IT-säkerhet och IT-säkerhetsdeklaration (ISD)

Dan Olofsson
FMV KravF och MetF IT-säkerhet
SystGL IT- säkerhet
070-6825904

IT-säkerhetsområdet idag inom försvarssektorn

- Projekt har fallerat p.g.a. IT-säkerhetsaspekter
- 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
- Krav i form av FFS, FIB och KSF som behöver hanteras

Budskap

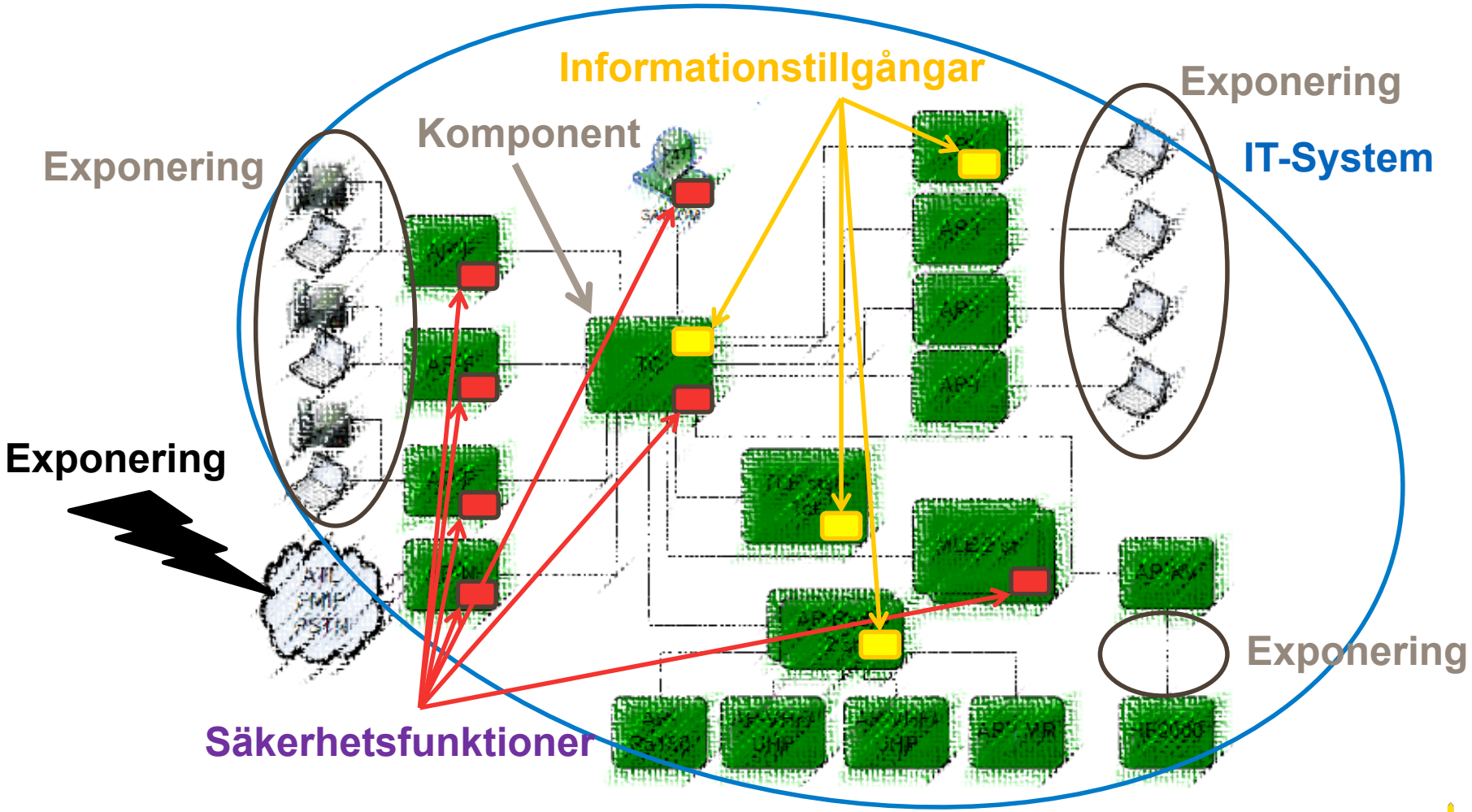
- Det går inte att i **efterhand granska** så att systemet har rätt säkerhetsnivå, ex Common Criteria, utan IT säkerhetsaspekten måste byggas in från början av SDLC.
- Det finns **ingen** teknisk lösning som skyddar all hantering av information vars spridning till obehöriga innebär synnerliga **Men** för Rikets Säkerhet utan den är beroende av fysiskt skydd samt verksamhetens säkerhetsmedvetande och –mognad.
- Alla tre aktörerna **beställare, kravförädlare samt leverantör** måste ha samma förståelse avseende förutsättningar, möjligheter och risker avseende ackrediterbarhet.
- **Slutsats:** Ackrediterbara IT system uppstår inte i källaren utan kräver en ordentlig integration i hela SDLC.

