ISD - IT-säkerhetsdeklaration

Information till SESAME

Dan Olofsson

PrL ISD

070- 6825904

FMV

Agenda

- Varför ISD?
- Omfattning ISD, Informationssäkerhet kontra IT-säkerhet
- Status
- Vad är ISD?

Varför ISD?

- Projekt har fallerat p.g.a. IT-säkerhetsaspekten
- Det saknar ett uttalat tekniskt designansvar för IT-säkerhet motsv. flyg- och systemsäkerhet. Det innebär:
  - Inga krav på kompetens
  - Inga krav på metodstöd
  - Inga krav på styrande processer
  - Inga krav på ansvar
  - Inga krav på uppföljning
- Det finns krav i form av FFS, FIB och KSF

FMV

Syftet med ISD

- Kostnadseffektivt och enhetligt IT-säkerhetsarbete i hela systemlivscykeln
- Att göra rätt från början
- Ökar förtroendet för FMVs leveranser
- Det ska vara enkelt att tillämpa ISD
- ISD fungerar ihop med KSF, DIT, VHL standard, ISO 27000 mm.

ISD - Integreras i och stöder…

ISD är en förutsättning för:

- FMV designansvar

ISD integreras med:

- FMV VHL och därmed SE-arbete inklusive VoV

ISD säkerställer leveranser till:

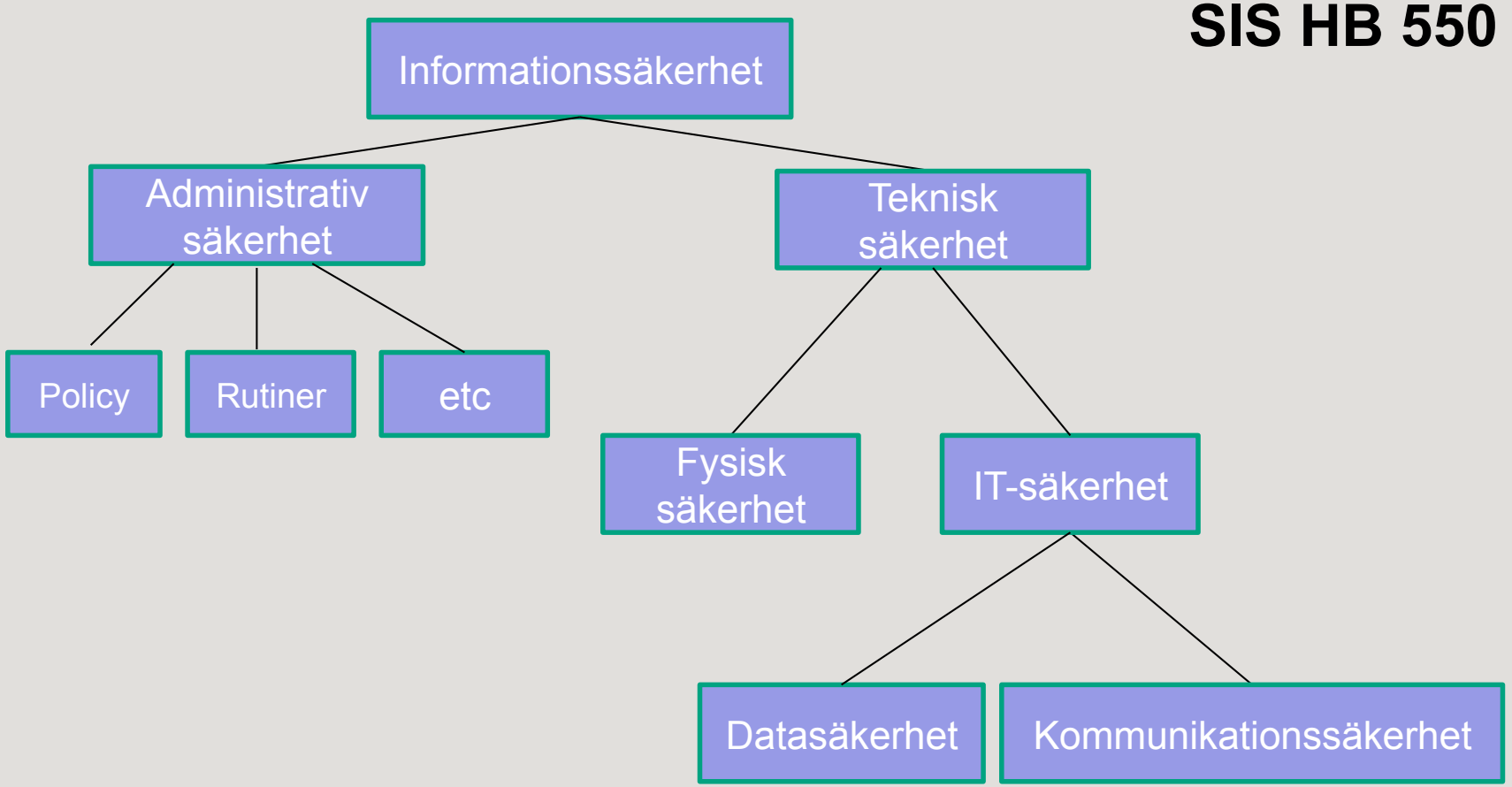
- FM Auktorisationsprocess

ISD integrerar:

- FM KSF 3.1
- FM IT-styrningsprocess

Definition Informationssäkerhet

SIS HB 550



FMV

IT-säkerhet

- Sekretess, Riktighet o Tillgänglighet (CIA)
- *Krav på säkerhetsfunktioner (KSF)*
- *Risk, Risk tolerans, Informationsvärdering*
- *Systemlivscykeln*
- *Vulnerability, oberoende granskning/värdering*
- Kan ställa krav på informationssäkerhet
- Samverkan och integration med SE
- *Styrning och uppföljning*

Krav på säkerhetsfunktioner

- Behörighetskontroll
- Säkerhetsloggning
- Intrångsskydd
- Skadlig kod
- Intrångsdetektering
- Skydd mot röjande signaler
- Skydd mot obehörig avlyssning
- Signalskydd

Risk, Risk Tolerans och Informationsvärdering

- Risk - kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad (konsekvens).
- Risk Tolerans – accepterbara gränser för risk i en organisation
- Informationsvärdering

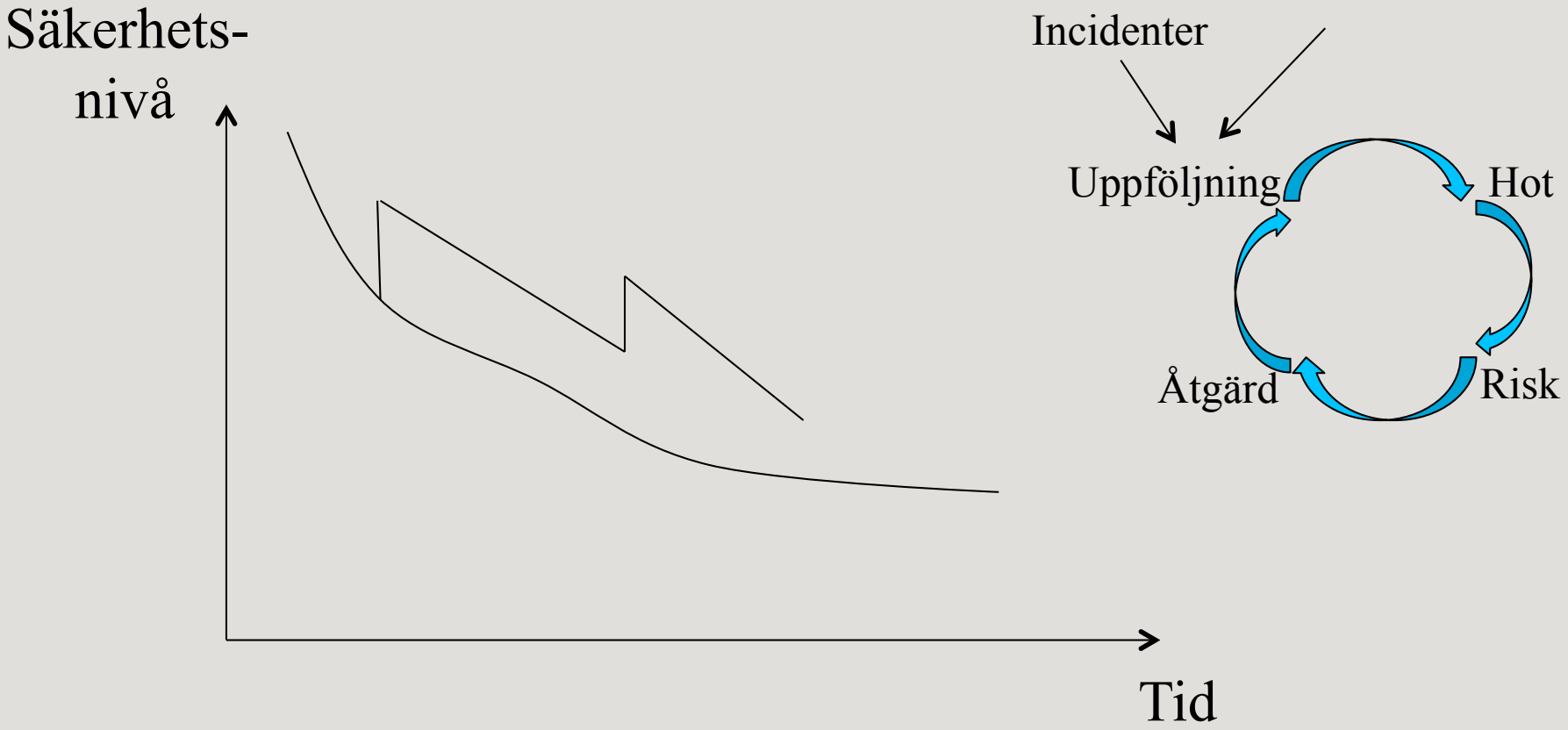
Utan dessa tre aspekter – inget effektivt system

