Sveriges Kommuner och Regioner

# KLASSA Användarforum #5

Zoom, 2024-06-13

Sveriges Kommuner och Regioner

# Välkomna till det femte användarforumet!

Sveriges Kommuner och Regioner

# Att tänka på under dagen

- Ingen sekretess
- Ljud och bild
- Frågor i chatten
- Speaker view/pin video
- Stanna kvar i mötet

# Agenda

10:00 – Inledning – *Lotta Nordström*
10:10 – Vad har hänt sen sist? – *Jonas Nilsson*
11:00 – Vad är planen framåt? – *Thomas Nilsson*
11:30 – Paus – sträck på benen
11:40 – Vad är planen framåt? – *Thomas Nilsson*
12:00 – Lunch
13:00 – ”Grupparbete”
14:45 – Summering – *Lotta, Jonas och Thomas*
15:00 – Avslut

Sveriges Kommuner och Regioner

# Inledning

Lotta Nordström

Sveriges Kommuner och Regioner

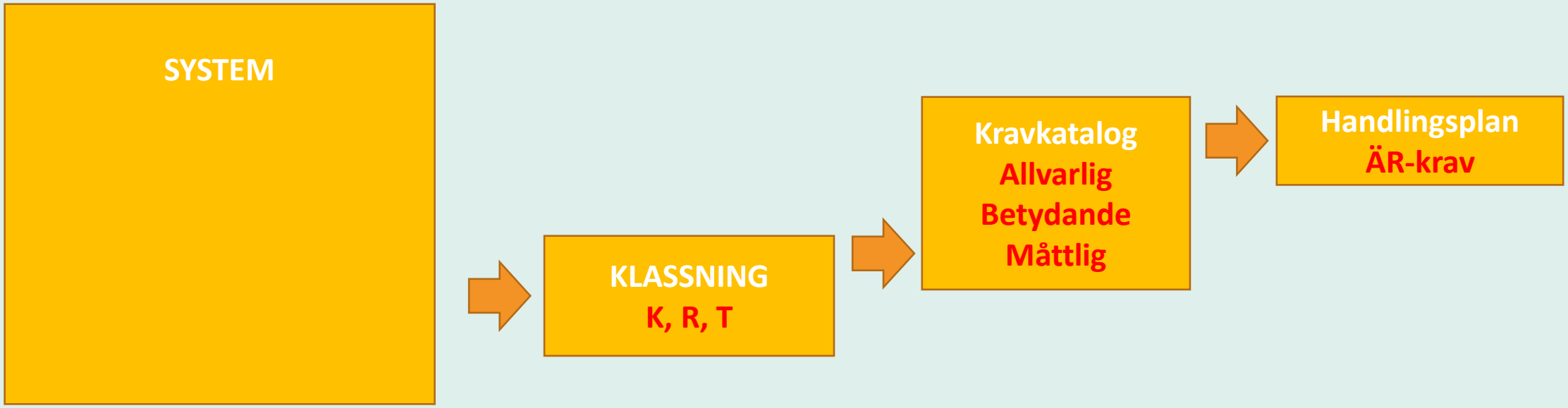
# Vad har hänt sedan sist

Jonas Nilsson

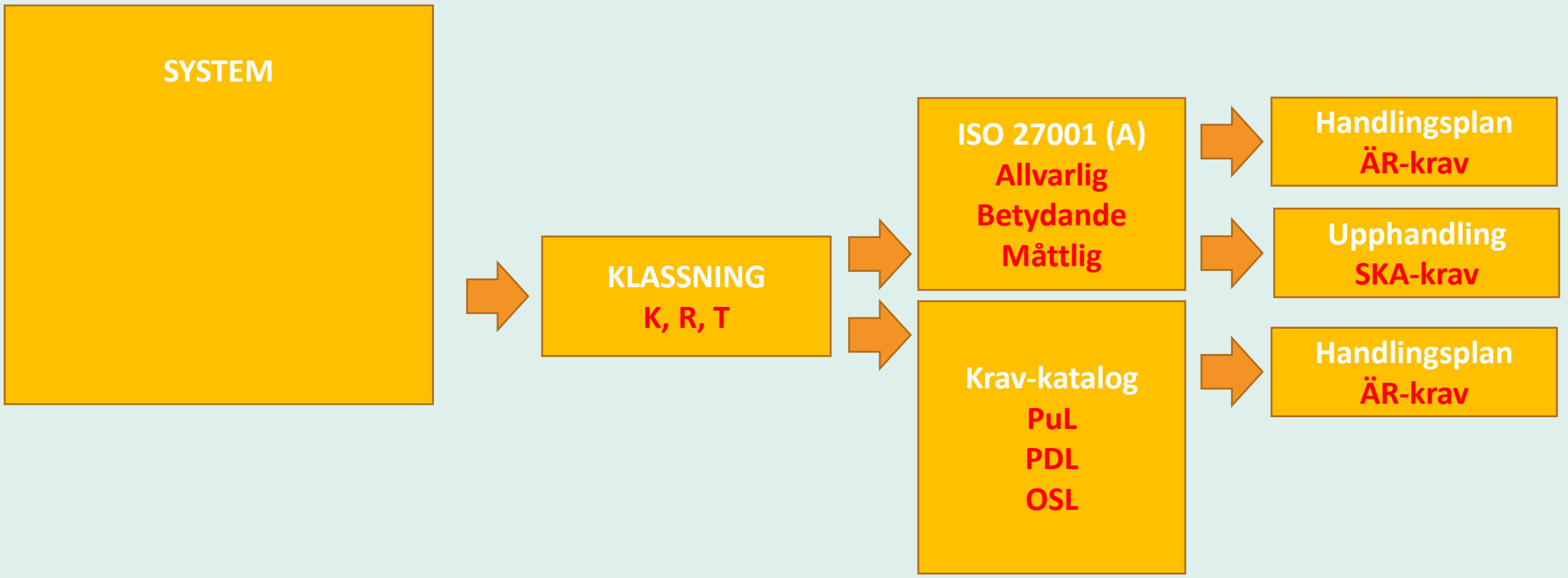
# Fröet till KLASSA

- Idén till KLASSA föddes i kölvattnet av de *16 principer för samverkan* som togs fram i Stockholmsregionen
  - En princip är att klassificera och värdera information på ett likartad sätt
  - Dock var det då oklart hur resultatet skulle omsättas i faktiska krav
- En matris med krav som tillämpades på systemnivån togs fram 2012 vilket var fröet till KLASSA som lanserades av SKR 2014
  - Utgångspunkten var en gemensam konsekvensskala från SiS/MSB
- Målgruppen för KLASSA var systemförvaltaren

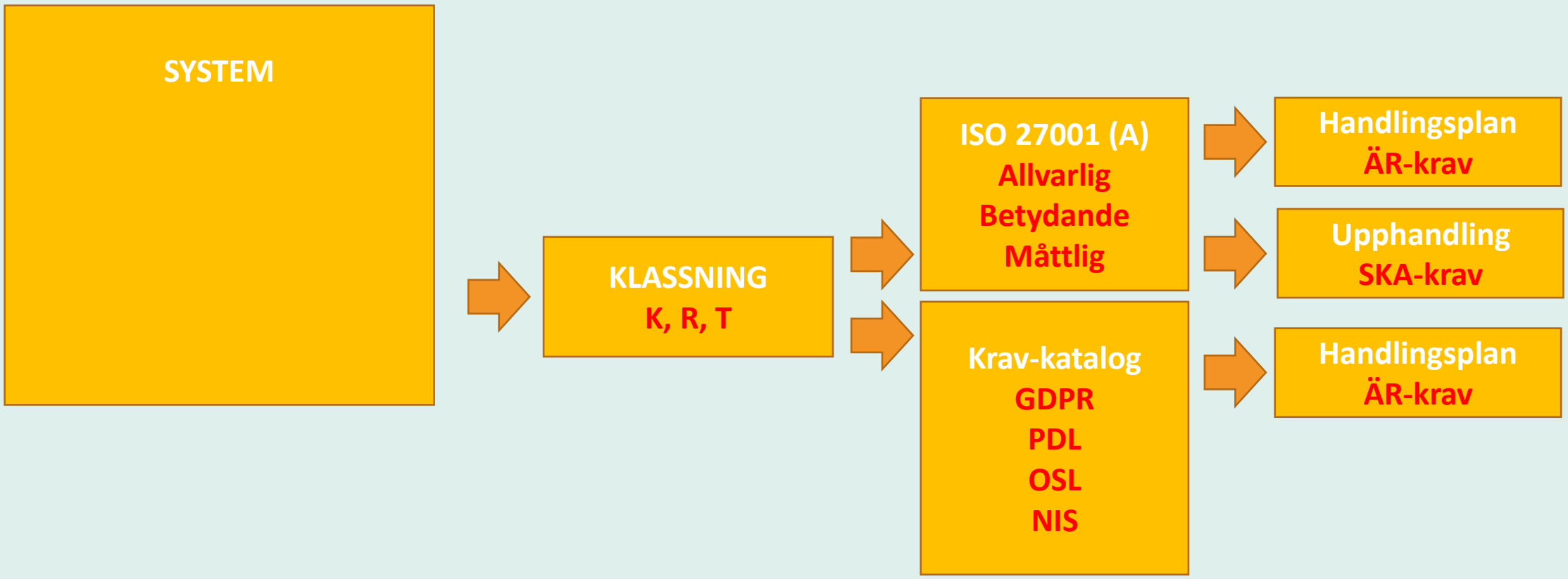
# KLASSA (v1)


SYSTEM
KLASSNING
K, R, T
Kravkatalog
Allvarlig
Betydande
Måttlig
Handlingsplan
ÄR-krav

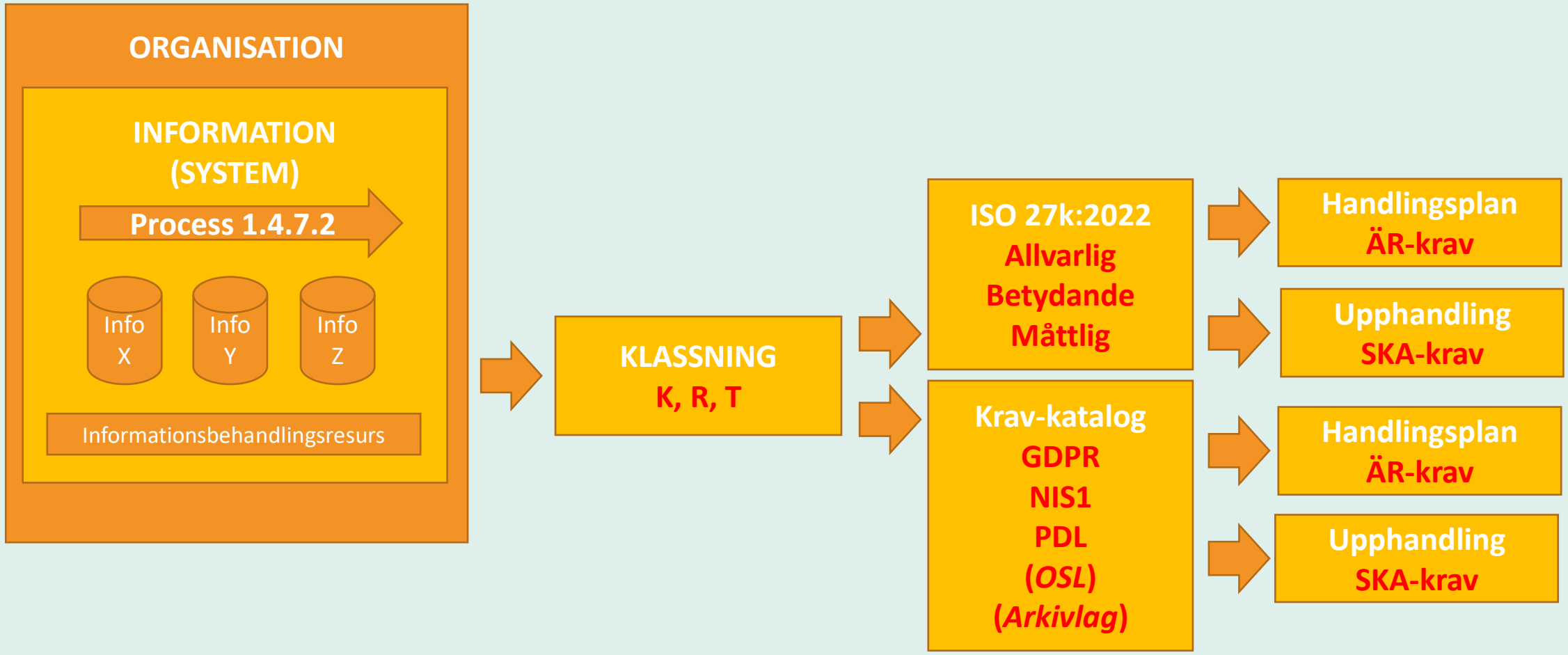
# KLASSA (v2)


SYSTEM
KLASSNING
K, R, T
ISO 27001 (A)
Allvarlig
Betydande
Måttlig
Krav-katalog
PuL
PDL
OSL
Handlingsplan
ÄR-krav
Upphandling
SKA-krav
Handlingsplan
ÄR-krav

# KLASSA (v3)


SYSTEM
KLASSNING
K, R, T
ISO 27001 (A)
Allvarlig
Betydande
Måttlig
Krav-katalog
GDPR
PDL
OSL
NIS
Handlingsplan
ÄR-krav
Upphandling
SKA-krav
Handlingsplan
ÄR-krav

# KLASSA (v4)


ORGANISATION
INFORMATION (SYSTEM)
Process 1.4.7.2
Info X
Info Y
Info Z
Informationsbehandlingsresurs
KLASSNING
K, R, T
ISO 27k:2022
Allvarlig
Betydande
Måttlig
Krav-katalog
GDPR
NIS1
PDL
(OSL)
(Arkivlag)
Handlingsplan
ÄR-krav
Upphandling
SKA-krav
Handlingsplan
ÄR-krav
Upphandling
SKA-krav

Sveriges Kommuner och Regioner

# Syftet och målet med KLASSA

- Syftet med KLASSA är att höja mognadsgraden i det systematiska informationssäkerhetsarbetet
- KLASSA ska vara lätt att använda och vända sig till breda målgrupper för att succesivt förbättra organisationens informationssäkerhet
- KLASSA ska utvecklas kontinuerligt för att följa en föränderlig omvärld med nya lagkrav, nya risker och nya sätt att behandla information

# Forum

- **Expertgruppen** är begränsad till åtta (8) namngivna experter från betalande organisationer
  - KLASSA:s styrgrupp bestämmer vilka som utgör KLASSA:s expertgrupp
  - Ansvarar t.ex. för utformning av metodik och innehåll i kravkataloger
- **Användarforum** består av samtliga betalande medlemmar har en plats i KLASSA användarforum
  - Rådgivande för KLASSA:s utveckling
  - Prioritering och omfattning
- Källkoden utvecklas av upphandlade utvecklingsresurser

# KLASSA - ett nav för infosäk

- Samlingspunkt för:
  - Informationssäkerhetsrelaterade vägledningar från SKR och andra vägledningar som bedöms relevanta för SKR:s medlemmar
  - Referenskonsekvensbedömningar
    - Office 365, Bildanalys mm
- Självstudiematerial för att lära sig mer om KLASSA och infosäk
  - Kräver licens för KLASSA

Sveriges Kommuner och Regioner

# Användare av KLASSA 4.0

347 organisationer:

- Kommuner
- Regioner
- Kommunala bolag
- Statliga myndigheter
  - T.ex. IVO, Skatteverket och SJ
- Övriga organisationer
  - T.ex. SKR och Adda