MUST yttrande

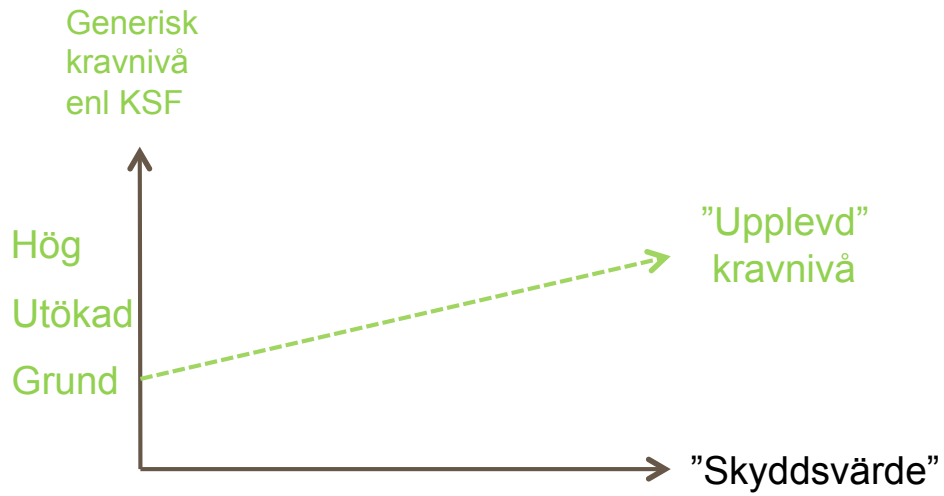
Försvarsmaktens interna bestämmelser om IT-säkerhet

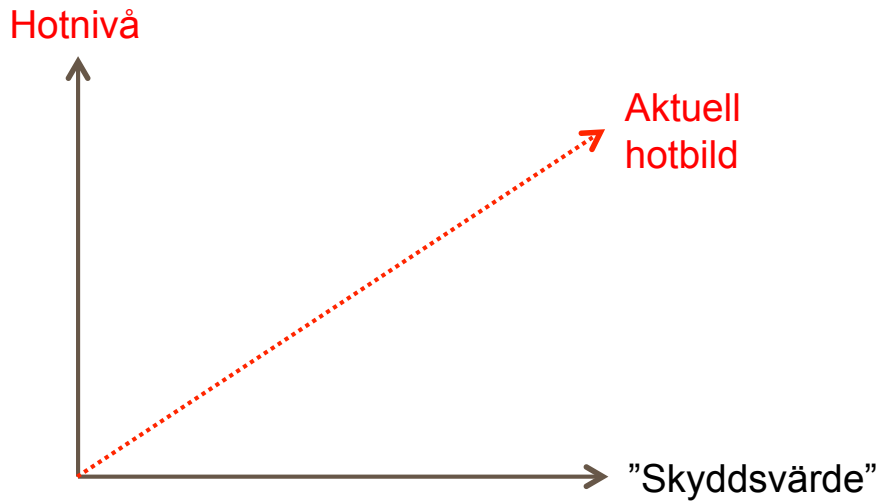
- IT-system inom Försvarsmakten ska vara försedda med godkända säkerhetsfunktioner. MUST ska godkänna säkerhetsfunktionerna.
- Innan ett IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer får ackrediteras centralt ska MUST yttra sig i fråga om säkerheten i systemet.

KSF 3 Begrepp



Kraven är generiska och måste tolkas!

