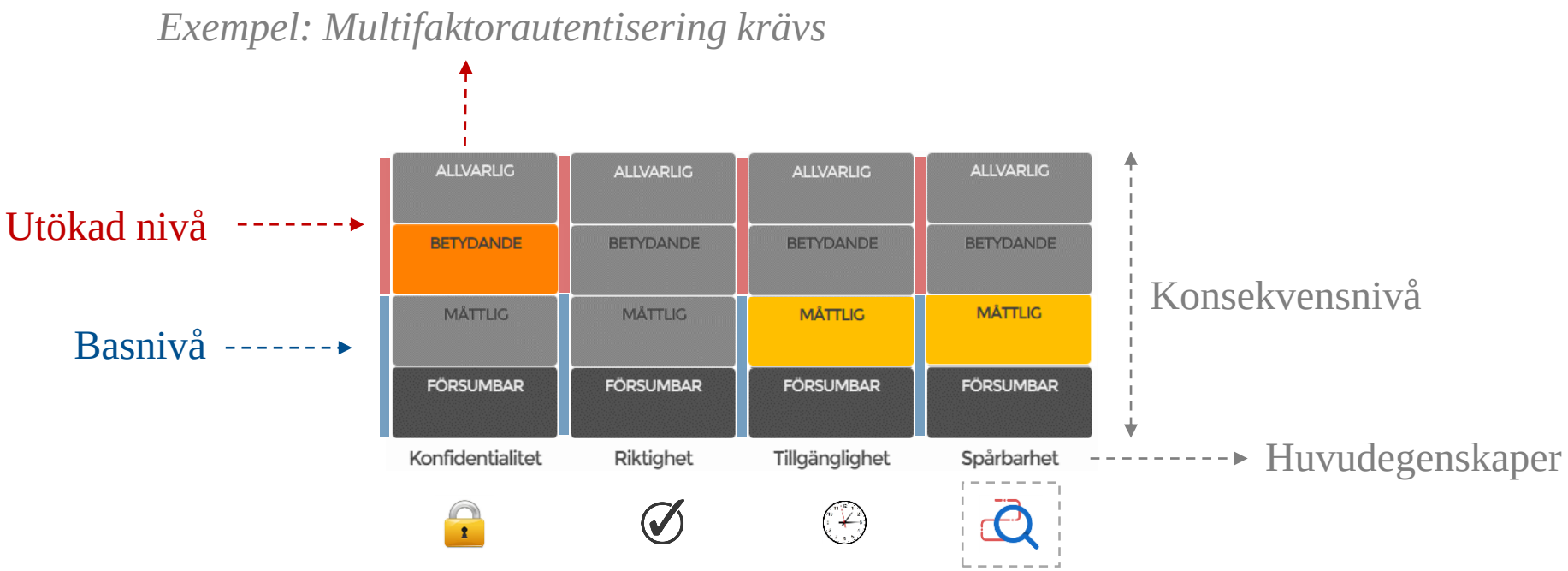
INFORMATIONSKLASSNING

- För att bedöma lämplig skyddsnivå (per egenskap) används exempelvis liknande frågeställning – *i exemplet nedan* ***konfidentialitet***
  - *Om aktuell information röjs till obehörig skulle det få* ***betydande*** *konsekvenser. <motiveringen är>…*