Vulnerability

Sårbarhet – innebär brist i skyddet av en tillgång exponerad för hot – kan avse fel i ett systems säkerhetsprocedurer, design, implementering eller interna kontroller.

FMVs tekniska designansvar

Säkerhetsnivå över tiden



Systemlivscykeln

Definition:

- Utveckling
- Anskaffning
- Förvaltning/vidmakthållande
- Avveckling

Systemledningens ISD-plan beskriver strategi för IT-säkerhetsarbete.

Status ISD 2.0

- Förankrat hos FM, infört i SAMO
- Infört i FMV VHL
- Beslut av Teknisk Direktör att alla IT-system ska följa ISD-processen fr.o.m 2014-04-01.
- Utbildning genomförs på FMV – FM MUST, FM CIO, FM MSA och FM KFA är välkomna.
- ISD utvärderas och uppdateras kontinuerligt
- FM kan använda befintligt ramavtal ISD
- Exempel på projekt som använder processen är:
  - JAS, StriC, Sweccis, Marina stödsystem, IFS Radar, SatKom, IP ATL, BMS

Vad är ISD?

- Metodstöd
- Process
- Systemgranskningsledare
- Deklaration

Metodstöd

- Förutsättning för FMVs teknisk designansvar:
  - FM behov och användning
  - Tydliggöra FMVs ansvar
  - Säkerställa kravnedbrytning och kravuppfyllnad
  - Styra och följa upp leverantörens IT-säkerhetsarbete
  - Tydliggöra leverantörens tekniska designansvar