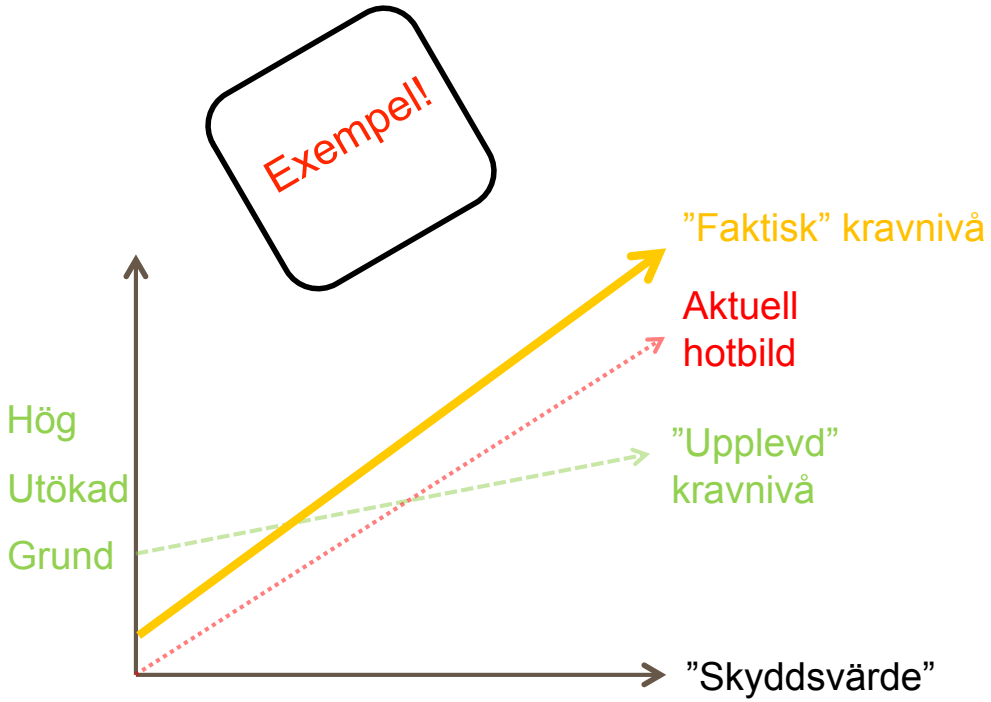




När man läser KSF-kraven kan man få uppfattningen att ”det här var väl enkelt, kraven finns ju och lösningarna med”. FMVs konsulter läser kraven ordagrant och vågar inte göra en egen tolkning.

Tolkningen av KSF-kraven baseras på den aktuella hotbilden. Till grund för denna ligger den generella hotbilden mot Sverige och de aktuella förutsättningarna för respektive verksamhet.

