



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	1(76)

---

ISD 3.1 Processbeskrivning



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	2(76)

## Innehåll

1	Basfakta.....	4
1.1	Syfte med detta dokument.....	4
1.2	Giltighet och version.....	4
1.3	Terminologi.....	4
1.4	Referenser.....	4
1.5	Bilagor.....	4
2	Inledning.....	5
2.1	Syfte.....	5
2.2	Tillämplighet.....	5
2.3	Bakgrund.....	6
3	ISD-Processen.....	7
3.1	Övergripande beskrivning.....	7
3.2	ISD i FMV VHL.....	8
3.3	Översikt av ISD faser.....	9
3.3.1	Identifiera.....	9
3.3.2	Definiera.....	10
3.3.3	Realisera.....	11
3.3.4	Vidmakthålla.....	12
3.3.5	Avveckla.....	13
3.4	ISD-processens metodstöd.....	14
3.5	Relation till FM-processer.....	17
3.6	Kravhantering i ISD-processen.....	22
3.7	ISD - definition av oberoende.....	26
4	Roller.....	28
4.1	ISD-roller.....	28
4.1.1	ISM – Information Security Manager.....	28
4.1.2	ISA – Information Security Architect.....	29
4.1.3	ISE – Information Security Evaluator.....	30
4.1.4	ISTM – Information Security Test Manager.....	30
4.2	Tillsättning av ISD-roller.....	31
4.3	FMV-roller med anknytning till ISD-processen.....	31
4.3.1	Produktledare (PrL).....	31



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	3(76)

4.3.2	Projektledare (PL) .....	31
4.3.3	Systemgranskningsledare IT-säk (SystGL IT-säk).....	32
4.4	Övriga roller .....	32
4.4.1	FM MOA.....	32
4.4.2	Leverantör .....	32
4.5	Ansvarsfördelning för ISD-arbete .....	32
5	Fördjupad processbeskrivning.....	34
5.1	Identifiera.....	35
5.1.1	Övergripande fasbeskrivning .....	35
5.1.2	Detaljerad fasbeskrivning.....	37
5.2	Definiera.....	46
5.2.1	Övergripande fasbeskrivning .....	47
5.2.2	Detaljerad fasbeskrivning.....	49
5.3	Realisera.....	54
5.3.1	Övergripande fasbeskrivning .....	54
5.3.2	Detaljerad fasbeskrivning.....	57
5.4	Vidmakthålla.....	67
5.4.1	Övergripande fasbeskrivning .....	67
5.4.2	Detaljerad fasbeskrivning.....	71



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	4(76)

## 1 Basfakta

### 1.1 Syfte med detta dokument

Detta dokument beskriver ISD-processen, version 3.1 (även benämnt ISD 3.1).

### 1.2 Giltighet och version

Datum	Version	Beskrivning	Ansvarig
2021-05-19	1.0	Första utgåvan	FMV MetF IT-säk

Tabell 1 – Versionshistorik

### 1.3 Terminologi

Se Bilaga 1 för en generell förteckning över begrepp och förkortningar som används inom ISD-processen.

### 1.4 Referenser

Referens	Benämning	Dokument Id
[1]	Beslut avseende tillämpning av Handbok FMV arbetssätt version 2	17FMV8044-26:1
[2]	ISD-Processen 3.0	18FMV6730-8:1
[3]	Beslut om krav på godkända säkerhetsfunktioner version 3.1 (KSF v3.1)	FM2014-5302:1
[4]	Fastställande av processhandbok för IT-processen version 1.3	FM2013-4411:3
[5]	Försvarsmaktens beslutsmodell för tekniska system (FM BMTS)	FM2017-22865:1

Tabell 2 – Referenser

### 1.5 Bilagor

Detta dokument har följande bilagor:

- Bilaga 1. ISD 3.1 Begrepp och Definitioner 20FMV5903-1:1.1

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	5(76)

## 2 Inledning

### 2.1 Syfte

Informationssäkerhetsdeklarationsprocessen (ISD-processen) är en stödprocess för FMV informationssäkerhetsarbete inom ramen för genomförandeprojekt samt vidmakthållandeuppdrag.

Huvudsyftet är att Forsvarsmakten ska erhålla IT-system i rätt tid, till rätt kostnad och till rätt kvalitet avseende informationssäkerhet.

Vidare ska MUST få underlag av sådan kvalitet att IT-systemet kan bedömas och godkännas utan omfattande egen resursinsats.

Ett annat syfte med ISD-processen är att säkerställa leverans av informationssystem som lever upp till Forsvarsmaktens informationssäkerhetskrav med processer, rutiner och kompetens som skapar förtroende för arbetet vid FMV. Förtroende uppnås genom tydlighet, enhetlighet, spårbarhet och effektivitet i informationssäkerhetsarbetet och förutsätter metodstöd och specifik kompetens inom området.