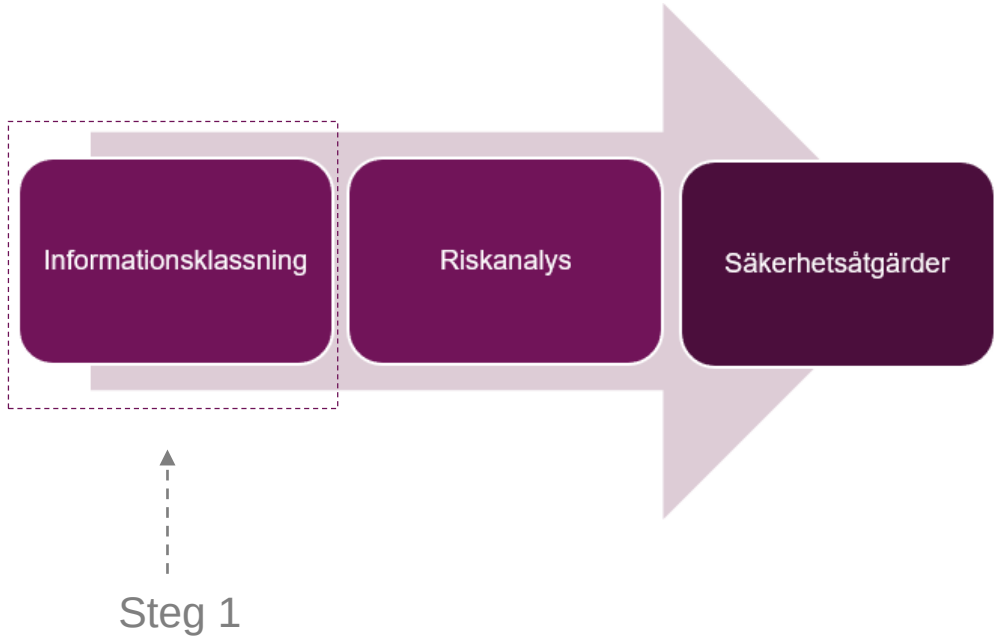
INFORMATIONSKLASSNING

- Nivå av säkerhetsåtgärder (*basnivå och utökad nivå*) beslutas beroende på vilken värdering som har gjorts avseende konsekvensnivå per egenskap.



INFORMATIONSKLASSNING

- Organisationens informationsklassning- och riskanalysmodell



INFORMATIONSKLASSNING - WORKSHOP

VÄGLEDANDE FRÅGOR

- **Verksamhetsområde/process**
  - Verksamhetsområde där IT-tjänsten och information primärt har sin tillhörighet

Ett verksamhetsområde kan också anges som en process om det ger en tydligare tillhörighet var IT-system och information har sin hemvist. Se även organisationens klassificeringsstruktur.

VÄGLEDANDE FRÅGOR

- **Placering av information och IT-tjänster**
  - Outsourcing - (Utkontraktering)
  - On-Prem - (Lokalt hos organisationen)
  - Hybrid - (En mix av ovanstående)

Klargör var information och IT-tjänster finns placerade. Exempelvis för att fastställa vilken lagstiftning som gäller och vilka eventuella avtal som ska tecknas och följas upp.

VÄGLEDANDE FRÅGOR

- **Inventera information**
  - Informationsmängder
    - Exempelvis *ekonomiuppgifter, forskningsuppgifter, personalinformation, …*
  - Informationstyper
    - Exempelvis *fakturor, biologiska prover, personnummer, …*

Informationsklassning ska alltid utgå ifrån den information som lagras, behandlas och överförs. Börja med att identifiera information utifrån ett brett perspektiv (informationsmängder) innan enskilda informationstyper identifieras.

VÄGLEDANDE FRÅGOR

- **Inventera informationssystem (IT-system/IT-tjänster)**
  - Informationssystem (IT-system/IT-tjänster) som nyttjas
  - Systemberoenden
    - Exempel *autentiseringssystem*, *databaser, …*
  - Leverantörer

Att identifiera informationssystem (IT-system/tjänster) och dess beroenden skapar en bred och viktig förståelse var information lagras, behandlas och överförs. Detta är viktig information vid val av eventuella säkerhetsåtgärder.

VÄGLEDANDE FRÅGOR

- **Ägare av information och IT-tjänster**
  - Ägare till aktuell information
  - Ägare till aktuell IT-tjänst

Det är svårt att upprätthålla informationssäkerhet utan tydliga ansvarsområden. Det är därför viktigt att klargöra hur ansvaret ser ut kring aktuell information och/eller IT-tjänst.

VÄGLEDANDE FRÅGOR

- **Arkivlagen/RA-FS**
  - IT-system/IT-tjänst är källsystem för allmänna handlingar
    - Krav på bevarande av handlingar
    - Krav på gallring av handlingar

I många fall gäller Riksarkivets lagar och föreskrifter. Det är därför viktigt att utreda om och hur dessa frågor ska hanteras.

VÄGLEDANDE FRÅGOR

- **Dataskyddsförordningen (GDPR)**
  - Personuppgifter
    - Känsliga personuppgifter
    - Omfattning av personuppgifter
    - Personuppgiftsbiträdesavtal

Om behandlingen av personuppgifter som kan leda till en hög risk för de registrerade ska en konsekvensbedömning göras. Detta görs som ett tillägg till denna informationsklassning i form av riskanalys/konsekvensanalys.