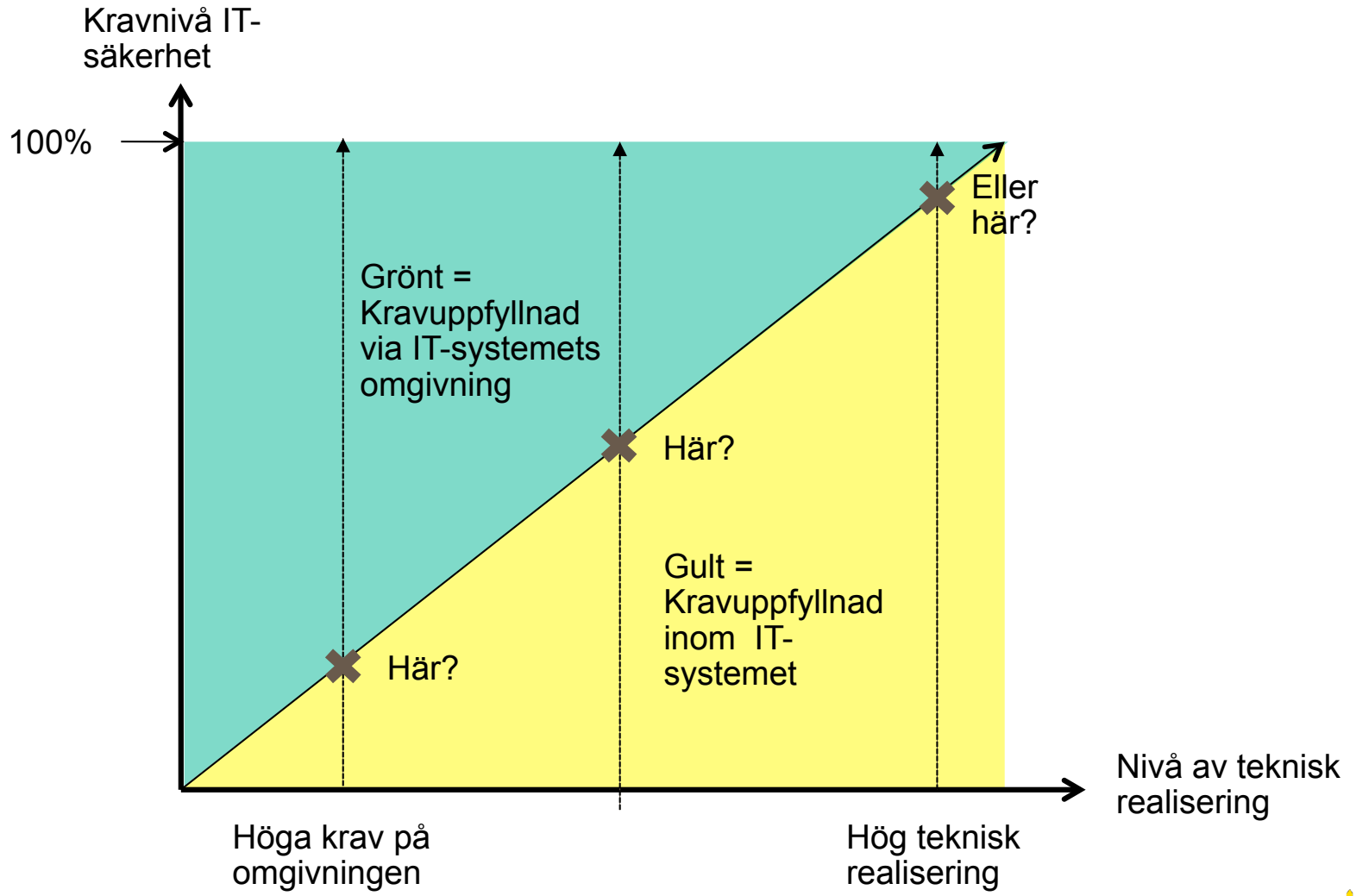
”Rätt” krav är en bedömning!



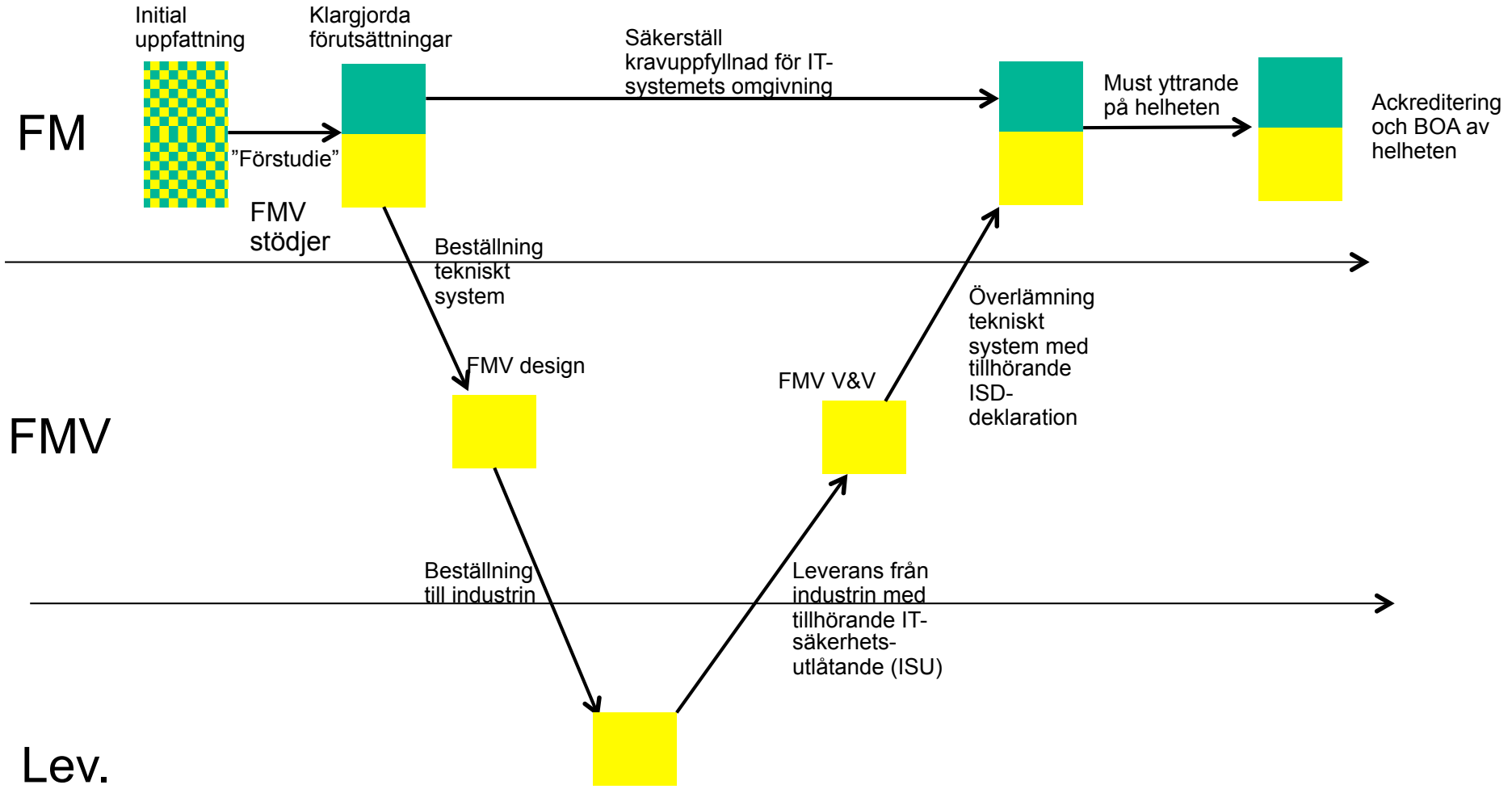
Generisk kravnivå enl KSF + Aktuell hotbild = Tolkade KSF-krav utifrån hotbild