# Finansiering av KLASSA

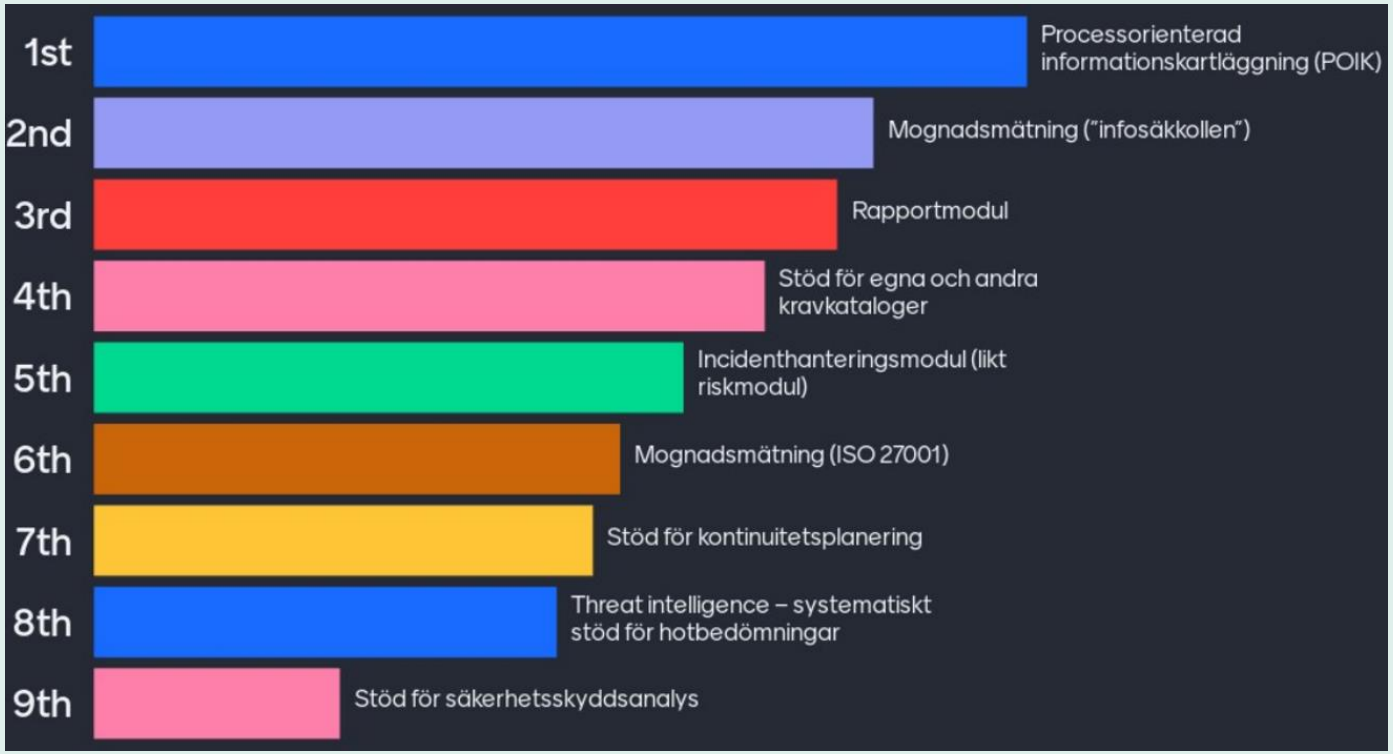
- SKR, Inera och Adda
- Fortsatt gratis…
- Den som väntar på något gott…

# Resultat från tidigare användarforum

- Börjat omhänderta resultatet med den nya utvecklingspartnern, men…

Sveriges Kommuner och Regioner

# Vilken funktionalitet är mest prioriterad i KLASSA?



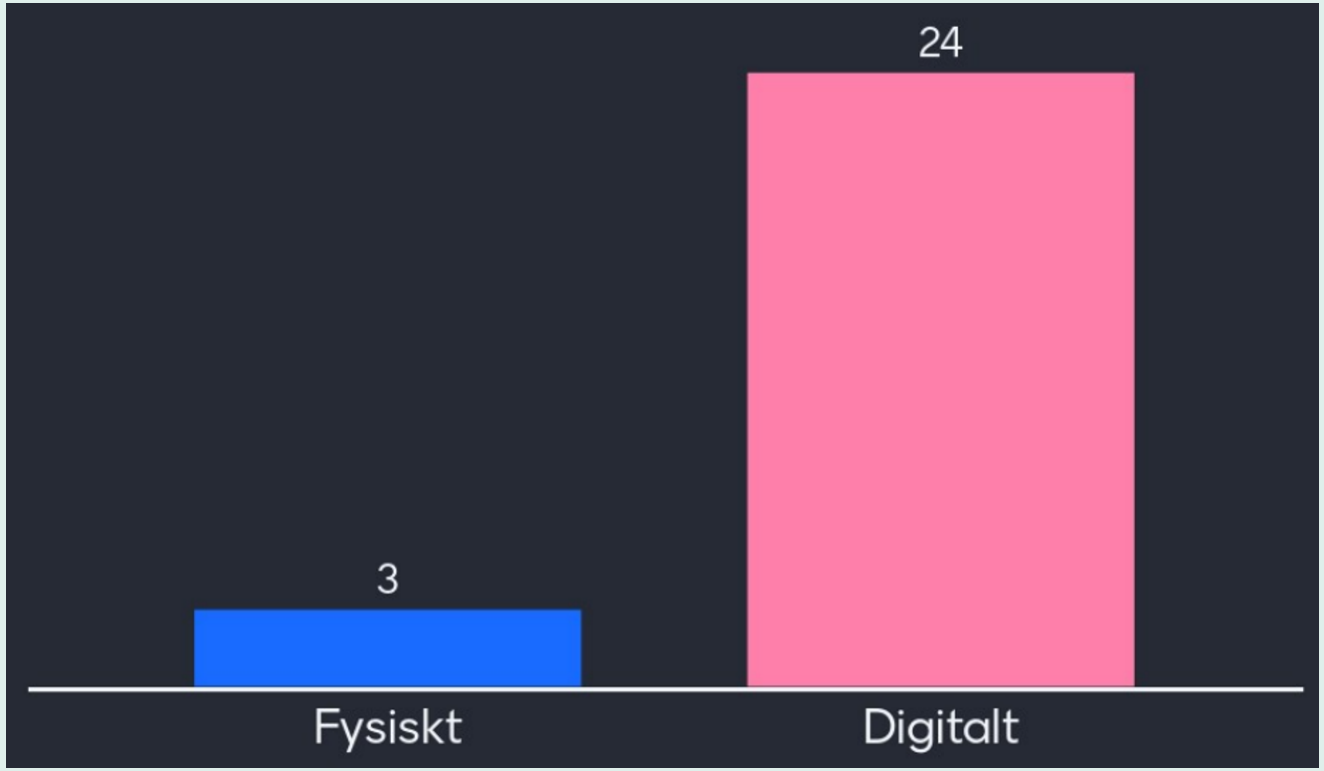
# Vilken annan funktionalitet ser ni att KLASSA bör erbjuda?

- Informationshanteringsplan
- GDPR
  - Registerförteckning
  - Konsekvensbedömning
- Incidenthanteringsmodul
- Export och import
- Rapportmodul

# Vilken funktionalitet, i KLASSA 4.0, vill ni ändra på?

- Förtydliga/förenkla ”kravfrågorna”
- Flytta informationstillgångar i organisationsträdet
- Kopiera en kravmall och utgå från den
- Vid gruppering av informationstillgångar, kunna välja från hela organisationen
- En väg för leverantörer att svara, inför upphandling
- Behörighetshanteringen
- Användarhandbok

# Hur vill ni att användarträffarna arrangeras?



Sveriges Kommuner och Regioner

# Vad är nytt?

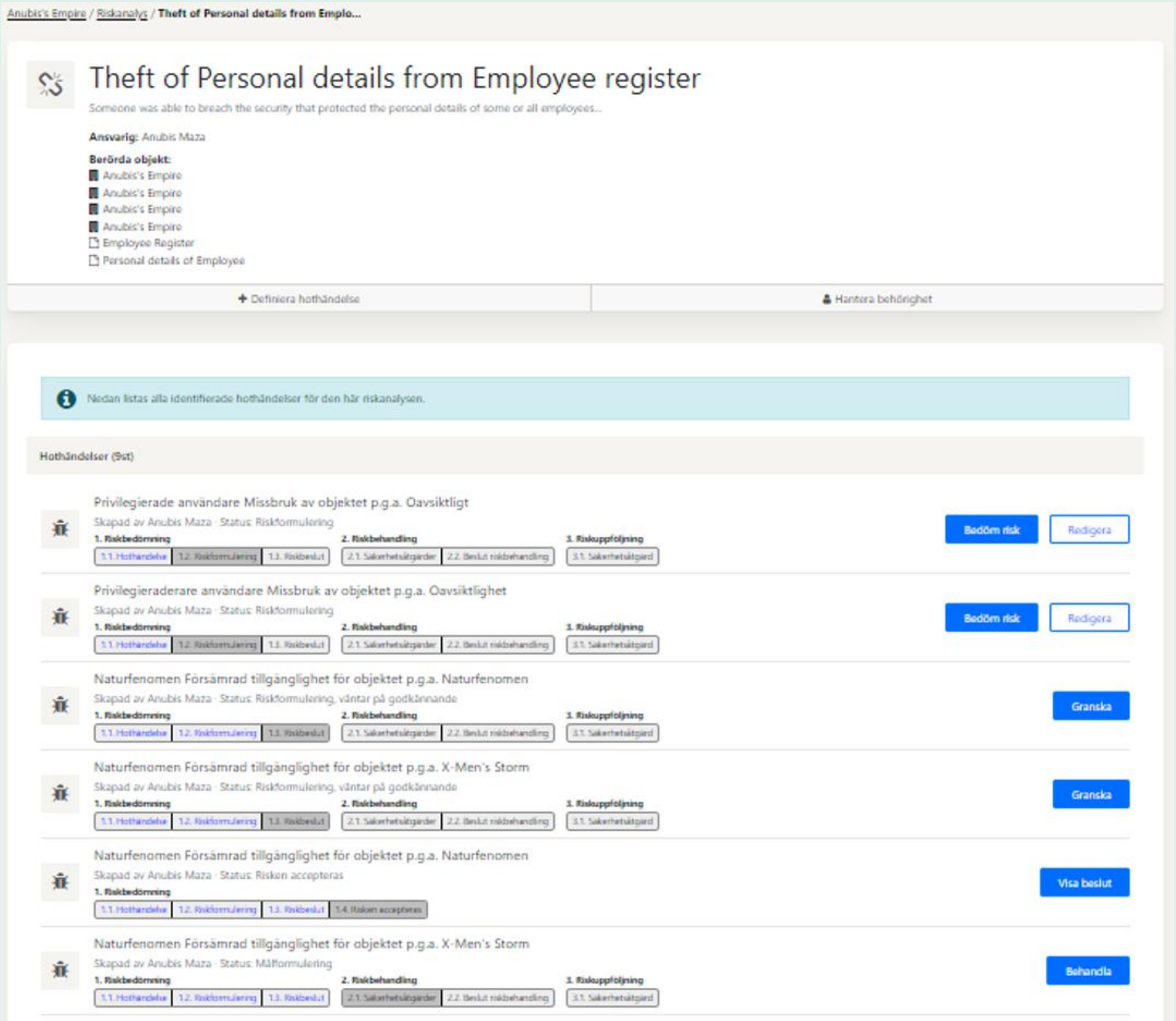
- Ny utvecklingspartner
  - Regent
- Uppdatering av kravkatalogen enligt ISO/IEC 27002:2022 samt lagrumskraven
  - Återinförande av Arkivlagen och OSL samt korrigeringar i KLASSA
- Sparsamt med utveckling…
  - Riskhanteringsmodulen
  - On-prem
  - Buggrättning

# KLASSA riskmodul – sommaren 2024

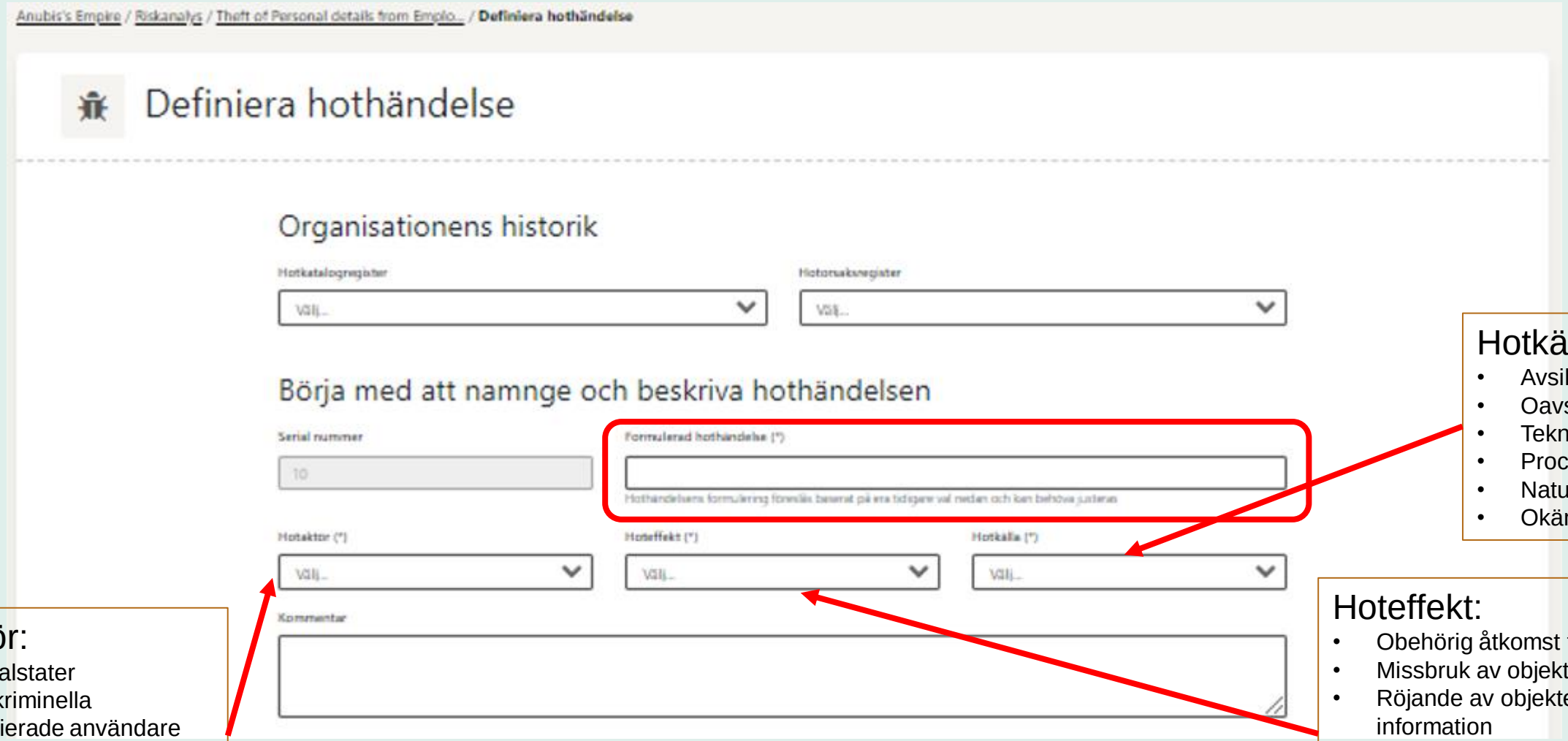
- Specifikt sammanhang/situation
- Tydliga riskformuleringar
- Ändamålsenliga och proportionella säkerhetsåtgärder
- Entydiga riskbeslut & effektmål

*…säkerställer att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat…*

Sveriges Kommuner och Regioner



Sveriges Kommuner och Regioner




## Hotaktör:

- Nationalstater
- Cyberkriminella
- Priviligierade användare
- Ej priviligierade användare
- Skadlig kod
- Naturfenomen
- Okänt