### 2.2 Tillämplighet

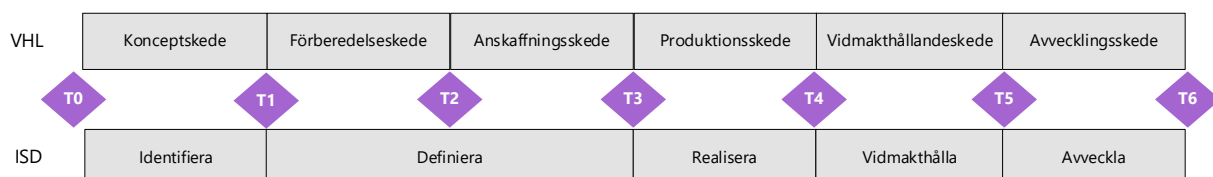
Alla genomförandeprojekt och uppdrag med att vidmakthålla system som utvecklar informationssystem ska följa ISD-processen. Detta innebär bl.a. att en Informationssäkerhetsdeklaration (ISD) ska överlämnas till FM.

ISD 3.1-processen stödjer FMV verksamhet i följande VHL-skeden (referens [1]).

VHL-skede	T-beslut	ISD-fas
Konceptskede	T0 till T1	Identifiera
Förberedelseskede	T1 till T2	Definiera
Anskaffningsskede	T2 till T3	Definiera
Produktionsskede	T3 till T4	Realisera
Vidmakthållandeskede	T4 till T5	Vidmakthålla
Avvecklingsskede	T5 till T6	Avveckla

Tabell 3 – VHL-skede relaterat till ISD-fas

Figur 1 nedan illustrerar korrelationen mellan FMV VHL-skede och ISD-faser. Notera att nedanstående korrelation är något förenklad. En mer detaljerad beskrivning finns senare i detta underlag.



Figur 1 VHL-skede och ISD-faser



**Ej sekretess**

## **ISD 3.1 Processbeskrivning**

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	6(76)

### **2.3 Bakgrund**

FMV ISD-process version 3.1 är en vidareutveckling av ISD version 3.0 (referens 0). ISD version 3.0 var en större modifiering av tidigare ISD-process (version 2.3). Syftet med uppdateringen från version 2.3 till 3.0 var att ISD-processen skulle omfatta samtliga faser i FMV VHL och även utgöra beslutsunderlag till det som tidigare benämndes S-beslut.

I samband med att FMV VHL uppdaterats så har det även identifierats behov av att anpassa ISD-processen. ISD 3.1 är anpassad till FMVs nya VHL.

De större modifieringarna mellan ISD 3.0 och 3.1 är:

- ISD 3.1 utgör beslutsunderlag till T-beslut (tidigare S-beslut)
- ISD 3.1 rollbeskrivningar har utvecklats och förtydligats
- Processen har uppdaterats utifrån erhållna erfarenheter i genomförandeprojekt
- Mallarna för de olika ISD-dokumenterna är uppdaterade för att påvisa förändringar i system

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	7(76)

### 3 ISD-Processen

#### 3.1 Övergripande beskrivning

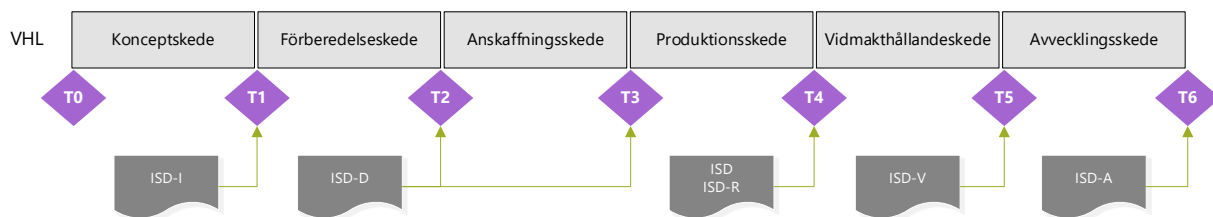
Realiserbarhet är den röda tråden i ISD-processen och bedömningen görs kontinuerligt inför varje FMV VHL T-beslut med utgångspunkt från:

- Ackrediterbarhet – bedömning av möjligheten att godkännas ur säkerhetssynpunkt.
- Kostnadseffektivitet – krav på informationssäkerhet vägs mot bedömd kostnad för informationssäkerhetslösningen
- Projektrisker
- Integration med Systems Engineering (SE) – informationssäkerhetsarbetets integration med SE för avvägning av krav och hur lösning kan implementeras.

Bedömningen dokumenteras i en informationssäkerhetsdeklaration, i processtödet benämnt ISD-I, ISD-D, ISD-R och ISD-V.