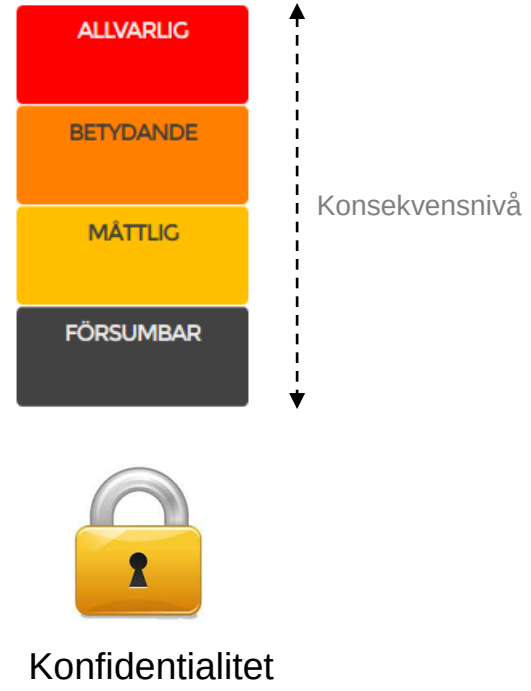
VÄGLEDANDE FRÅGOR

- **Övriga avtal**
  - Avtal med intressenter som reglerar informationssäkerhet

Om det förekommer avtal med intressenter som reglerar informationssäkerhet måste dessa tas i beaktning i samband med val av säkerhetsåtgärder.

VÄGLEDANDE FRÅGOR

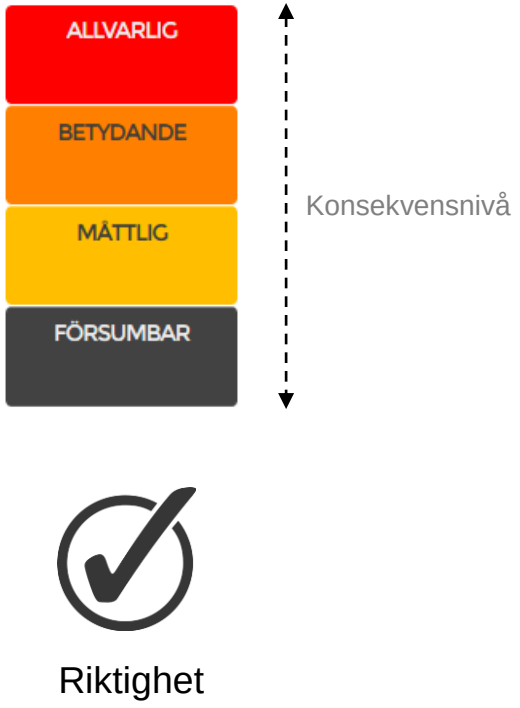
- **Konsekvens om informationssystem/information röjs/sprids till obehöriga**
  - Förslag på perspektiv:
    - *Lagar, förordningar och avtal*
    - *Integritet och hälsa*
    - *Hela eller delar av organisationens anseende*
    - *Ekonomiska och/eller kärnverksamhetsrelaterade förutsättningar*



VÄGLEDANDE FRÅGOR

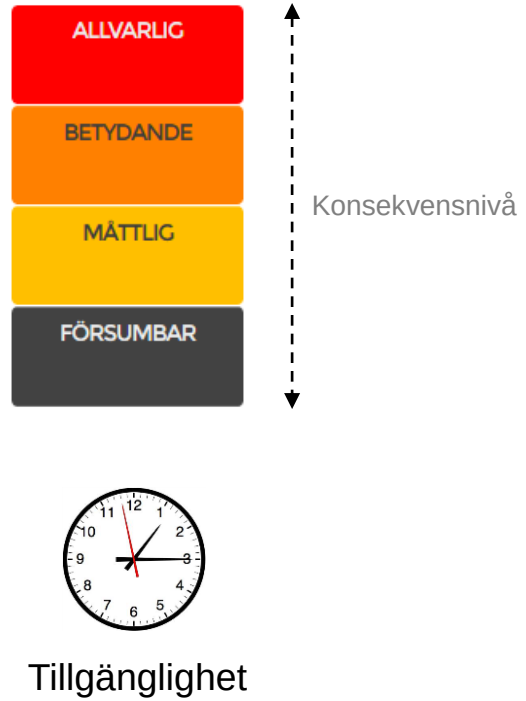
- **Konsekvens om informationssystem/information inte är riktigt/fullständig**

  - Förslag på perspektiv:
    - *Lagar, förordningar och avtal*
    - *Integritet och hälsa*
    - *Hela eller delar av organisationens anseende*
    - *Ekonomiska och/eller kärnverksamhetsrelaterade förutsättningar*