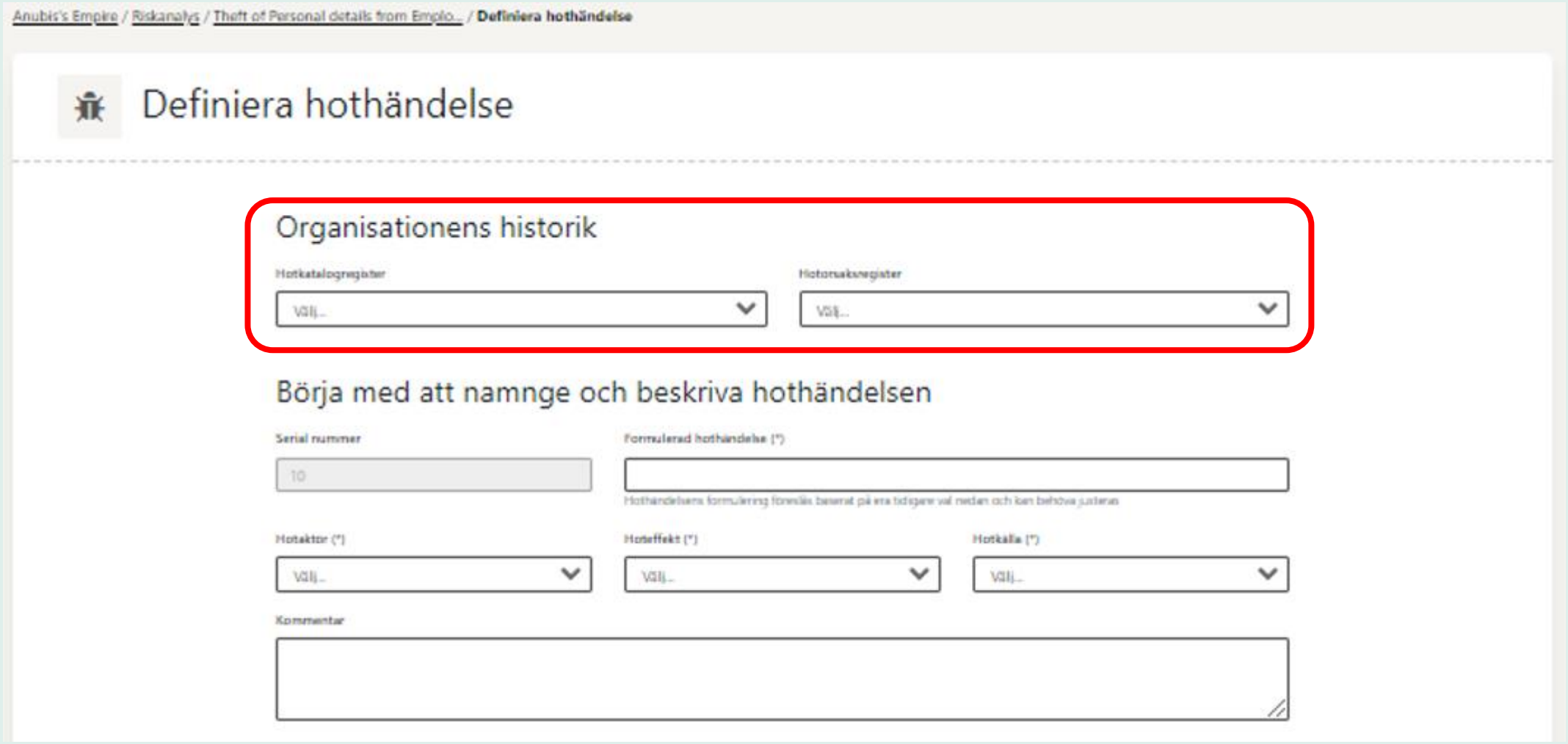
## Hotkälla:

- Avsiktligt
- Oavsiktligt
- Tekniskt fel
- Processfel
- Naturfenomen
- Okänt

## Hoteffekt:

- Obehörig åtkomst till objekt
- Missbruk av objektet
- Röjande av objektets information
- Försämrad riktighet hos objektet
- Försämrad tillgänglighet för objektet
- Okänt

Sveriges Kommuner och Regioner



Sveriges Kommuner och Regioner



# Definiera hothändelse

## Organisationens historik

Hotkatalogregister
Välj...

Hotorsaksregister
Välj...

## Börja med att namnge och beskriva hothändelsen

Serial nummer
10

Formulerad hothändelse (*)

Hothändelsens formulering föreslås baserat på era tidigare val nedan och kan behöva justeras

Hotaktör (*)
Välj...

Hoteffekt (*)
Välj...

Hotkälla (*)
Välj...

Kommentar

## Skadepåverkan

Försämrad/förlorad
☐ Konfidentialitet
☐ Riktighet
☐ Tillgänglighet

## Ange hotorsaker som kan utlösa händelsen

Orsak (*)

Inverkan (*)
Välj...

Beskriv orsaken

Ta bort

+ Lägg till hotorsak

Definiera hothändelse

# Formulera risk för #2

System users not knowing what they are doing...

**Ansvarig:** Anubis Maza

**Formulerad hothändelse:** "Privilegieraderare användare Missbruk av objektet p.g.a. Oavsiktlighet"

## Bedömda värden före att åtgärder har implementerats

### Konsekvensbedömning (tkr/år)

| Min (*) | Mest Troligt (*) | Max (*) | Beräknad konsekvens |
|---|---|---|---|
| 50 | 200 | 300 | 192 |

Motivera bedömningen (*)

Konsekvensbedömning text

### Sannolikhetsbedömning (ggr/år)

| Min (*) | Mest Troligt (*) | Max (*) | Beräknad sannolikhet |
|---|---|---|---|
| 0.50 | 65.00 | 90.00 | 58.42 |

Motivera bedömningen (*)

Sannolikhetsbedömning text

Riskformulering (*)

Privilegierade användare Missbruk av objektet p.g.a. Oavsiktligt. Detta bedöms ske 58,42 ggr/år med en trolig skada per händelse på 192 tkr.

Riskformuleringen föreslås baserat på era tidigare val och kan behöva justeras

Du har här möjlighet att fastställa bedömningen. När bedömningen är fastställd så kommer inga fler ändringar att kunna göras. Eller så kan du spara och fortsätta senare.

Spara Fortsätt

Sverig
Komm
och R

Anubis's Empire / Riskanalys / Theft of Personal details from Emplo... / **Riskbeslut**

# Fastställ risk för #3

Mother nature had her own ideas...

**Ansvarig:** Anubis Maza

**Formulerad hothändelse:** "Naturfenomen Försämrad tillgänglighet för objektet p.g.a. Naturfenomen"

## Riskbedömning

**Riskformulering**

"Naturfenomen Försämrad tillgänglighet för objektet p.g.a. Naturfenomen. Detta bedöms ske 9 ggr/år med en trolig skada per händelse på 6 tkr."

**Bedömd konsekvensnivå (tkr)**

6

**Motivering**

Konsekvensbedömning text

**Bedömd sannolikhetsnivå (ggr/år)**

9.00

**Motivering**

Sannolikhetsbedömning text

## Riskbeslut

Beslut (*)

○ Risken accepteras ○ Risken accepteras ej

Motivering för beslut (*)

Fastställ

Sveriges Kommuner och Regioner



# Lägg till säkerhetsåtgärd för Harder to reach the structure

## Organisationens historik

Säkerhetsåtgärdregister

Välj...

## Namnge och beskriv åtgärden

Namn (*)

Beskrivning (*)

## Bedömd reduktionsförmåga

Reducering sannolikhet (*)

Välj...

Motivering av reduktion för sannolikhet (*)

Reducering konsekvens (*)

Välj...

Motivering av reduktion för konsekvens (*)

Bedömda sideeffekter (neg/pos)

## Bedömda kostnader

Bedömd investeringskostnad (*)

Bedömd driftskostnad (*)

Lägg till säkerhetsåtgärd

Sveriges Kommuner och Regioner

Sveriges Komm och R

Anubis's Empire / Riskanalys / Theft of Personal details from Emplo... / **Granska målformulering**

# Fastställ målformulering för #9

Mother nature had her own ideas...

**Ansvarig:** Anubis Maza

**Formulerad hothändelse:** "Naturfenomen Försämrad tillgänglighet för objektet p.g.a. X-Men's Storm"

**Riskformulering:** "Naturfenomen Försämrad tillgänglighet för objektet p.g.a. X-Men's Storm. Detta bedöms ske 1000000 ggr/år med en trolig skada per händelse på 1000 tkr."

## Föreslagna säkerhetsåtgärder

Här nedan listas de säkerhetsåtgärder som är föreslagna för hanteringen av de identifierade hotorsakerna. Utifrån dessa skall du bedöma nya nivåer för sannolikhet, konsekvens och sårbarhet. I nästa steg får du se det nya riskvärdet och då ta beslut om målformuleringen godkänns eller skickas tillbaka för vidare bearbetning.

### 1. Harder to reach the structure - Betydande

**A: Contact X-Men's leader** — **Invest.kostn.:** 3 **Driftskostn.:** 3

**Beskrivning:**
A: To help with this we can contact the X-Men's leader called Charles Francis Xavier as he has control over all mutants...

**Reducering sannolikhet:** Okänd
**Motivering av reduktion för sannolikhet:**
Sannolikhet text

**Reducering konsekvens:** Okänd
**Motivering av reduktion för konsekvens:**
Konsekvens text

**Bedömda sidoeffekter (neg/pos):** I do NOT need to write something...

**Bedömd investeringskostnad:** 3

**Bedömd driftskostnad:** 3

**AA: Contact X-Men's leader** — **Invest.kostn.:** 6 **Driftskostn.:** 6

**Beskrivning:**
AA: To help with this we can contact the X-Men's leader called Charles Francis Xavier as he has control over all mutants... AA: To help with this we can contact the X-Men's leader called Charles Francis Xavier as he has control over all mutants... AA: To help with this we can contact the X-Men's

Sveriges Kommun och Regi

**Bedömda sidoeffekter (neg/pos):** I do NOT need to write something...

**Bedömd investeringskostnad:** 9

**Bedömd driftskostnad:** 9

## Bedömda värden efter att åtgärder har implementerats

### Konsekvensbedömning (tkr/år)

Min (*) | Mest Troligt (*) | Max (*) | Beräknad konsekvens

Motivera bedömningen (*)

### Sannolikhetsbedömning (ggr/år)

Min (*) | Mest Troligt (*) | Max (*) | Beräknad sannolikhet

Motivera bedömningen (*)

Riskformulering (*)

Riskformuleringen föreslås baserat på era tidigare val och kan behöva justeras

### Bedömda kostnader

Bedömd investeringskostnad (*) | Bedömd driftskostnad (*)

Fortsätt

Sveriges Kommuner och Regioner

| **Identifiering** | | | **Värdering** | | | | **Riskbehandling** | | | | **Uppföljning** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Risk ID | Informations-tillgång /process | Riskformulering | Negativ påverkan på: | Konsekvens | Sannolikhet | Riskvärde | Prioritet | Bedömning av nuvarande åtgärder | Beskrivning av ytterligare åtgärder | Ansvarig för åtgärd | Uppföljning |
| | | | | | | | | | | | |

Sveriges Kommuner och Regioner

# Vad kommer SKR att syssla med?

Sveriges Kommuner och Regioner

# Kompetensgemenskap

- Informationssäkerhet (*pågående*)
- Cybersäkerhet (*uppstart*)
- Informationshantering (*uppstart*)
- Digitaliseringsjuridik (*uppstart*)
- AI-rådet (*pågående*)
- Arkitekturrådet (*pågående*)

# Kompetensgemenskap informationssäkerhet

- 13 representanter från kommuner och regioner
  - 4 regionrepresentanter
  - 8 kommunrepresentanter
  - Adda

- Hantera resultatet från ”kommunrapporten” och ”regionrapporten”

Sveriges Kommuner och Regioner

# Kompetensgemenskap informationssäkerhet

- Systematiskt informationssäkerhetsarbete
  - Skapa de rätta förutsättningarna
  - Tillämpning
  - Uppföljning
  - Stödmaterial
  - **Checklistor**
- Kommunikationsmaterial

# Utbildning

- KLASSA
  - Grundläggande utbildning i KLASSA (*under hösten*)
- NIS2

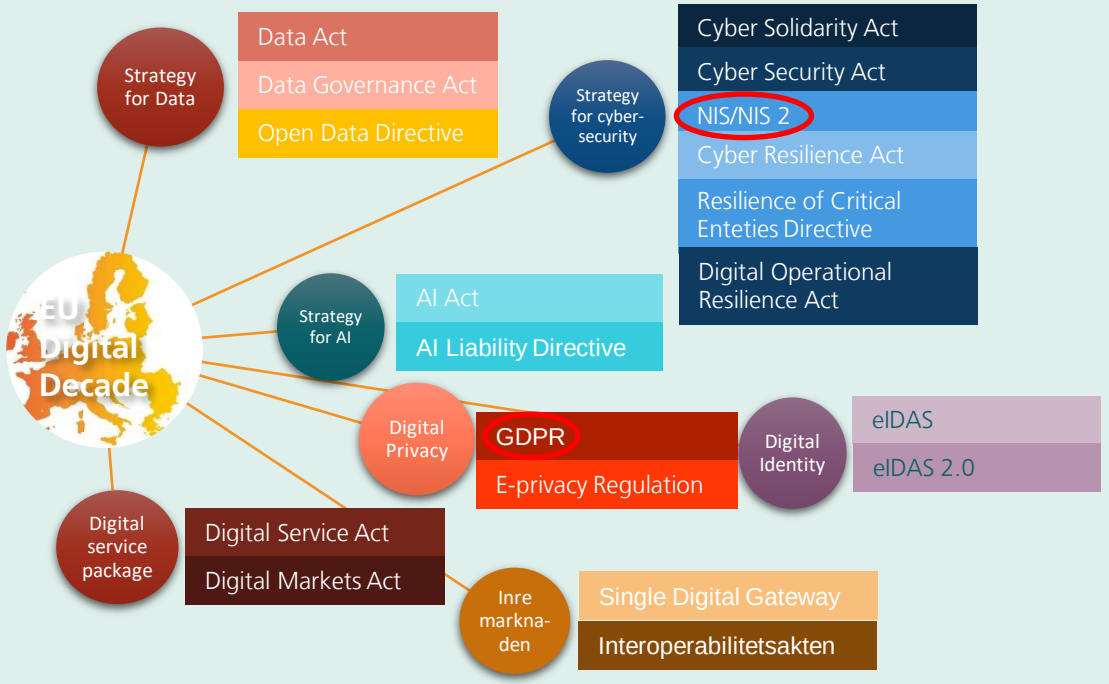
Sveriges Kommuner och Regioner

# Vad är planen framåt?

Thomas Nilsson

Sveriges Kommuner och Regioner

# Högre grad av reglering från EU



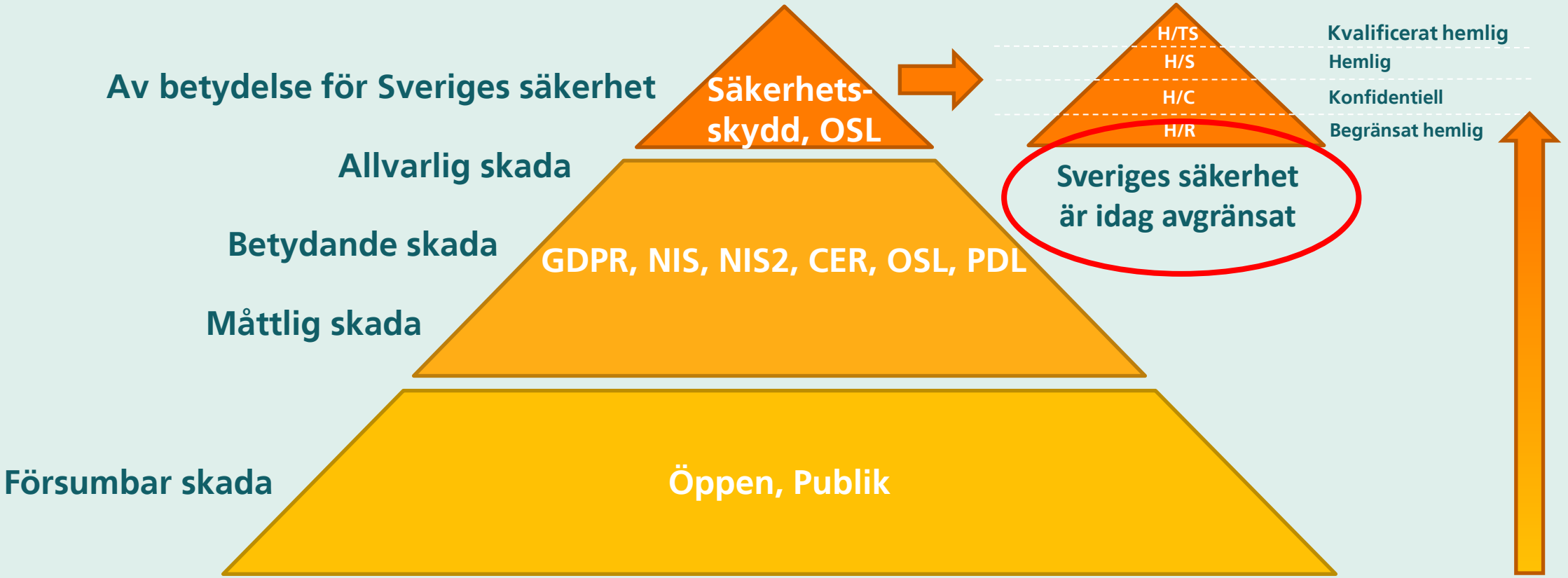

- Certifieringsordningar
- Lag med kompletterande bestämmelser
- Genomförandeakter
- Öppna data-lagen
- NIS2/CER-lag
- MSB-föreskrifter
- Lag om ändring av skadeståndslagen
- Lag om auktorisationssystem
- ”Statlig e-legitimationslag”
- Lag med kompletterande bestämmelser
- Lag med kompletterande bestämmelser
- Certifieringsordning 5G

NIS och GDPR är numera bara några exempel på regleringen av informations- och cybersäkerheten.