När man tolkar kraven utifrån aktuell hotbild får man en annan kravnivå som kan vara både **högre eller lägre** än den ”upplevda”. Denna miss i kravhanteringen upptäcks oftast först när systemet är färdigt och slutgranskas.

Kravuppfyllnad för IT-systemet i dess omgivning



IT-system = tekniskt system + dess omgivning

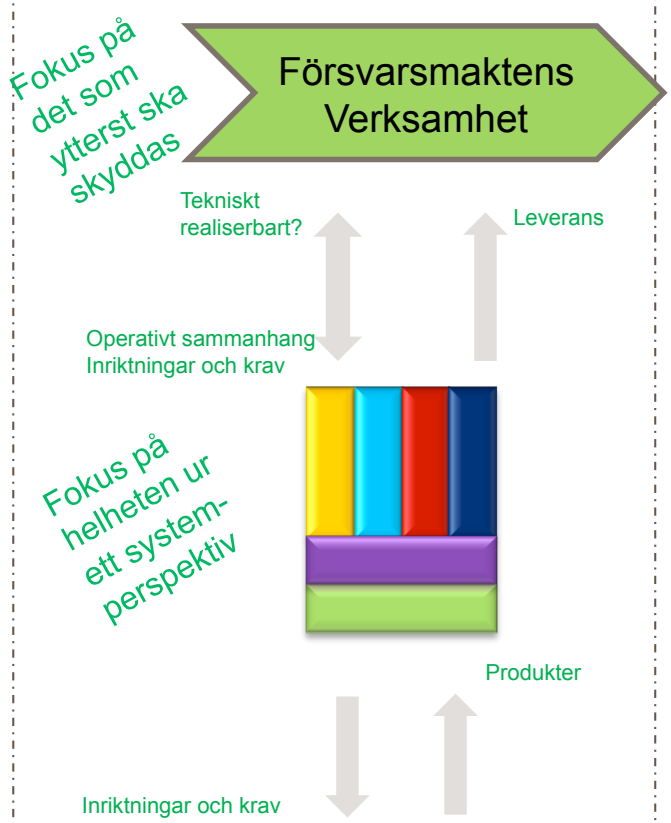


FMV SPL

Vem?

FMV
SPL

Vad?