Metodstöd - Användningsfall

Syftet med metodstödet – Effektivisera arbetet

Innehåll

Principer för genomförande

Förberedelser

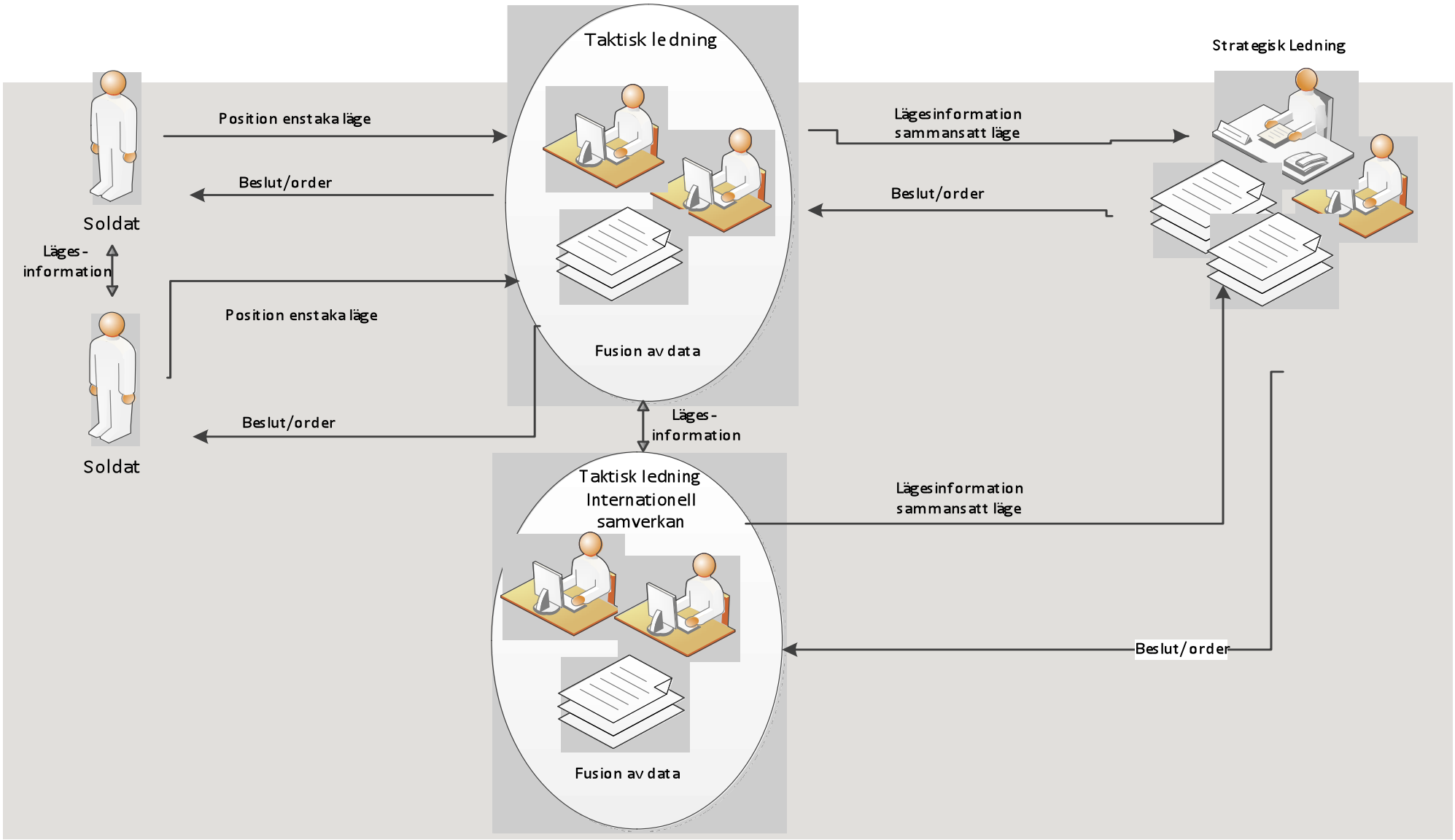
- Initial analys
  - Finns versioner av systemet sen tidigare?
  - Finns beslut från FM för vidare arbete?
- Planering av arbetet
  - Vilka ska delta?
  - På vilket sätt genomförs arbetet?

FMV

Användningsfall forts..

Genomförande

- 2 st workshops
  - Säkerhetsanalys
  - Dimensionerande Användningsfall –ger svar på:
    - Vilken typ av information som systemet kan komma hantera.
    - Vilka driftmiljöer som kan tänkas bli aktuella.
    - Vilka hot och risker som bör belysas i en separat analys.
    - Vilka regelverksområden som kan komma att påverkas i och med behovet av en viss informationsstruktur.
  - Risk- och sårbarhetsanalys (ej sannolikheter och åtgärder)


Taktisk ledning
Strategisk Ledning
Position enstaka läge
Beslut/order
Lägesinformation
sammansatt läge
Beslut/order
Soldat
Läges-
information
Position enstaka läge
Fusion av data
Beslut/order
Läges-
information
Soldat
Taktisk ledning
Internationell
samverkan
Lägesinformation
sammansatt läge
Beslut/order
Fusion av data