# Utmaningen med regleringen

- GDPR, eIDAS 2, NIS2, DORA, CER, AI-akten….
  - Krav på riskhantering och systematiskt informationssäkerhetsarbete
    - Olika fokus för riskanalyserna
  - Specifika krav på tillvägagångssätt
  - Rätt tekniska och organisatoriska skyddsåtgärder över tid
- Nationell lagstiftning
  - Säkerhetsskydd/OSL
    - Säkerhetspolisens vägledningar
- Orimligt att varje lagrum beaktas i en isolerad silo
  - Gränsöverskridande riskhantering och systematiskt informationssäkerhetsarbete

# Det finns även behov av ny verkshöjd



Sveriges Kommuner och Regioner

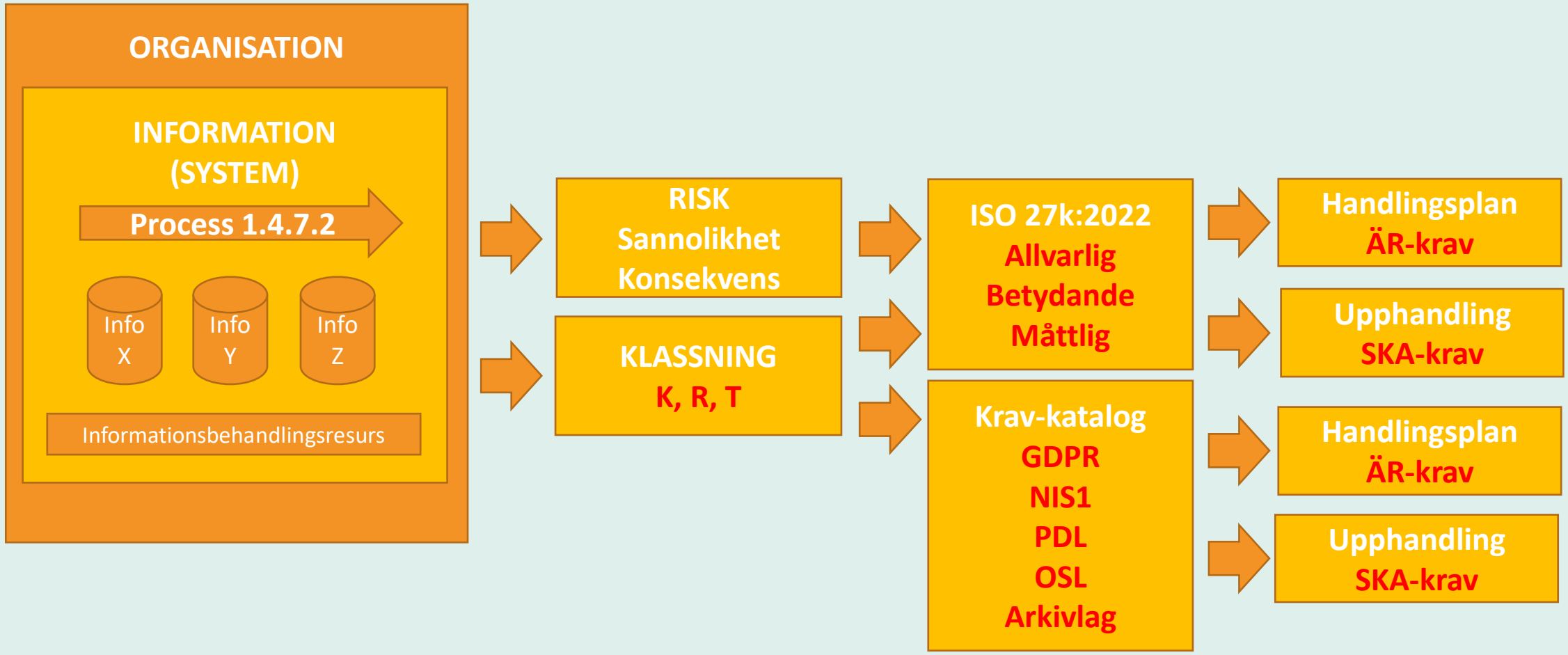
# Problembilden

Idag fångas externa krav på ett simplistiskt sätt, vilket lämnar en del avgränsningar och bedömningar som görs utanför KLASSA.

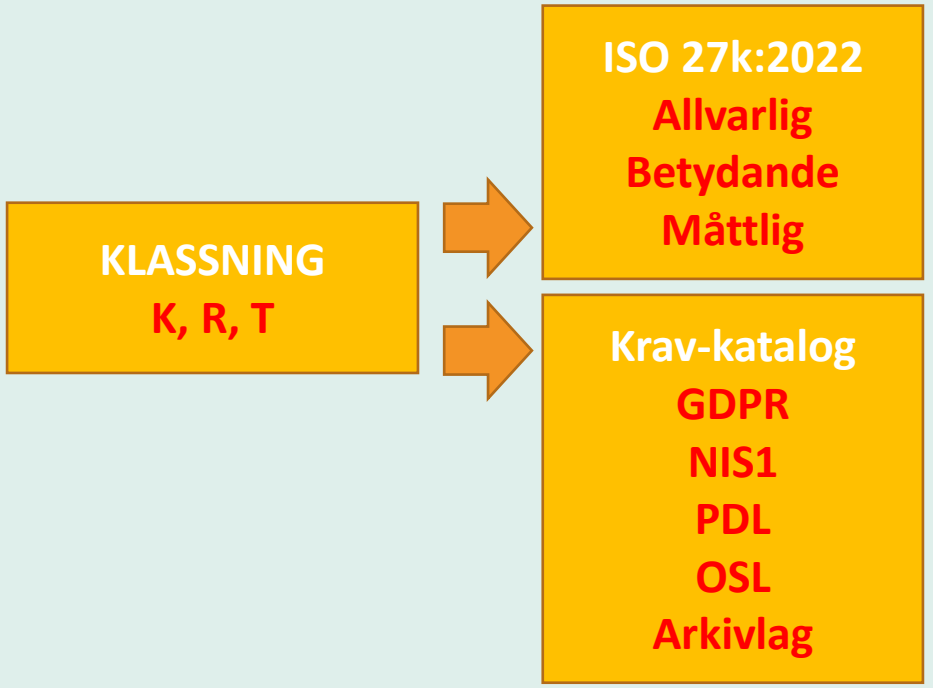
Idag utelämnas organisationens egna bedömningar om hot & risker.

KLASSA guidar inte organisationen genom alla de frågeställningar som de behöver ta ställning till.

# Dagens KLASSA (v4)



# KLASSA (v4) – Kärnan i metodstödet



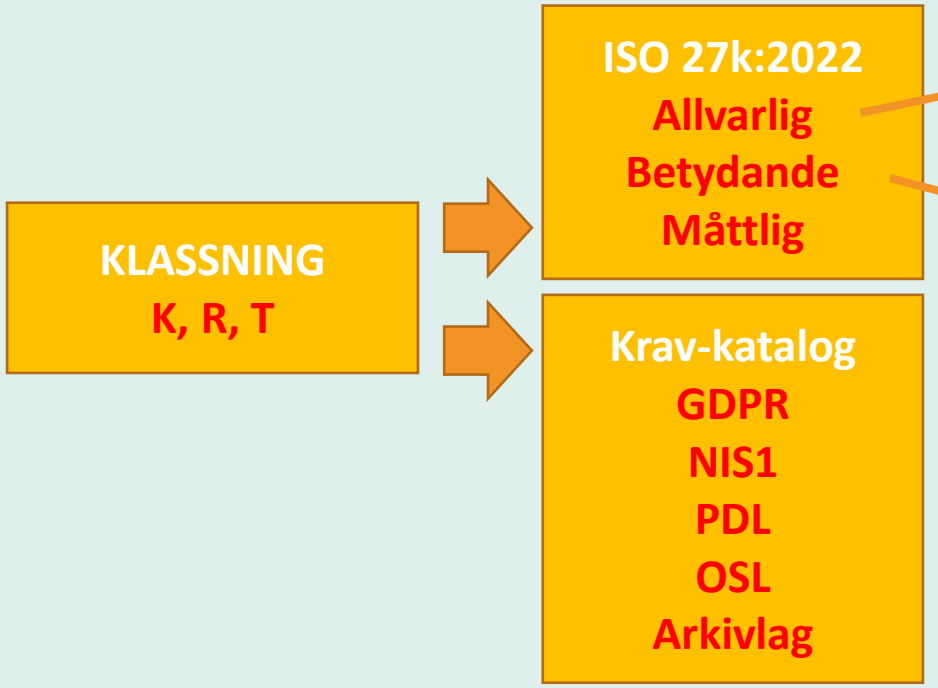
# KLASSA (v4) – Ett praktiskt exempel

**VÄGLEDNING**

**GDPR känslig personuppgift**
**K=Allvarlig, R=Allvarlig**

**GDPR personuppgift**
**K=Betydande, R=Betydande**

**NIS1 samhällsviktig process**
**K=Allvarlig, R=Allvarlig**




Exempel på autentiseringskrav:

- Autentisering tillitsnivå 3
- Autentisering tillitsnivå 2

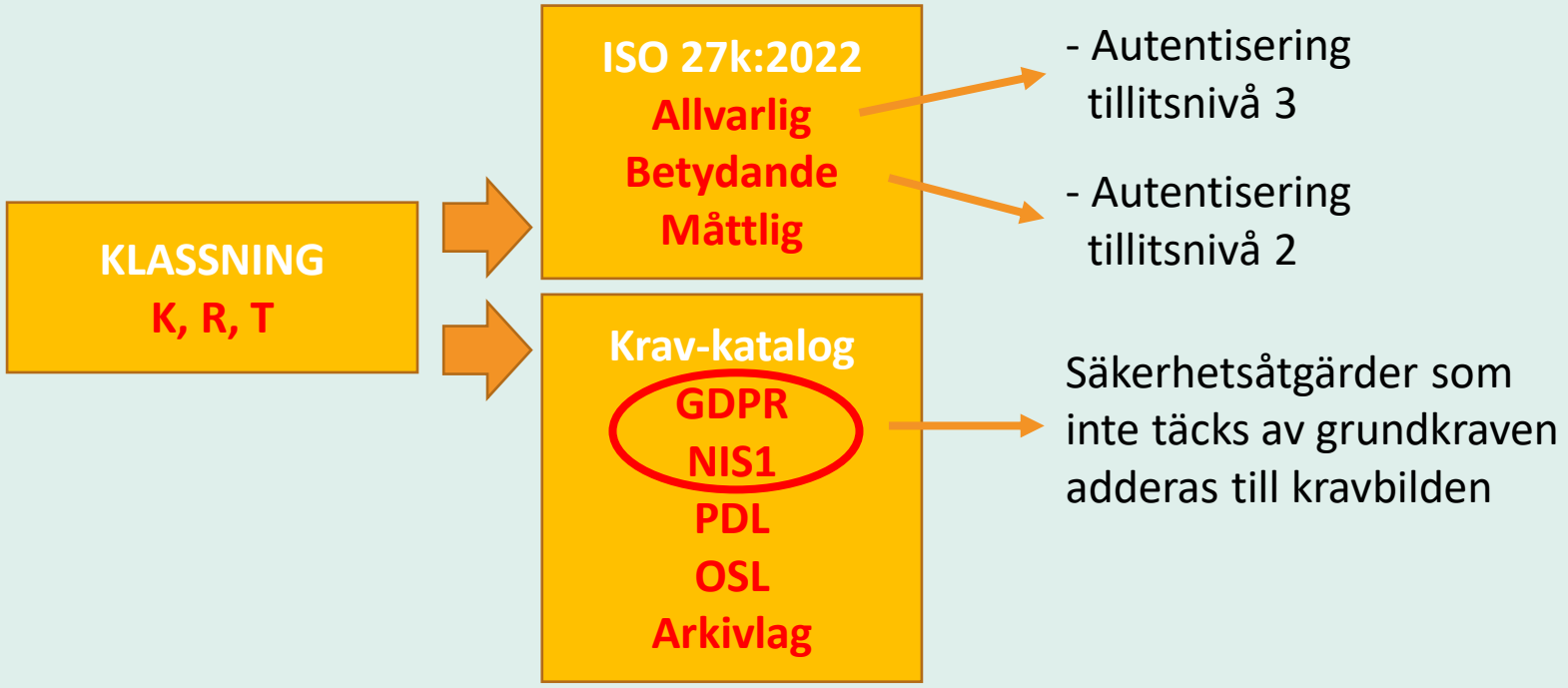
# KLASSA (v4) – Ett praktiskt exempel

**VÄGLEDNING**

**GDPR känslig personuppgift**
**K=Allvarlig, R=Allvarlig**

**GDPR personuppgift**
**K=Betydande, R=Betydande**

**NIS1 samhällsviktig process**
**K=Allvarlig, R=Allvarlig**

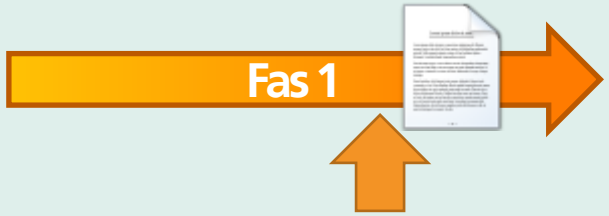


# Vinnova – Gemensamma kravkataloger

- Ett Vinnovafinansierat projekt i fyra faser (hösten 2023 - våren 2025)

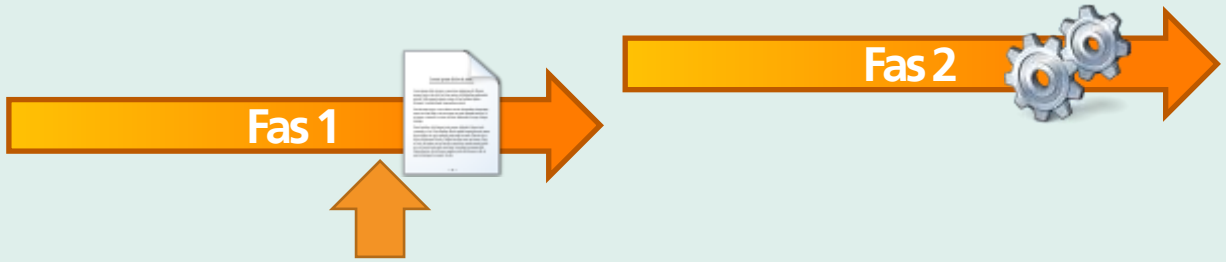
# Vinnova – Gemensamma kravkataloger

- Ett Vinnovafinansierat projekt i fyra faser (hösten 2023 - våren 2025)
  - Fas 1 – Beskriva nuläget och ge förslag på väg fram med en tydlig målbild
    - Lagrum, klassning, konsekvensnivåer, kravkataloger, samverkan, avgränsningar mm