FMV
AL

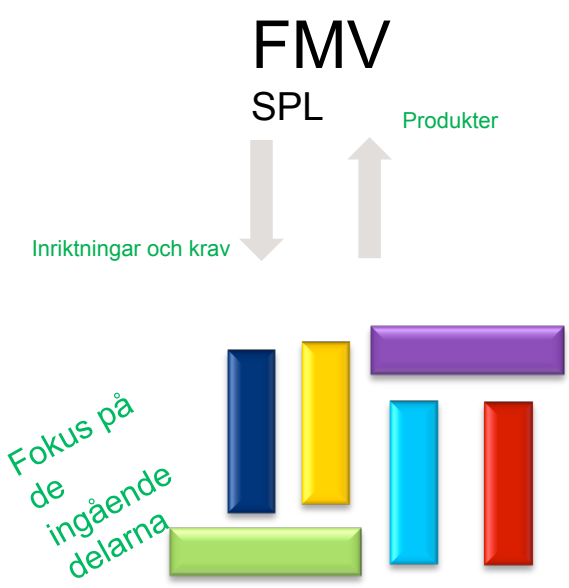
Varför?

Informationssäkerhet är kvalitetsegenskap som är starkt integrerad i helheten och är en kritisk faktor vid nästan all materiel-anskaffning.
Starta rätt saker i rätt tid och med rätt förutsättningar.
FMV SPL tar ett totalansvar för (M)-et och levererar en helhet som stödjer FM förmåga. Verksamhetsrisker ska identifieras och värderas för att kunna hanteras i tid.
SPL utgår från system av system och säkerställer att generella lösningar kan återbrukas.

Hur?

SPL ska i tid bedöma teknisk realiserbarhet och ge inriktningar för det fortsatta arbetet.
Dessutom ska SPL föreslå förbättringar för Försvarsmakten ur ett materielperspektiv bl.a. genom effektanalyser.
Som stöd för detta utvecklas metoder och vägledningar.
Dessutom erbjuds stöd till systemledningen. Granskning och kontroll med förslag på inriktningar.

FMV AL

Vem?	Vad?	Varför?	Hur?
FMV AL	 Plattformar , applikationer, infrastruktur, generella IT-säkerhetskomponenter, krypton etc. med de egenskaper som krävs för att hålla rätt risknivå.	SPLs inriktningar ger AL förutsättningar att fokusera på levereransen genom att dels minimera tiden för onödiga störningar och samtidigt möjliggöra samverkan med andra genom att sätta leveransen i ett sammanhang. Dessa aspekter medför lägre kostnader och lägre projektrisker och sist men inte minst stor nytta för verksamheten.	SPLs krav och inriktningar. Stöd i form av ISD metodstöd och vägledningar avseende kravdefinition, kravnedbrytning/arkitektur/ upphandling, verifiering/ oberoende granskning samt överlämning. Kvalitetssäkring och granskning.

Förutsättningar och krav

Förutsättningar och krav tydliggörs på resp. nivå

Vem?	Vad?	Vad ingår?
FMV SPL	Fokus på det som ytterst ska skyddas Försvarsmaktens Verksamhet Tekniskt realiserbart? Leverans Operativt sammanhang Inriktningar och krav Fokus på helheten ur ett system-perspektiv Produkter	Målsättningsarbete/koncept-arbete för nya förmågor för att klargöra exponering (hotbild), behörighetsstruktur, geografisk spridning, antal användare, informationsflöden, sekretess-, tillgänglighets- och riktighetsaspekter, externa regelverk att ta hänsyn till etc. -Kravdefinition, kravnedbrytning och säkerhetsarkitektur på systemnivå -Definition av generella säkerhetsfunktioner -Krav på komponentassurans Etc.
FMV AL	Inriktningar och krav Fokus på de ingående delarna	-Kravdefinition, kravnedbrytning och säkerhetsarkitektur på delsystemnivå Etc. Krav för att klara: -Kryptoverifiering -Komponentassurans (Komponentgodkännannde) -CC-evaluering etc