Genom att använda realiserbarhetsbedömning som en del av beslutsunderlag för T-beslut skapas en projektriskhantering som möjliggör tidig åtgärd och inbromsning ifall inte tillräckliga förutsättningar bedöms finnas.

I Figur 2 illustreras hur deklarationerna kopplar till FMV Verksamhetsledningssystem (FMV VHL). ISD beslutsunderlag inför T4 utgörs av deklarationen ISD, där ISD-R utgör underlag.



Figur 2 FMV VHL i relation till ISD-processens deklaration av realiserbarhetsbedömningar

Genomförandeprojekt kan ta fram:

1. IT-system som ska överlämnas till FM
2. IT-system som ingår som delsystem i en system-i-system-lösning
3. IT-system som utgör en komponent för återbruk inom FMV

För IT-system som ska överlämnas till FM tas beslut T4 baserat på dels ISD-R, dels en informationssäkerhetsdeklaration (ISD). ISD deklarerar att FMV anser att IT-systemet som levereras till FM uppfyller de ställda informationssäkerhetskraven och att informationssäkerhetsarbetet har genomförts i enlighet med produktområdets ISD-strategi, samt att FMV ISD-process har följt såsom specificerats i ISD-planen.



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	8(76)

I ISD sammanfattas även eventuella resterande risker samt de krav och förutsättningar som ställs på driftmiljön för att systemet ska vara säkert. ISD utgör därmed toppdokumentet på informationssäkerhetsunderlaget som överlämnas till FM i samband med systemöverlämningen.

### 3.2 ISD i FMV VHL

ISD-processen stödjer FMVs arbete med informationssäkerhet i de olika VHL-skedena. Översiktligt ges följande stöd i respektive skede:

#### FMV VHL Konceptskede

Konceptskedet sammanfaller med ISD-processens Identifiera-fas. Här sker informationssäkerhetsanalys av FMs behov och av indata från FM. En strategi för ISD-arbetet skapas, en övergripande kravbild sammanställs och, ett eller flera genomförandeprojekt definieras med var sin realiserbarhetsbedömning som deklarerar i projektspecifika ISD-I.

När T1 tas för respektive genomförandeprojekt är Försvarmaktens övergripande kravbild avseende informationssäkerhet känd. Det finns även en strategi för att hantera IT-säkerhetsaspekterna i projektet och ackrediteringsobjektet (IT-objekt som enligt G-beslut ska godkännas ur säkerhetssynpunkt) är definierat.

Vid positivt T1-beslut bedöms respektive genomförandeprojekt ha förutsättningar att starta.

#### FMV VHL Förberedelseskede

Ingår i ISD-processens Definiera-fas. Här skapas först en ISD-plan som innefattar informationssäkerhetsarbetet i genomförandeprojektet. Under Definiera-fasen genomförs design av systemet och framtagning av informationssäkerhetskrav tillsammans med Systems Engineering (SE).

Kravarbetet slutar med Teknisk Specifikation (TS) och Verksamhetsåtagandespecifikation (VÅS), vilka används vid upphandling för utveckling av systemet. Realiserbarhetsbedömningen som deklarerar i ISD-D innehåller beskrivning av säkerhetsarkitektur, genomförda analyser samt informationssäkerhetskraven på systemet och dess driftsmiljö.

Vid positivt T2-beslut bedöms det finnas förutsättningar att påbörja anskaffning av systemet.

#### FMV VHL Anskaffningsskede

Ingår i ISD-processens Definiera-fas. Här utvärderas anbuderna som inkommit ur ett informationssäkerhetsperspektiv.

Eventuellt genomförs en förnyad realiserbarhetsbedömning beroende på innehåll i angivna anbud eller på uppdaterad indata från FM. Vid positivt T3-beslut bedöms det finnas förutsättningar att starta utvecklingen av systemet.

#### FMV VHL Produktionsskede

Sammanfaller med ISD-processens Realisera-fas. Under tiden utveckling av systemet sker, ges stöd till leverantör samtidigt som verifieringen av de assuranceskrav som leverantören ska uppfylla påbörjas.





Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	9(76)

Evaluering av systemunderlag och säkerheten sker innan leverans av informationssystem till FMV. Realiserbarhetsbedömningen som deklarerar i ISD-R innehåller redovisning av kravuppfyllnad och bedömning av resterande risker.

En informationssäkerhetsdeklaration (ISD) tas också fram där informationssystemet är avsett att överlämnas till FM.

Vid positivt T4-beslut bedöms utvecklat system vara tillräckligt säkert, och möjligt att överlämna till FM (ifall det är avsett att överlämnas).

### FMV VHL Vidmakthållandeskede

Sammanfaller med ISD-processens Vidmakthållande-fas. Här sker omvärldsbevakning av händelser som kan påverka IT-systemets säkerhet. Bedömning av säkerhetspåverkan på planerad modifiering utförs. Säkerhetsarbete för att stödja modifieringsarbetet och evaluera dess resulterande påverkan på säkerheten. Realiserbarhetsbedömningen deklarerar i ISD-V.