Punkt	Ja	Nej	Bedömning
Är samtliga underlag är konsekventa d.v.s. fria från motsägelser och tvetydiga krav och mål?			
Är verksamheten kring systemet är väl beskriven inklusive tydliga avgränsningar?			
Framgår roller och ansvar (som minst produktägare och produktansvarig)?			
Är informationsmängder väl definierade och beskrivna?			
Är informationsmängder inplacerade i informationssäkerhetsklass?			
Är informationsflöden översiktligt beskrivna?			
Är dimensionerande informationssäkerhetsklass beslutad?			
Finns beskrivning över hur systemet skall användas, t.ex. användningsscenarier?			
Går säkerhetskrav/-mål att spåra mot väl genomförda analyser, t.ex. hot-, risk och sårbarhetsanalys, författningsanalys eller verksamhetsanalys?			
Är styrande regelverk utöver det som är omhändertaget i inkommande kravmassa utpekat, t.ex. KSF, internationella standarder, etc?			
Framgår det vilka krav som ställs på verifiering, evaluering och andra kvalitetssäkrande aktiviteter framgår?			
Framgår det huruvida systemet innehåller signalskydd som måste hanteras enligt särskild process, t.ex. kryptoverifiering?			
Saknas krav eller analyser som borde vara redovisade? -Om Ja, vilka krav eller analyser är det?			