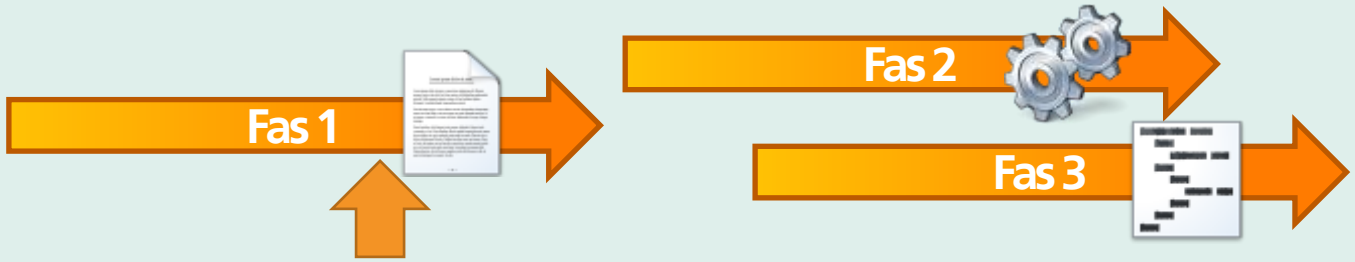
# Vinnova – Gemensamma kravkataloger

- Ett Vinnovafinansierat projekt i fyra faser (hösten 2023 - våren 2025)
  - Fas 1 – Beskriva nuläget och ge förslag på väg fram med en tydlig målbild
    - Lagrum, klassning, konsekvensnivåer, kravkataloger, samverkan, avgränsningar mm
  - Fas 2 – Realisera de föreslagna vägen fram för att nå målbilden
    - Metodik, djup/bredd på kravkataloger, samverkan, avgränsningar mm



# Vinnova – Gemensamma kravkataloger

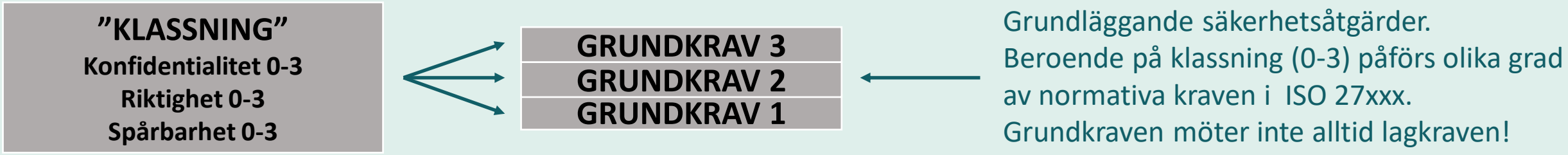
- Ett Vinnovafinansierat projekt i fyra faser (hösten 2023 - våren 2025)
  - Fas 1 – Beskriva nuläget och ge förslag på väg fram med en tydlig målbild
    - Lagrum, klassning, konsekvensnivåer, kravkataloger, samverkan, avgränsningar mm
  - Fas 2 – Realisera de föreslagna vägen fram för att nå målbilden
    - Metodik, djup/bredd på kravkataloger, samverkan, avgränsningar mm
  - Fas 3 – Vidareutveckla KLASSA (v5) för att möta den nya målbilden



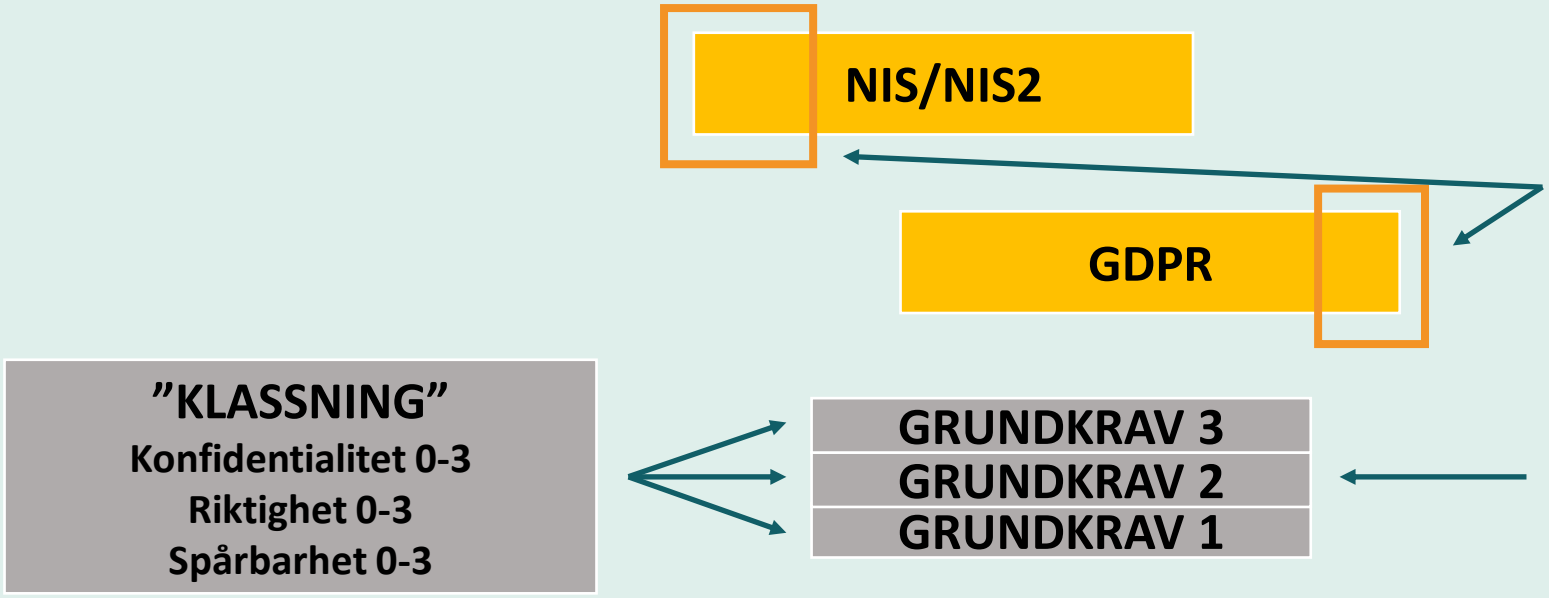
# Vinnova – Gemensamma kravkataloger

- Ett Vinnovafinansierat projekt i fyra faser (hösten 2023 - våren 2025)
  - Fas 1 – Beskriva nuläget och ge förslag på väg fram med en tydlig målbild
    - Lagrum, klassning, konsekvensnivåer, kravkataloger, samverkan, avgränsningar mm
  - Fas 2 – Realisera de föreslagna vägen fram för att nå målbilden
    - Metodik, djup/bredd på kravkataloger, samverkan, avgränsningar mm
  - Fas 3 – Vidareutveckla KLASSA (v5) för att möta den nya målbilden
  - Fas 4 – Med Fas 2 och Fas 3 i ryggen genomföra piloter

# Fas 1 – Allra först ”Lagrum vs Grundkrav”



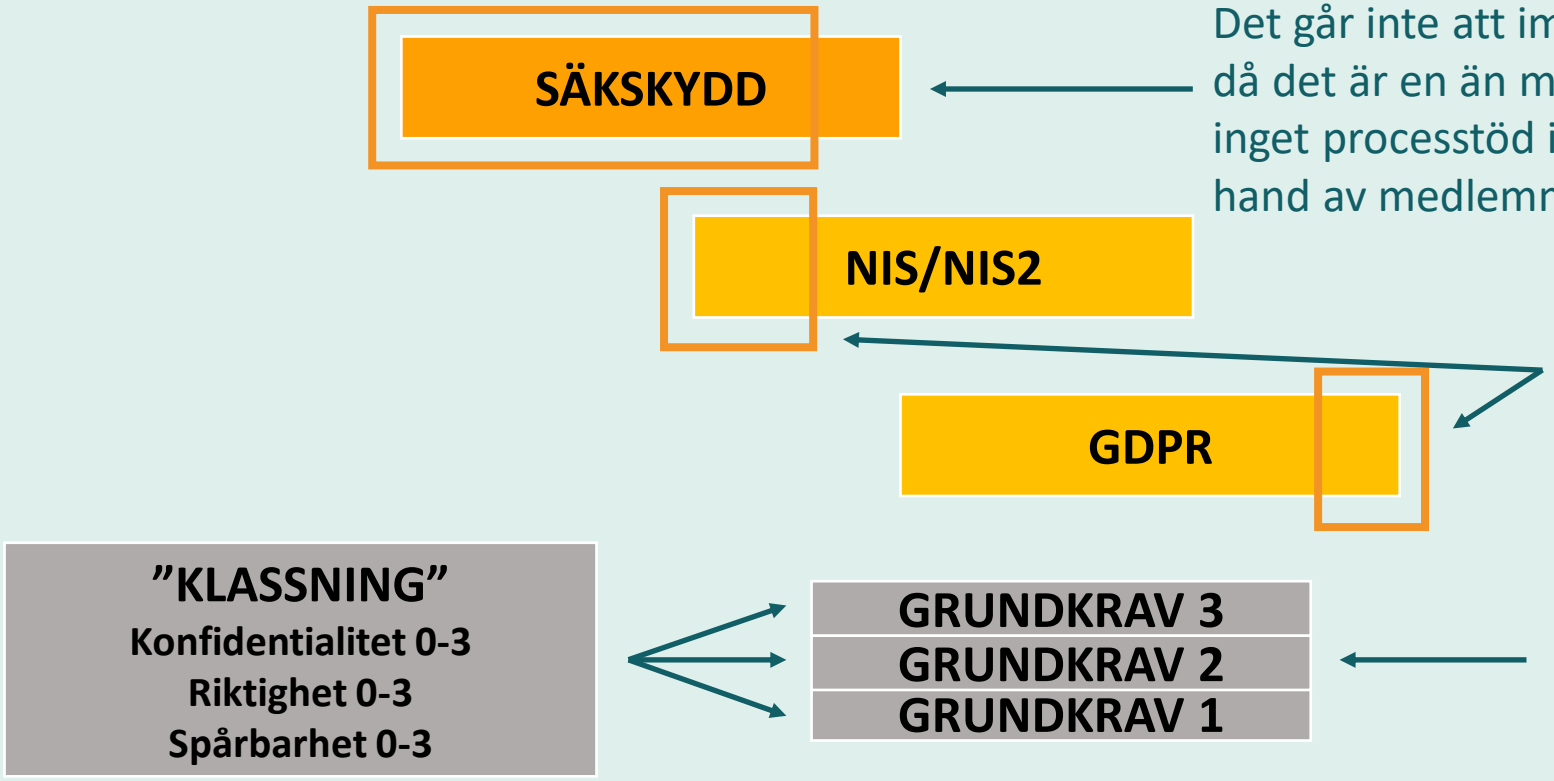
# Fas 1 – Allra först ”Lagrum vs Grundkrav”




I GDPR/NIS påförs säkerhetsåtgärder.
Dock få tydliga säkerhetsåtgärder i lag.
Olika föreskrifter för olika verksamheter.

Grundläggande säkerhetsåtgärder.
Beroende på klassning (0-3) påförs olika grad av normativa kraven i ISO 27xxx.
Grundkraven möter inte alltid lagkraven!

# Fas 1 – Allra först ”Lagrum vs Grundkrav”



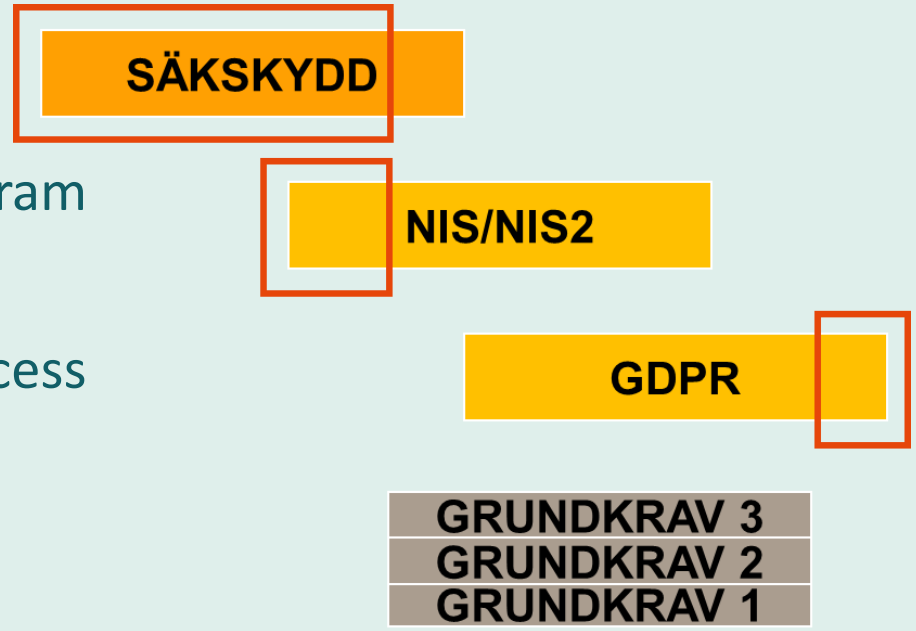

Säkerhetsskyddskrav finns inte i KLASSA idag.
Det går inte att implementera säkerhetsskydd likt GDPR/NIS då det är en än mer strikt lagstyrd process. Det finns heller inget processtöd i KLASSA för GDPR/NIS utan det görs för hand av medlemmarna.

I GDPR/NIS påförs säkerhetsåtgärder.
Dock få tydliga säkerhetsåtgärder i lag.
Olika föreskrifter för olika verksamheter.

Grundläggande säkerhetsåtgärder.
Beroende på klassning (0-3) påförs olika grad av normativa kraven i ISO 27xxx.
Grundkraven möter inte alltid lagkraven!

# Fas 1 – Allra först ”Lagrum vs Grundkrav”

- Vem ska kompletterar vem framgent?
  - Idag är de regulatoriska kraven kompletterande
  - Givet allt mer omfattande reglering är det inte en väg fram
- Behov av bättre metodstöd kring varje reglering
  - Varje lagrum har oavsett metodstödet sin uttalade process
- Vilka regulatoriska krav ska omfamnas?
  - Säkskydd, NIS2/CER, AI-akten, GDPR, LEK…



Sveriges Kommuner och Regioner

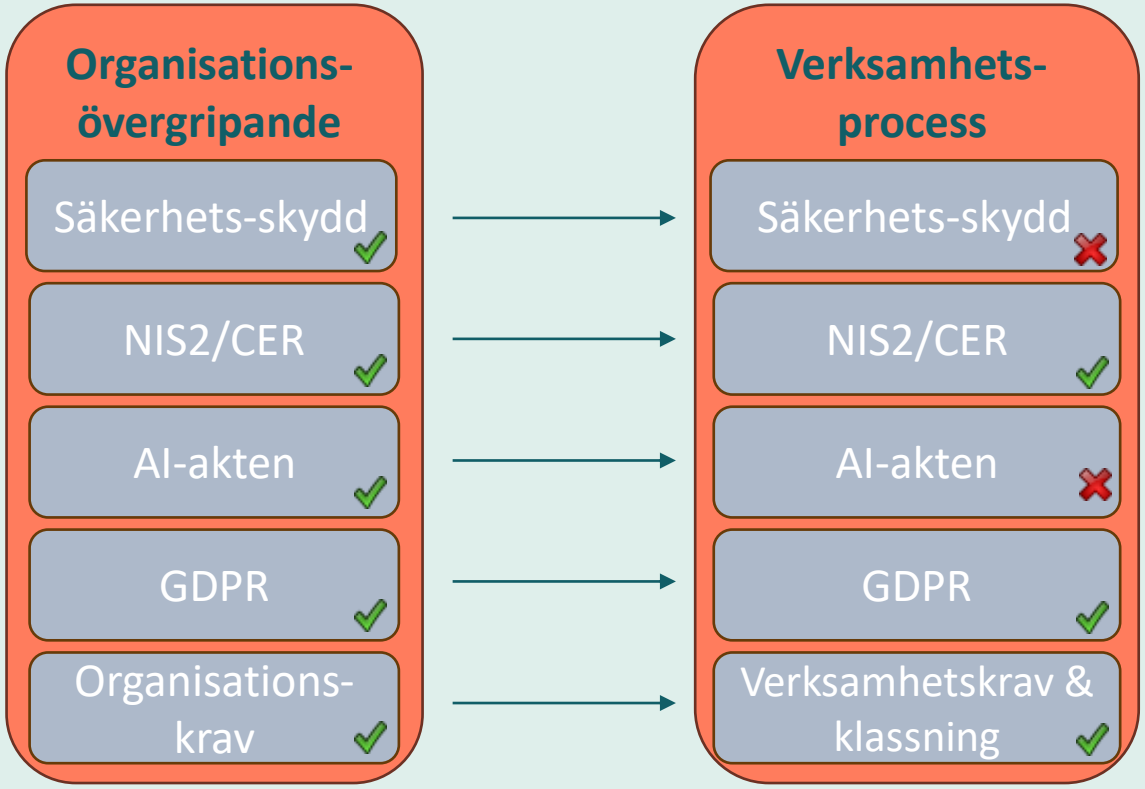
# Fas 1 - Vägen fram?