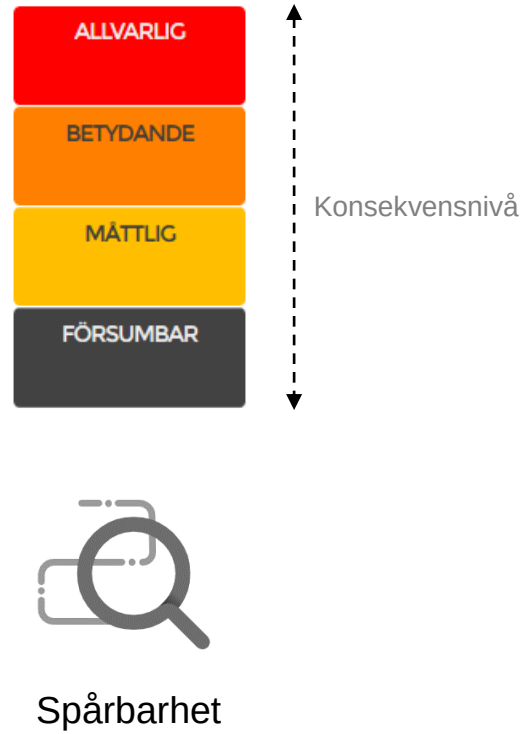
VÄGLEDANDE FRÅGOR

- **Konsekvens om informationssystem/information inte är tillgänglig under 2 arbetsdagar**
  - Förslag på perspektiv:
    - *Lagar, förordningar och avtal*
    - *Integritet och hälsa*
    - *Hela eller delar av organisationens anseende*
    - *Ekonomiska och/eller kärnverksamhetsrelaterade förutsättningar*



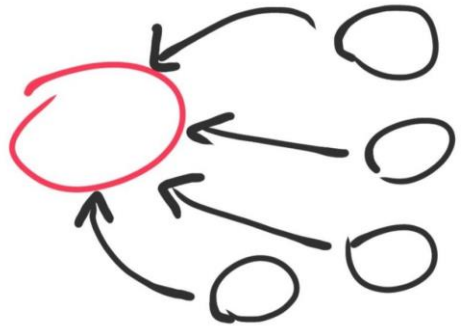
VÄGLEDANDE FRÅGOR

- **Konsekvensen om åtkomst och ändringar i informationssystem/information inte är spårbara**
  - Förslag på perspektiv:
    - *Lagar, förordningar och avtal*
    - *Integritet och hälsa*
    - *Hela eller delar av organisationens anseende*
    - *Ekonomiska och/eller kärnverksamhetsrelaterade förutsättningar*



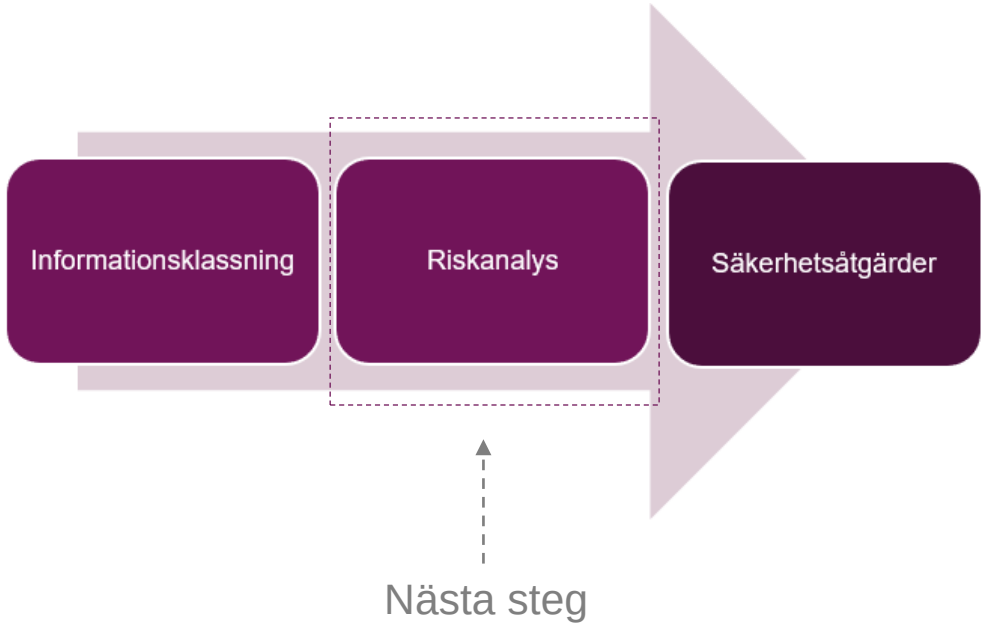
SAMMANFATTNING AV INFORMATIONSKLASSNINGEN

- Rättsliga och organisatoriska förutsättningar
  - Vilka rättsliga och organisatoriska förutsättningar har identifierats?
- Genomförd informationsklassning
  - Vilken informationsklassningsnivå (säkerhetsprofil) har vi kommit fram till?
- Vad är nästa steg?
  - Rapport från t.ex. externt konsult
  - Bedömning om riskanalys ska genomföras
  - Bedömning vilka eventuella säkerhetsåtgärder som ska vidtas



RISKANALYS

- Nästa steg är att genomföra riskanalys



VILKA SKA VARA MED PÅ RISKANALYSEN?

BRA JOBBAT!