FMV

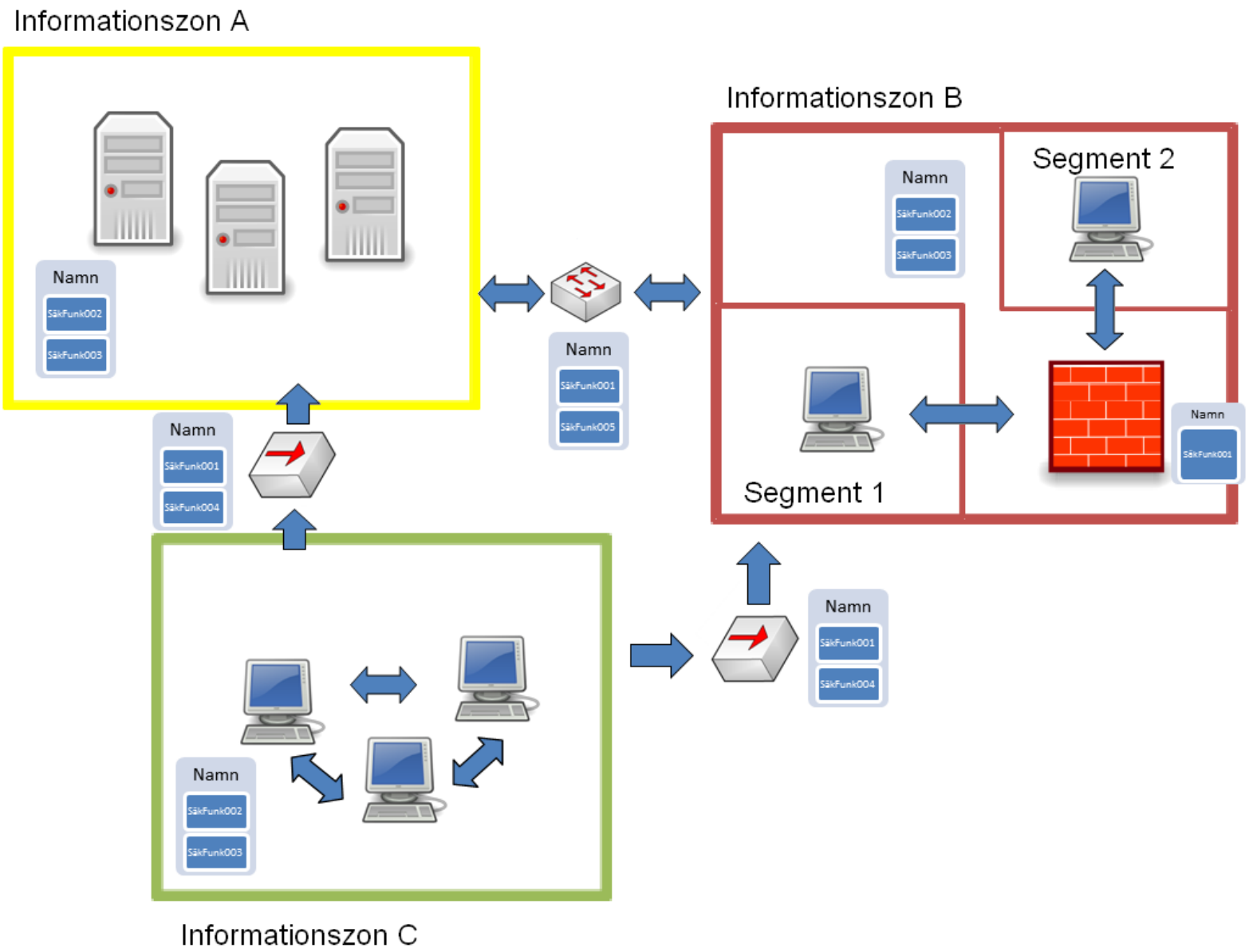
Mall STAU 2

Syfte: Komplettera Teknisk spec – underlätta för industri och öka kvalitén.

Övergripande design – visa vilken IT-säkerhetsfunktion som ska lösa ut vilka krav.

STAU 2

- SYSTEMÖVERSIKT
  - ÖVERGRIPANDE RIKTLINJER OCH DESIGNPRINCIPER
- KRAV
  - IT-SÄKERHETSKRAV
  - HOT
- IT-SÄKERHETSFUNKTIONER
  - INTRÅNGSSKYDD/SEPARATION
  - LOGGHANTERING
  - AUTENTISERING OCH BEHÖRIGHETER
  - SIGNALSKYDD
  - IDS-FUNKTIONALITET
  - INFORMATIONSHANTERING OCH BACK UP
  - SKYDD MOT RÖS
  - INTEGRITETSSKYDD
  - SÄKERHETSADMINISTRATION
  - SKYDD MOT SKADLIG KOD
  - ÖVRIGT
- IT-SÄKERHETSFUNKTIONER SOM KRÄVER SÄRSKILD ASSURANS
- GFE-PLAN


Informationszon A
Namn
SäkFunk002
SäkFunk003
Informationszon B
Namn
SäkFunk002
SäkFunk003
Segment 2
Namn
SäkFunk001
SäkFunk005
Segment 1
Namn
SäkFunk001
Namn
SäkFunk001
SäkFunk004
Namn
SäkFunk001
SäkFunk004
Namn
SäkFunk002
SäkFunk003
Informationszon C

Verksamhetsåtagande

- Krav på:
  - Planering av IT-säkerhetsarbetet (ISPP)
  - Test och verifiering
  - Ändringshantering
  - Roller och organisation
  - Nedbrytning av IT-säkerhetsarkitektur
  - Milstolpeleveranser

Oberoende granskning

Granskningsplan

- Scope
- Roller
- Resultat
- Realiserbarhet

Granskningsrapport

- Vilka slutsatser kan beställaren dra?

ISD-plan

- Definierar omfattning av ackrediteringsobjektet
- Klargör utmaningar, förutsättningar och problem för projektets ackrediteringsarbete
- Klargör hur utmaningarna ska hanteras i projektet
- Klargör roller för projektets ackrediteringsarbete
- Klargör säkerhetskritiska samverkansbehov