Externa och interna krav på organisationen ska fångas upp i KLASSA utifrån regulatoriska krav.

Varje regulatoriskt krav hanteras genom en process som organisationen guidas genom vilket leder fram till krav på säkerhetsåtgärder.

Processerna interagerar med varandra och utgår från ett  övergripande förarbete.

# Fas 1 – Förslaget till väg fram

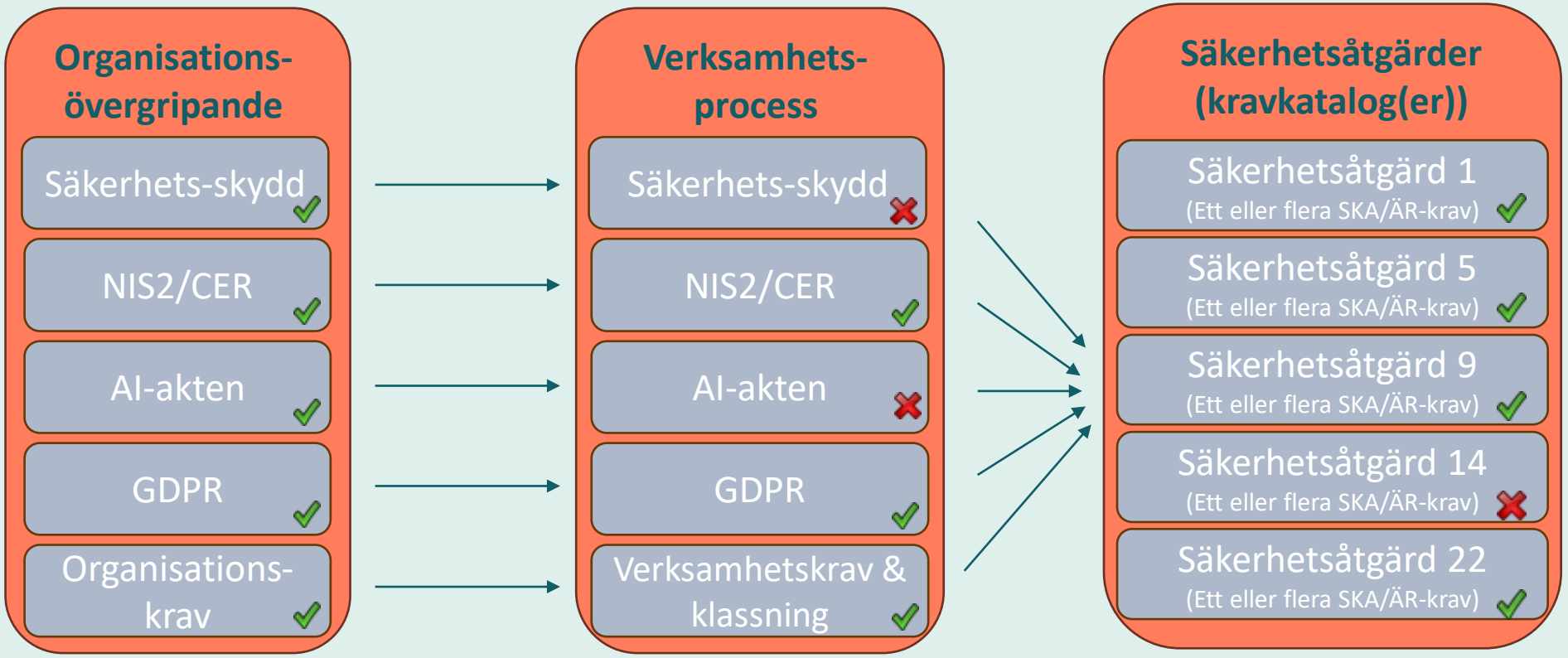



Stöd i det övergripande arbetet i organisationen

Stöd i analysen av verksamhetsprocessen

Mål: Att minimera arbetet som görs i verksamheten och i möjligaste mån lägga grunden för säkerhetsarbetet på en övergripande nivå.

# Fas 1 – Förslaget till väg fram



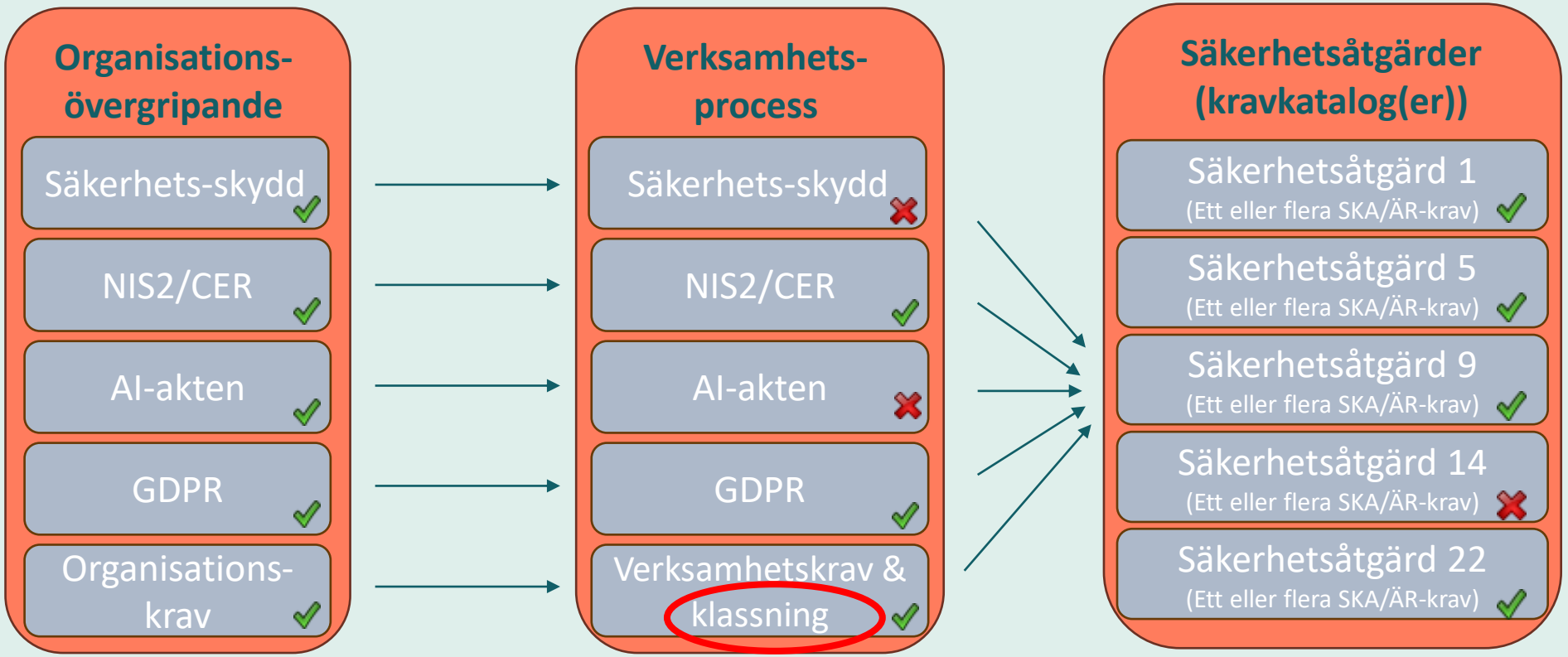

Stöd i det övergripande arbetet i organisationen

Stöd i analysen av verksamhetsprocessen

Handlingsplan och kravunderlag

Mål: Att de tekniska och organisatoriska säkerhetsåtgärderna möter lagstiftarens och verksamhetens krav över tid.

# Fas 1 – Förslaget till väg fram



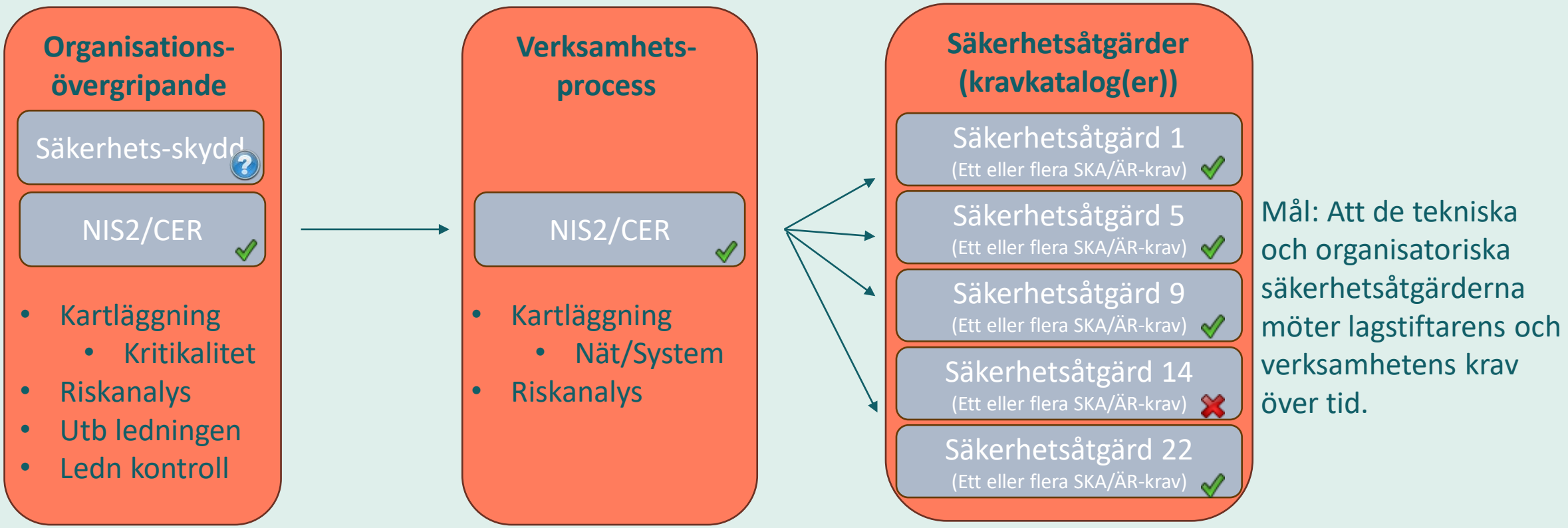

Klassningen kan fortsatt styra vilka säkerhetsåtgärder som påförs, men det är valfritt då det inte är tillräckligt rättssäkert längre!

Stöd i det övergripande arbetet i organisationen

Stöd i analysen av verksamhetsprocessen

Handlingsplan och kravunderlag

# Fas 1 – Exemplet ”NIS2/CER”



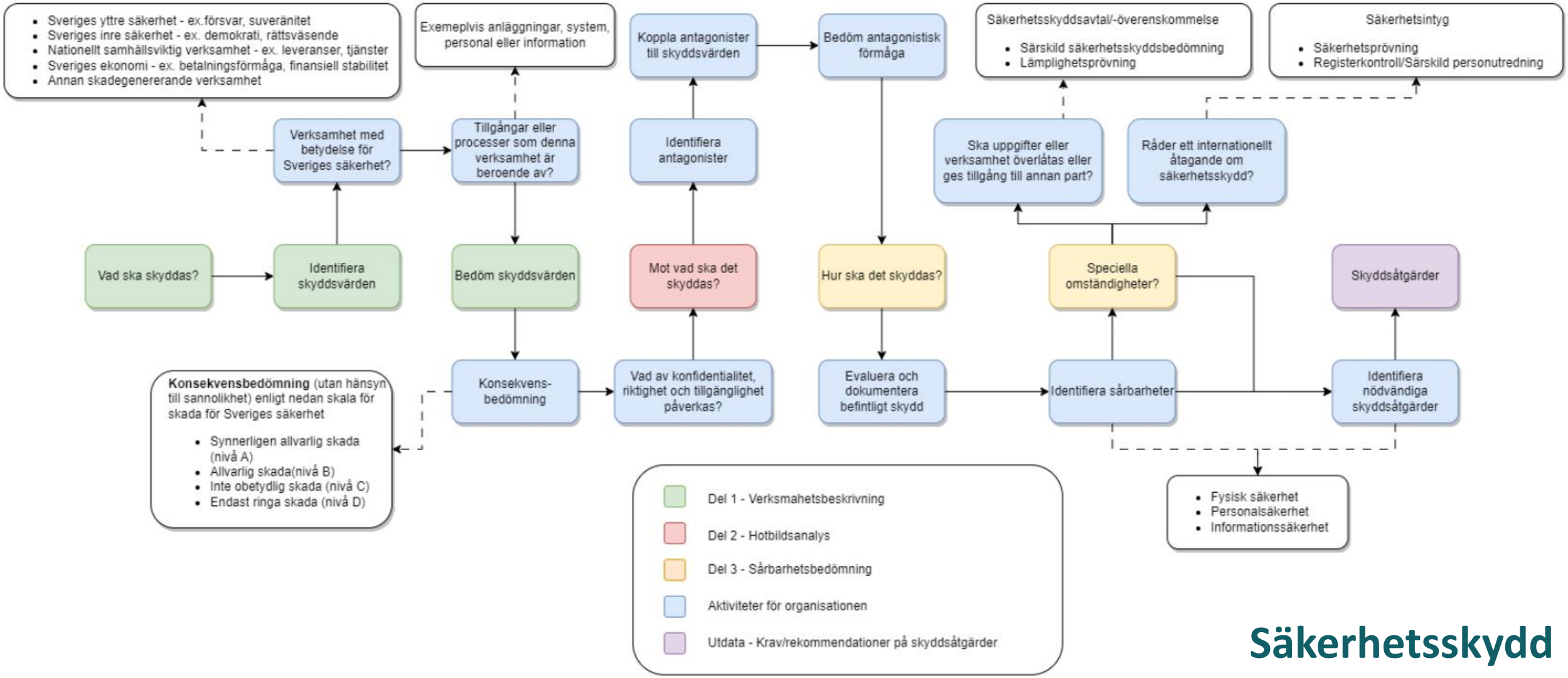

Mål: Att de tekniska och organisatoriska säkerhetsåtgärderna möter lagstiftarens och verksamhetens krav över tid.