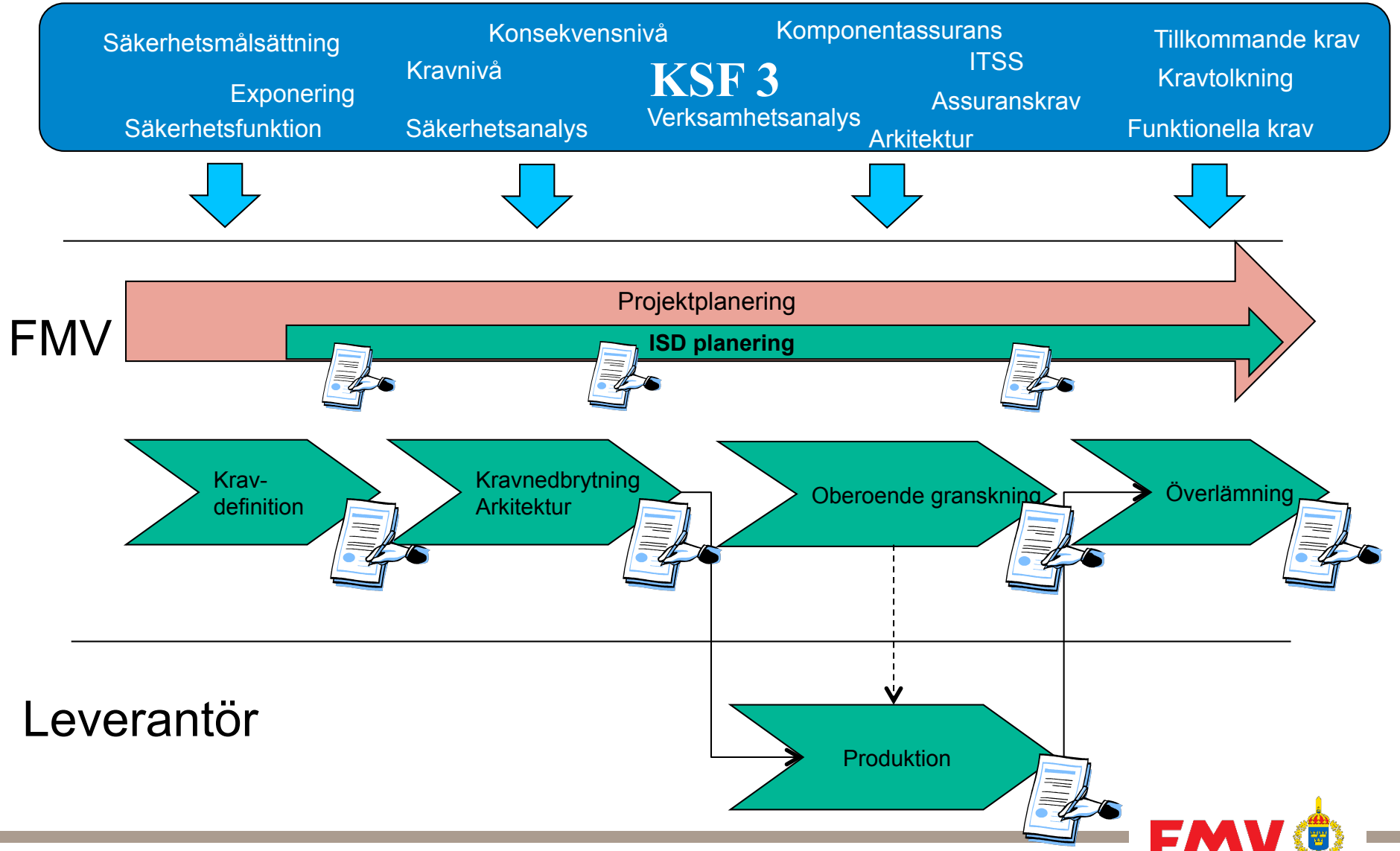
Övriga tekniska säkerhetskrav

FMV

Hur hanterar vi säkerhetsaspekterna på bästa sätt?

Komplext - många faktorer och allt hänger ihop

Dela upp arbetet i olika faser, gör rätt från början!



Fas 1 - Kravdefinition

Säkerhetsmålsättning
Konsekvensnivå
Komponentassurans
Tillkommande krav
Kravnivå
ITSS
Kravtolkning
Exponering
KSF 3
Assuranskrav
Säkerhetsfunktion
Säkerhetsanalys
Verksamhetsanalys
Funktionella krav
Arkitektur

ISD-planering

Fastställd ISD-plan

Krav-definition

Definiera gränsytor för informations-utbyte

Identifiera och bedöm dimensionerande IT-säkerhetsutmaningar i det fortsatta arbetet

Definiera dimensionerande användningsfall

Definiera konsekvenser av oönskade händelser

Definiera Exponering

Definiera informations-klassificering

Definiera grundläggande säkerhetskrav

Definiera tillkommande säkerhetskrav

STAU 1 (ITSS 1)