Deklaration ISD

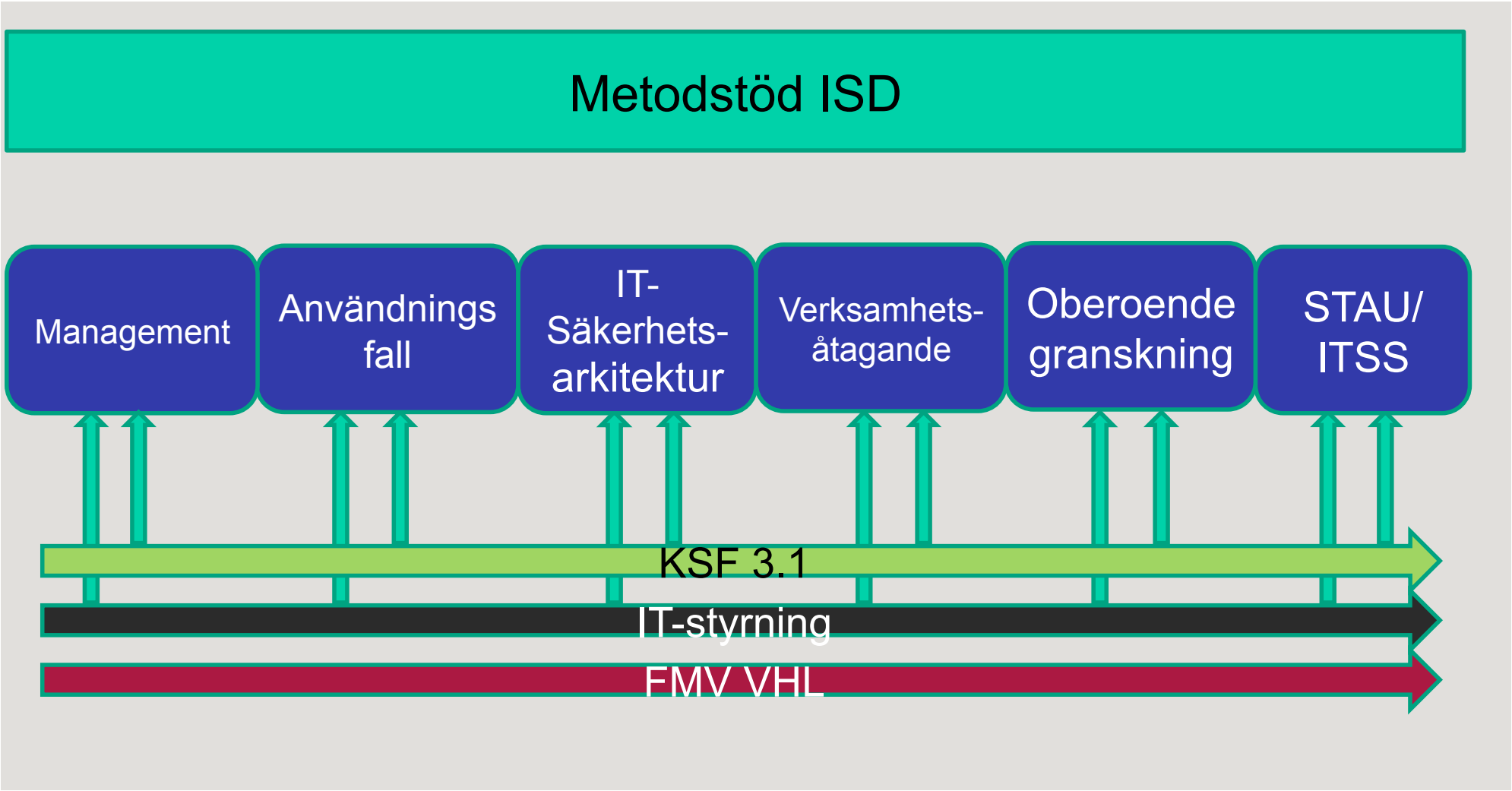
FMV tar ansvar för IT-säkerhetslösningen i systemet och deklarerar att:

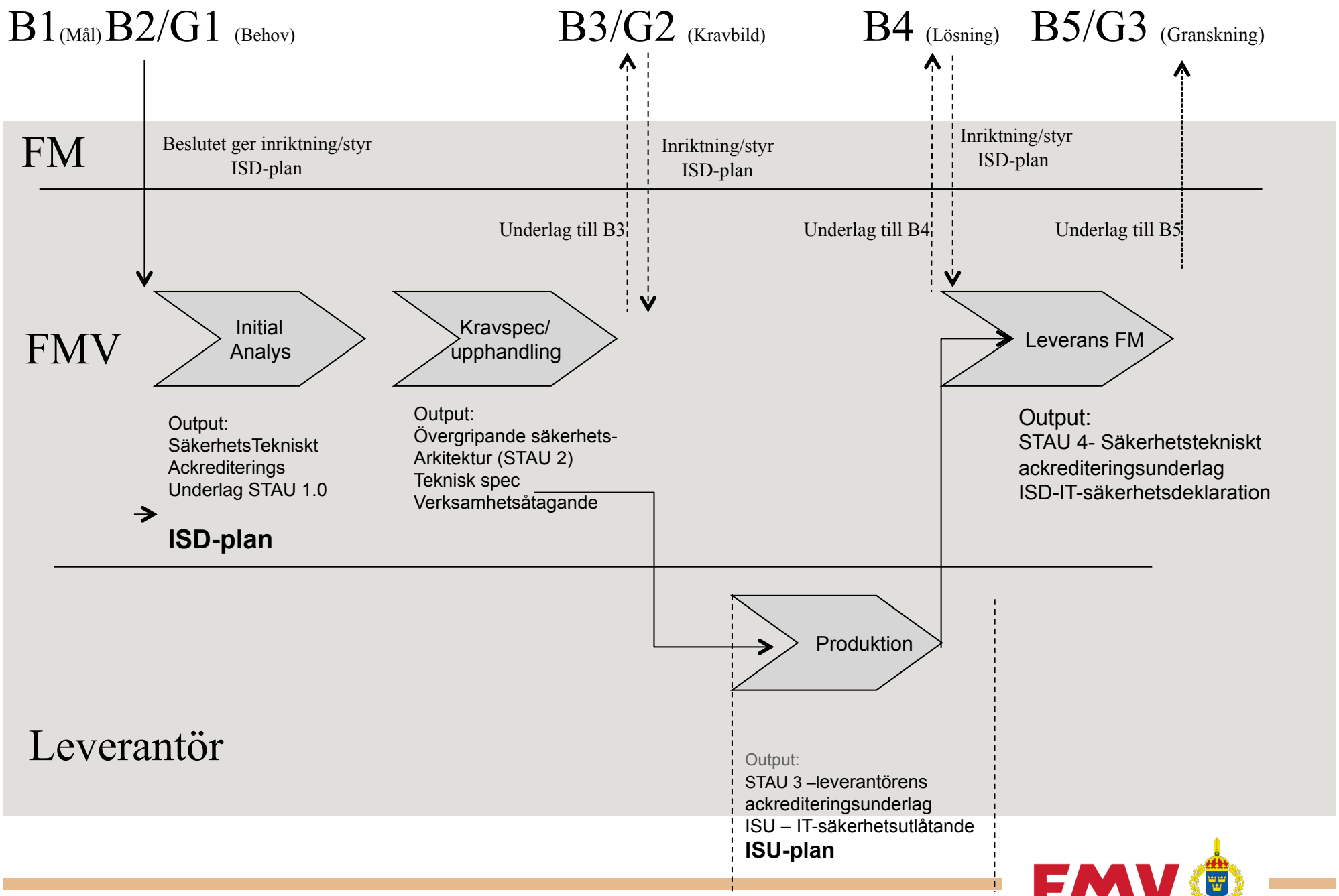
- *[Systemet/ackrediteringsobjektet]* uppfyller Försvarsmaktens krav på IT-säkerhetslösning för systemet.

- IT-säkerhetslösningen för systemet är utformad med utgångspunkt från Försvarsmaktens krav på tolererbar risk.

- det säkerhetstekniska underlaget för systemet (STAU 4) är utformat enligt den norm som kravställts inom FMV. Bevisen för kravuppfyllnad och tolererbar risk finns i STAU 4.

- IT-säkerhetsarbetet har följt fastställd ISD-plan.


Metodstöd ISD
Management
Användnings fall
IT-Säkerhets-arkitektur
Verksamhets-åtagande
Oberoende granskning
STAU/ ITSS
KSF 3.1
IT-styrning
FMV VHL


B1 (Mål) B2/G1 (Behov)
B3/G2 (Kravbild)
B4 (Lösning)
B5/G3 (Granskning)
FM
Beslutet ger inriktning/styr ISD-plan
Inriktning/styr ISD-plan
Inriktning/styr ISD-plan
Underlag till B3
Underlag till B4
Underlag till B5
FMV
Initial Analys
Kravspec/ upphandling
Leverans FM
Output:
SäkerhetsTekniskt Ackrediterings Underlag STAU 1.0
ISD-plan
Output:
Övergripande säkerhets-Arkitektur (STAU 2)
Teknisk spec
Verksamhetsåtagande
Output:
STAU 4- Säkerhetstekniskt ackrediteringsunderlag
ISD-IT-säkerhetsdeklaration
Produktion
Leverantör
Output:
STAU 3 –leverantörens ackrediteringsunderlag
ISU – IT-säkerhetsutlåtande
ISU-plan

SystGL - Systemgranskningsledare

- För att garantera kvalitén krävs en system-granskningsledare (SystGL)
- Oberoende granskning inför TC- beslut avseende ISD-plan och STAU 4/ISD.
- Kräver kompetens och erfarenhet