Stöd i det övergripande arbetet i organisationen

Stöd i analysen av verksamhetsprocessen

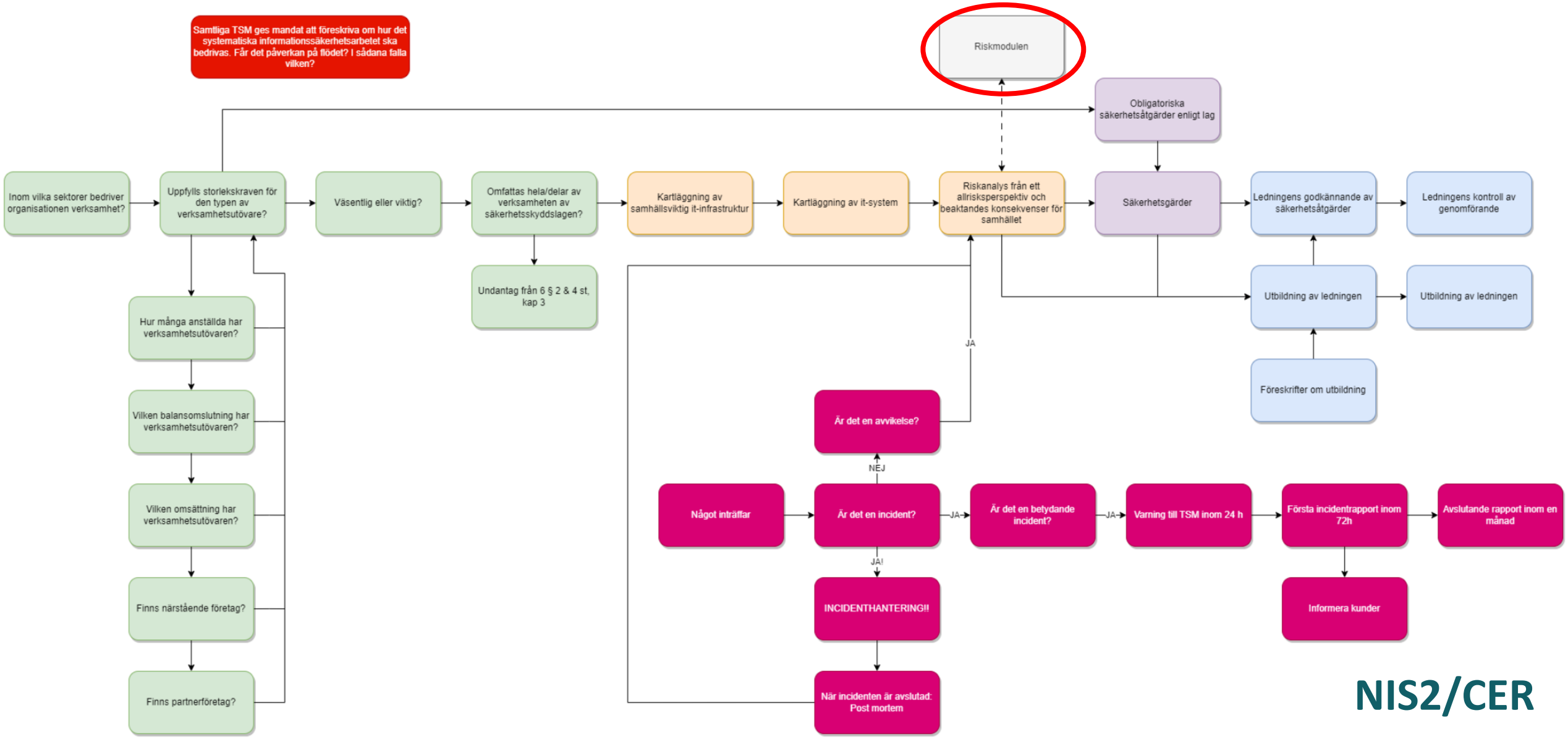
Handlingsplan och kravunderlag

Sveriges Kommuner och Regioner




# Säkerhetsskydd

Sveriges Kommuner och Regioner

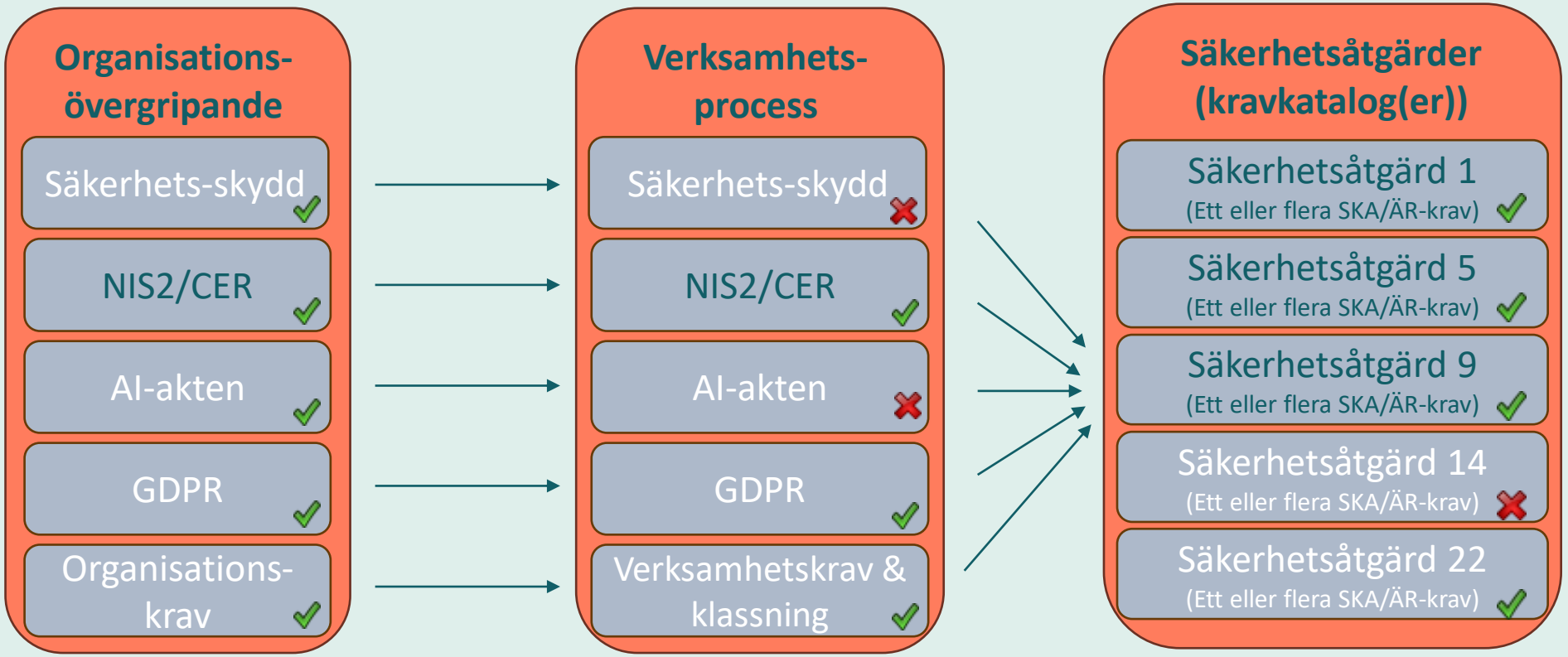



NIS2/CER

# Fas 1 – Cybersäkerhetslag (SOU 2024:18)

- Kommuner och regioner kommer sannolikt att omfattas av förslaget till cybersäkerhetslag
  - För att de är kommuner eller regioner, och inte bara för att de har en viss tjänst.
- Hela verksamheten, med få undantag, omfattas av cybersäkerhetslagens krav
  - Inte som i dagens NIS-lag där kraven ska tillämpas på "de nätverks- och informationssystem som används för att tillhandahålla tjänsten".
  - Givetvis trumfar säkerhetsskyddet som tidigare!
- Tillsynsmyndigheterna (11 st!) får föreskriva om riskhanteringsåtgärder, systematiskt informationssäkerhetsarbete och cybersäkerhetsutbildning.
- Ett förslag till väg fram är att CER/NIS2 utgör grunden för kravkatalogen i KLASSA
  - Dagens SS-ISO/IEC 27001/2-baserade struktur ersätts, men referenserna till ISO 27k-standarden normativa krav kvarstår, likväl som referenser till andra ramverk.

# Fas 1 – NIS2/CER som grundkatalog?




Handlingsplan och kravunderlag

Mål: Att möta risk-hanteringsåtgärder som följer av NIS2-direktivet artikel 21.

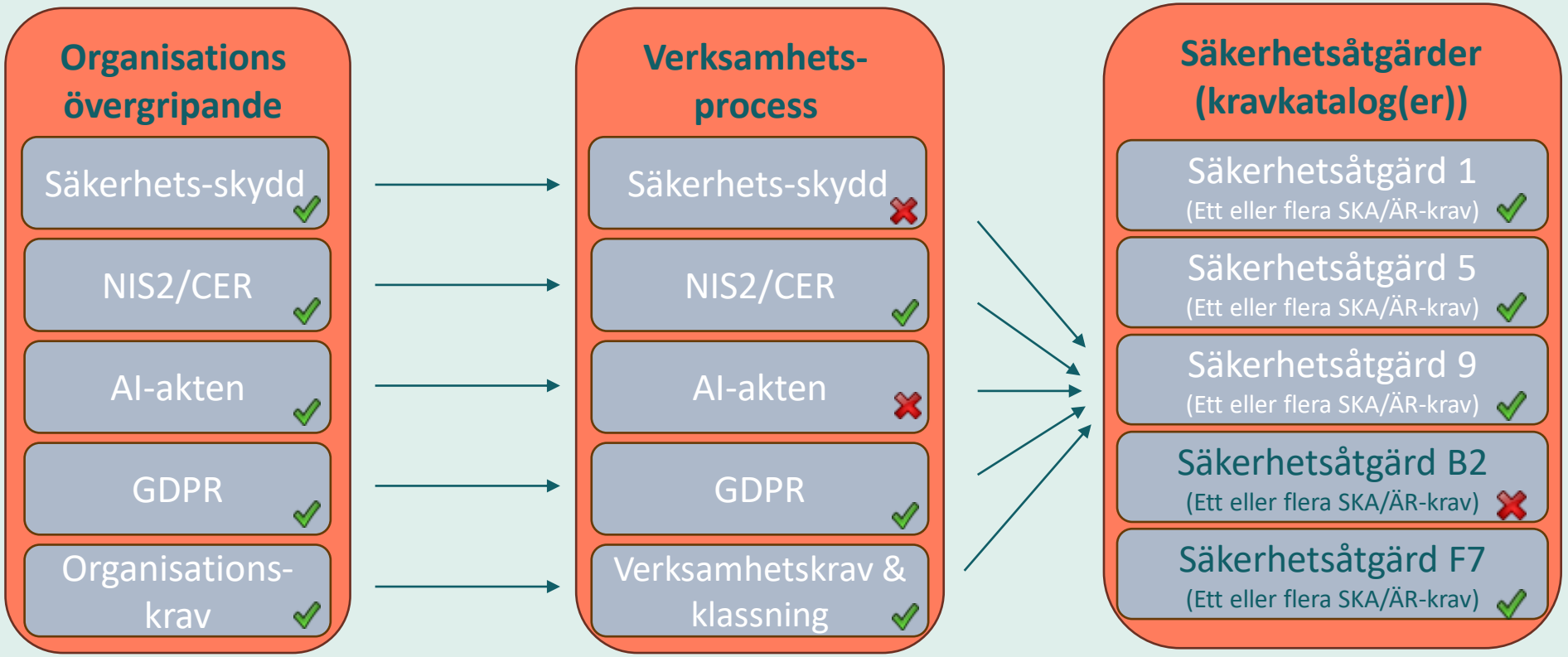
# Fas 1 – Riskhanteringsåtgärder enl art 21

- Riskhantering
- Systemsäkerhet
- Incidenthantering
- Driftskontinuitet
- Säkerhet i leveranskedjor
- Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem
- Förmåga att bedöma effektiviteten i vidtagna åtgärder
- Cyberhygien och utbildning i cybersäkerhet
- Användning av kryptografi och krypto
- Personalsäkerhet, åtkomstkontroll och tillgångsförvaltning
- Användning av lösningar för multifaktorautentisering

# Fas 1 – Riskhanteringsåtgärder enl art 21 (ex)

- Riskhantering
- Systemsäkerhet
- Incidenthantering
  - *Ansvar, rutiner, kontaktvägar och kommunikationsplaner vid informationssäkerhetsincidenter finns dokumenterat och är kommunicerat. (Ref ISO 27k 5.24)*
- Driftskontinuitet
- Säkerhet i leveranskedjor
- Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem
- Förmåga att bedöma effektiviteten i vidtagna åtgärder
- Cyberhygien och utbildning i cybersäkerhet
- Användning av kryptografi och krypto
- Personalsäkerhet, åtkomstkontroll och tillgångsförvaltning
- Användning av lösningar för multifaktorautentisering

# Fas 1 – Stöd för flera kravkataloger

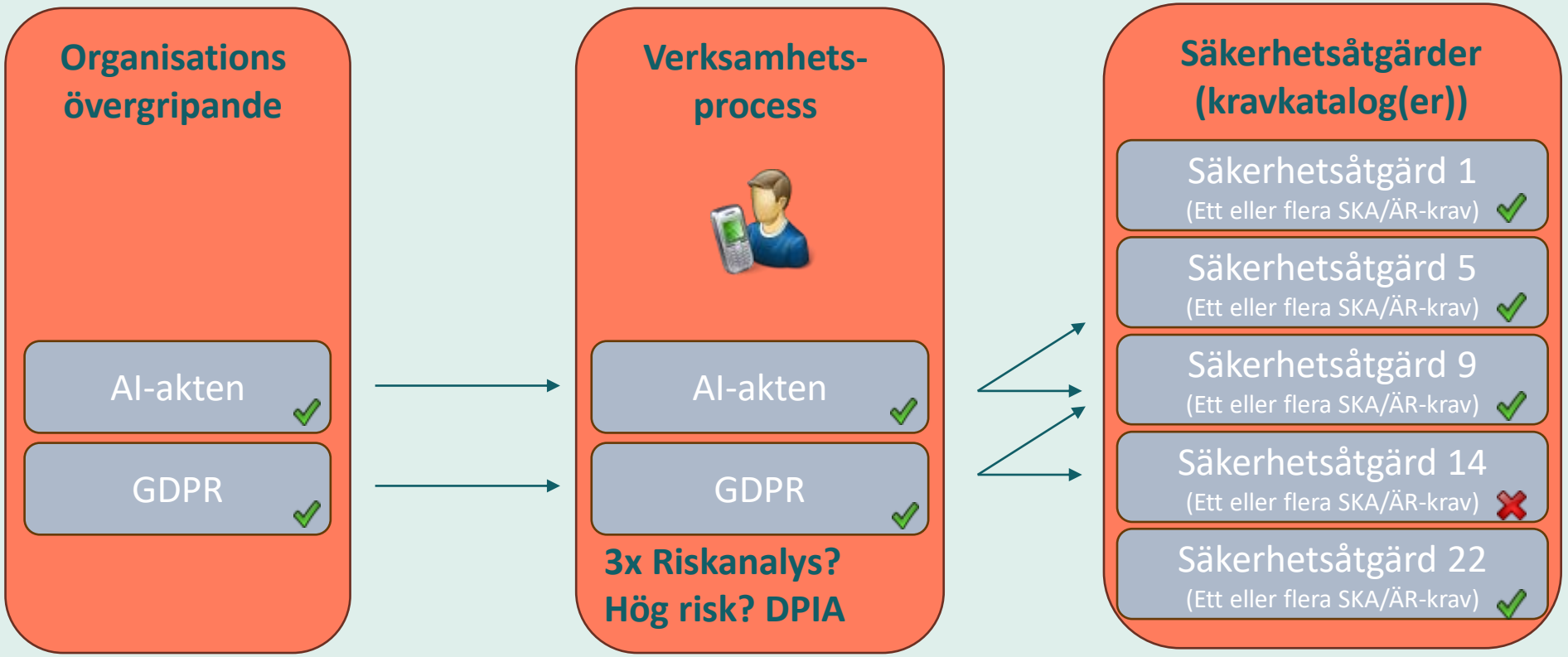



Mål:

Stöd att addera sektorspecifika krav ex SSNF:s IoT-krav

Stöd att addera egna detaljerade krav

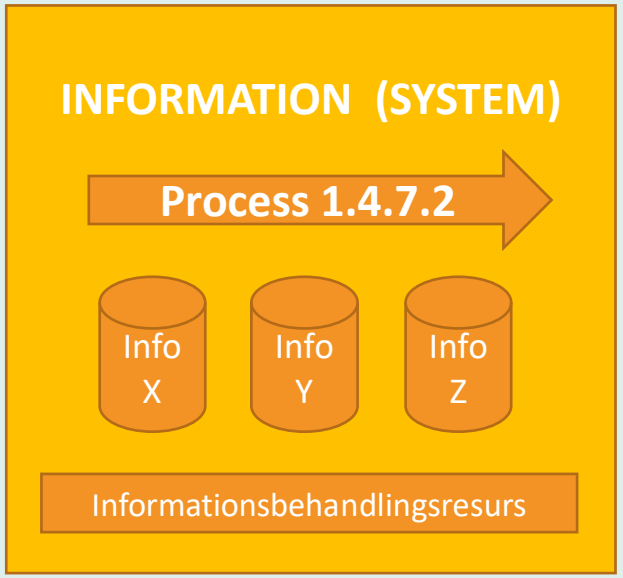
# Fas 1 – Fler exempel ”AI & GDPR”



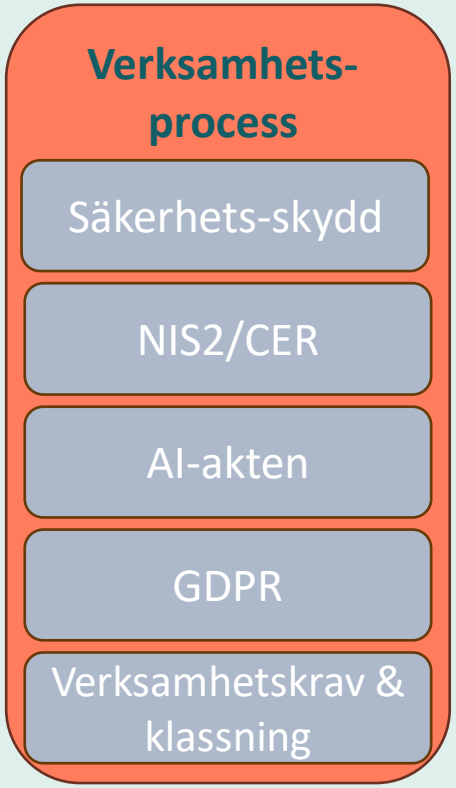

AI i mobilen för socialsekreteraren

Handlingsplan och kravunderlag

# Fas 1 – Verksamhetsprocessorienterat




Förstärker bilden av ett processorienterat förhållningssätt.