FMV

Fas 2 – Kravnedbrytning och arkitektur

Säkerhetsmålsättning
Konsekvensnivå
Komponentassurans
Tillkommande krav
Kravnivå
KSF 3
ITSS
Kravtolkning
Exponering
Assuranskrav
Säkerhetsfunktion
Säkerhetsanalys
Verksamhetsanalys
Arkitektur
Funktionella krav

ISD-planering

Uppdaterad ISD-plan

Genomför kravallokering

Krav-nedbrytning och arkitektur

Konkretisera gränsytor för informationsutbyte

Definiera designlösning

Definiera säkerhetsarkitektur

Minimera exponering

Bryt ner insamlade krav

Identifiera och hantera risker

Definiera komponent-assuransnivåer

STAU 2
(ITSS 2)
Underlag till TS och VÅS

Fas 3a – Kravuppfyllnad från leverantör

Säkerhetsmålsättning
Konsekvensnivå
Komponentassurans
Tillkommande krav
Kravnivå
ITSS
Exponering
KSF 3
Kravtolkning
Assuranskrav
Säkerhetsfunktion
Säkerhetsanalys
Verksamhetsanalys
Funktionella krav
Arkitektur

ISU-planering

Fastställd ISU-plan

Krav-uppfyllnad från leverantör

- Ta fram PPR, SRR, SDR, CDR, TRR
- Definiera skydd av leverans
- Påvisa Kravuppfyllnad i leveransen
- Definiera krav på användning
- Genomför säkerhetsgranskning
- Dokumentera och fastställ installations- och konfigurationsanvisningar
- Beskriv realiseringen av säkerhetsarkitekturen i en systemöversikt

ISU

Fas 3b - Oberoende granskning från FMV

Säkerhetsmålsättning
Konsekvensnivå
Komponentassurans
Tillkommande krav
Kravnivå
ITSS
Exponering
KSF 3
Kravtolkning
Assuranskrav
Säkerhetsfunktion
Säkerhetsanalys
Verksamhetsanalys
Arkitektur
Funktionella krav

Uppdragsplan

Planera oberoende granskning

Fastställd granskningsplan

Genomföra oberoende granskning

- Dokumentations-granska
- Genomför kodgranskning
- Genomför penetrationstest
- Genomför funktionstest
- Dokumentera resultat
- Genomför sårbarhets-scanning

Granskningsrapport

Fas 4 – FMVs kravuppfyllnad inför lev till FM

Säkerhetsmålsättning
Konsekvensnivå
Komponentassurans
Tillkommande krav
Kravnivå
ITSS
Exponering
KSF 3
Kravtolkning
Assuranskrav
Säkerhetsfunktion
Säkerhetsanalys
Verksamhetsanalys
Arkitektur
Funktionella krav

ISD-planering

Definiera ack-rediteringsobjektets slutliga omfattning

Överlämning

Definiera skydd av leverans

Påvisa total kravuppfyllnad

Definiera krav på användning

Genomför säkerhetsgranskning

Dokumentera och fastställ installations- och konfigurationsanvisningar

Beskriv realiseringen av säkerhetsarkitekturen i en systemöversikt

IT-säkerhets-deklaration (ISD)

STAU 4 (ITSS 4)

FMV

Förändringshantering i förvaltning

- Klassning av ändring i 4 klasser
  - Klass 1
    - Aktuell STAU 4 och ISD deklaration påverkas inte. Kräver inget ytterligare fastställande av Teknisk Ledning.
  - Klass 2
    - STAU 4 påverkas men ej STAU 2. De kravområden som påverkas ska ses över samt vid behov även enskilda krav. Kan resultera i en ny STAU 4 samt ny ISD-deklaration.
  - Klass 3
    - STAU4 och även STAU 2 påverkas. Kräver översyn av säkerhetsarkitekturen och kravuppfyllnaden. Resulterar i ny STAU 2, STAU 4 och ISD-deklaration.
  - Klass 4
    - STAU 4, STAU 2 samt STAU 1 påverkas. Kräver ny kravdefinition, ny säkerhetsarkitektur och ny kravuppfyllnad. Resulterar i ny STAU 1, STAU 2, STAU 4 samt ISD-deklaration.

FM IT-process och FMV Produktprocess