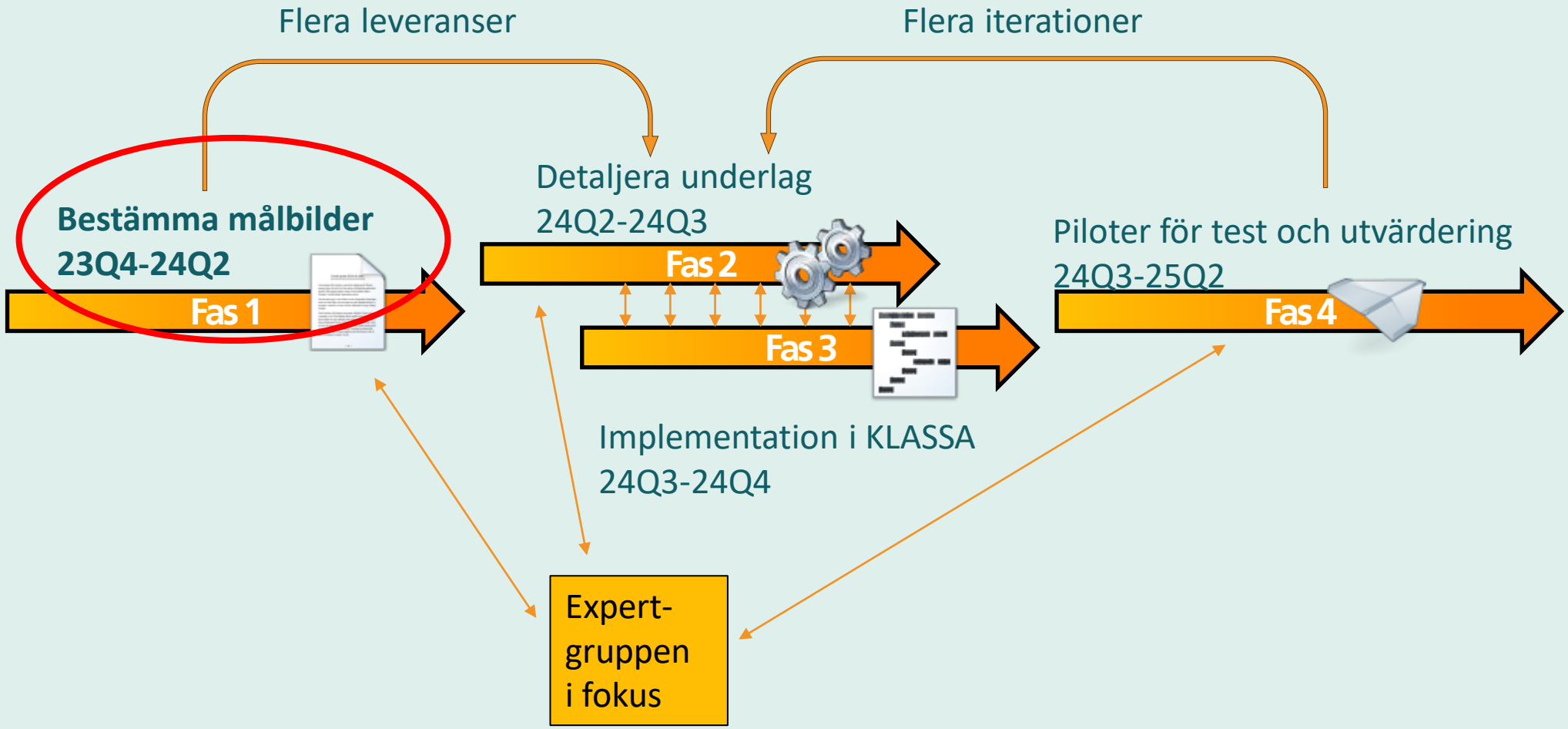

Stöd i analysen av verksamhetsprocessen

Mål:

Att i möjligaste mån stötta det verksamhets-processorienterade arbetssättet med stöd för processorienterad informationskartläggning (POIK).

Att interagera med befintliga verktyg samt att erbjuda enklare stöd i KLASSA för POIK

# Relationerna fas 1-4



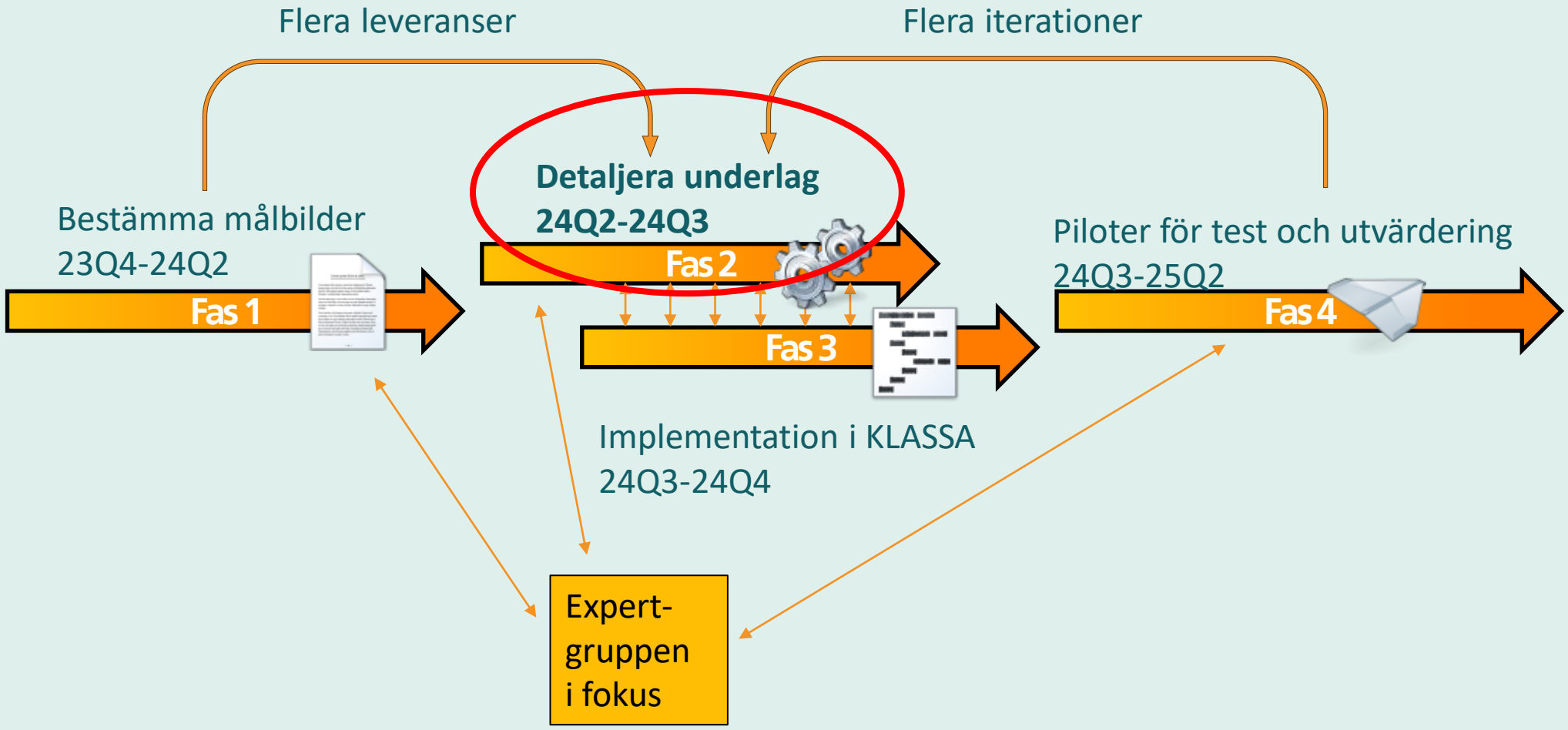
# Fas 1 – Klart

- Kartläggning av kravkataloglandskapet
- Utredning av relationen lagrum vs krav
- Processexempel för Säkskydd, NIS2, GPDR, AI-akten
- Ett faktiskt exempel med GDPR och AI-akten
  - AI i mobilen för  socialsekreteraren
- Kartläggning av regulatoriska krav på ”klassning”
  - Arkivklassificering, informationsklassning, säkerhetsskyddsklassificering…
- Förslag på väg fram för federerad inloggning (SAML och ev OIDC)

# Fas 1 – Kvarstående

- Grundkravkatalog med NIS2/CER som grund
  - Utgå från befintlig kravkatalog som inordnas enligt NIS2 art 21
- Identifiera behovet av interaktion
  - av befintliga verktyg för POIK (ex via API)
  - av interaktion med källor för organisationsstruktur, ex katalog (via LDAP)

# Relationerna fas 1-4



# Fas 2 – Inledande

- Detaljera kravunderlag (Fas 2) för utveckling av KLASSAv5 (Fas 3)
  - Fas 1 är mer detaljerad än planerat vilket gör Fas 2 kortare/snabbare.
    - Processerna har detaljerats i högre grad än först planerat
- Identifierade behov av nya förmågor:
  - att dynamiskt utforma processer och förmåga till visualisering
    - Regulatoriska processer (Säkerhetsskydd, NIS2, AI, GPDR mfl)
    - Verksamhetsprocesser (POIK)
  - att extrahera information för olika ändamål
    - Incidentunderlag, registerförteckning, behandlingar, informationshanteringsplaner etc

Sveriges Kommuner och Regioner

# Lunchpaus till 13:00

Sveriges Kommuner och Regioner

# Gruppdiskussion

Mentikod: 14 01 53 16

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Är det rätt väg att gå, d.v.s. att ändra strukturen på kravkatalogen från ett ISO-perspektiv till ett regelverksperspektiv?
  - Fritext

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Vilken annan funktionalitet ser ni att KLASSA bör erbjuda?
  - Fritext

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Vilka funktionaliteter är mest prioriterade i KLASSA?
  - Incidenthanteringsmodul (likt riskmodul)
  - Mognadsmätning (”infosäkkollen”)
  - Processorienterad informationskartläggning (POIK)
  - Rapportmodul
  - Stöd för kontinuitetsplanering
  - Stöd för säkerhetsskyddsanalys

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Vilken funktionalitet, i KLASSA 4.0, vill ni ändra på?
  - Exempel:
    - Vill kunna ändra namn på en informationstillgång
    - Vill kunna ta bort en skapad informationstillgång

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Tänker vi rätt kring riskhanteringsmodulen, är det rätt sätt att generera hot?
    - Hotaktör
    - Hoteffekt
    - Hotkälla

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Tänker vi rätt kring riskhanteringsmodulen, är det rätt sätt att bedöma sannolikhet och konsekvens?
    - Min
    - Mest troligt
    - Max

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Vilka rapporter vill ni kunna generera från KLASSA?

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Vilka integrationsmöjligheter önskar ni i KLASSA?

Sveriges Kommuner och Regioner

Mentikod: 14 01 53 16

# Menti-fråga

- Hur vill ni att användarträffarna arrangeras?
  - Fysiskt
  - Digitalt

Sveriges Kommuner och Regioner

# Summering

Jonas Nilsson och Thomas Nilsson

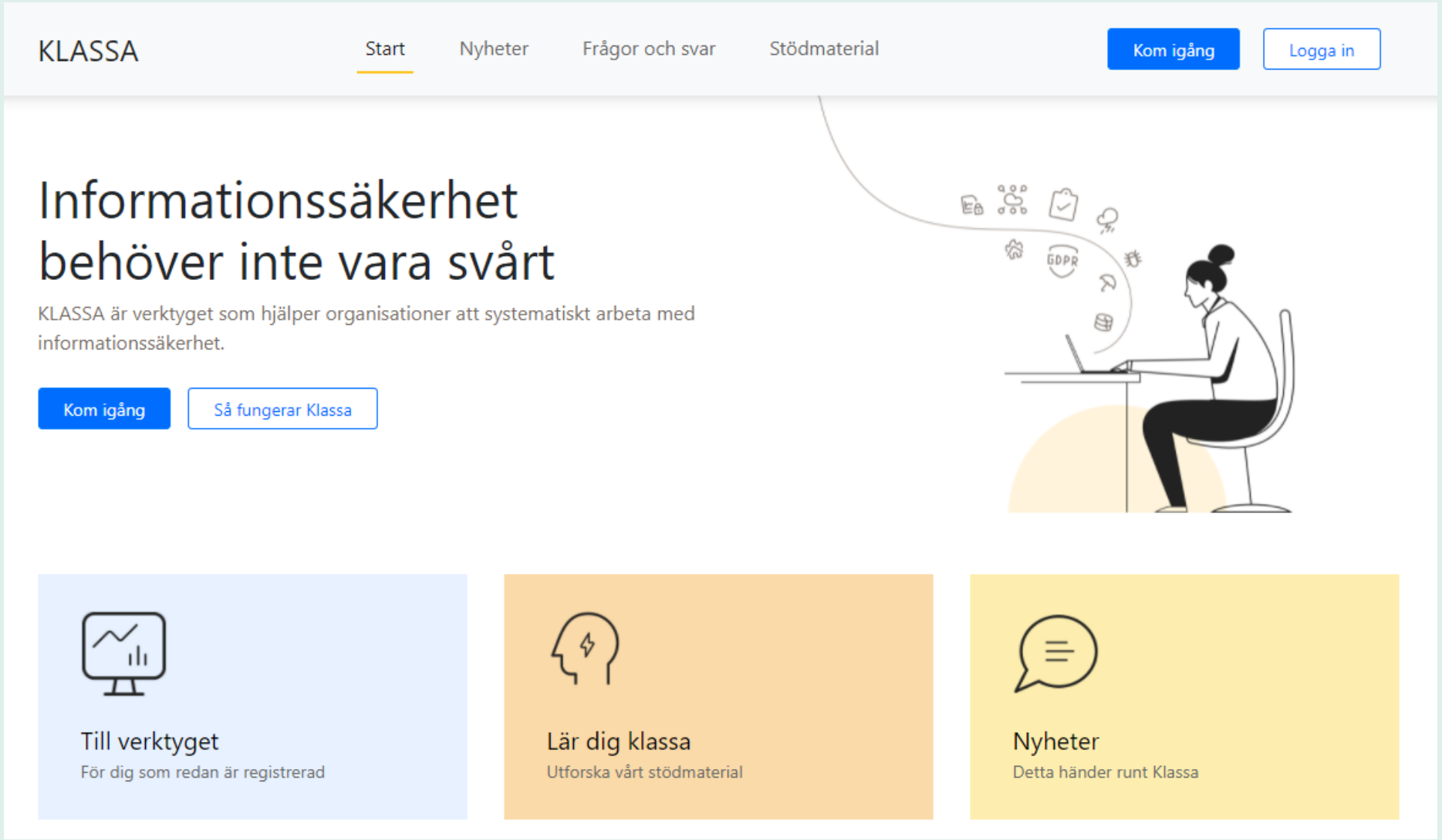
Sveriges Kommuner och Regioner

# Användarforum #6

- Nästa användarträff sker digitalt den 28 november kl 10-15

Sveriges Kommuner och Regioner

# Tack!




klassa@skr.se