### FMV VHL Avvecklingskede

Sammanfaller med ISD-processens Avveckla-fas. Här tas en instruktion fram som beskriver hur säker avveckling ska göras tillsammans med en deklaration som beskriver att säker avveckling är gjord inför T6-beslut.

## 3.3 Översikt av ISD faser

Detta kapitel innehåller en övergripande beskrivning av syftet med, och innehållet i, ISD-processens olika faser; Identifiera, Definiera, Realisera och Vidmakthålla och Avveckla.

En mer utförlig beskrivning av respektive fas återfinns i kapitel 5.

### 3.3.1 Identifiera

Realiserbarhetsbedömningen (ISD-I) i Identifiera görs inför FMV VHL T1-beslut för att säkerställa att genomförandeprojektet har förutsättning att leverera ett ackrediterbart IT-system. Den baseras huvudsakligen på att relevant indata har erhållits från FM, så att genomförandeprojektet har förutsättning att leverera ett ackrediterbart IT-system. Realiserbarhetsbedömning ska göras även om informationssystem inte ska ackrediteras.

Bedömningen görs med utgångspunkt från analyser på hur IT-systemet ska användas, verksamhetsmässig/operativ exponering, säkerhetsskyddsklassificering, verksamhetens sårbarheter och konsekvenser av identifierade risker m.m.

Indata från FM kan vara systemmålsättning (SMS), FM ITSS inklusive Särskild säkerhetsskyddsbedömning (SSB) samt G1-beslut<sup>1</sup>. Arbetet med analyserna kan göras iterativt för att FM och FMV ska förstå varandras behov. Resultatet från analyserna dokumenteras i AU-I (Analysunderlag Identifiera), och de kravkällor som framkommer i analyserna dokumenteras i ITSS-I.

---

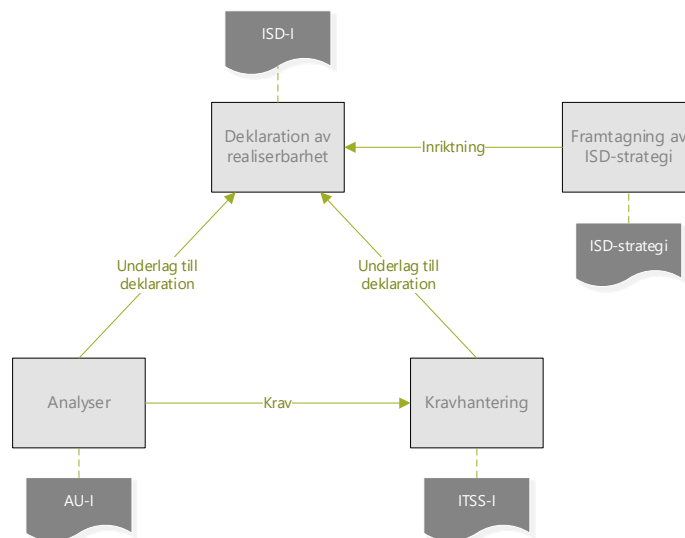
<sup>1</sup> G1 beslut är ett beslut i Försvarmaktens IT-process och innehåller normalt förtydligande att det är ett informationssystem, vad som är ackrediteringsobjekt och om det ska godkännas i säkerhetssynpunkt (ackrediteras).

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	10(76)

ISD-strategin utgör underlag för att klargöra förutsättningarna för IT-säkerhetsarbetet. Strategin pekar på utmaningar, främst med avseende på system av system, och ger inriktningar avseende återbruk av komponenter. Vidare beskriver den relationer till andra projekt och kan fördela krav som finns på system av system.

Aktiviteter för Identifiera beskrivs mer i detalj i kapitel 5.1. Figur 3 illustrerar de dokument som används för realiserbarhetsbedömning i Identifiera-fasen, samt deras inbördes förhållande.

Aktiviteterna illustreras med ljusa rektanglar, och de dokument som huvudsakligen produceras genom dessa aktiviteter illustreras med mörkare dokumentfigurer. Aktiviteterna utgör grunden för informationssäkerhetsarbetet i fasen genom t.ex. planering, kravinsamling och kravidentifiering.



Figur 3 Realiserbarhetsbedömning i Identifiera

### 3.3.2 Definiera

Realiserbarhetsbedömningen i Definiera inför FMV VHL T2- och T3-beslut baseras på nedbrytning och tolkning av kraven, samt framtagen IT-säkerhetsarkitektur. Arkitekturen visar på balansen mellan verksamhetens behov (funktionalitet) och säkerhetsfunktioner baserat på definierad kravnivå. Realiserbarhetsbedömning ska göras även om informationssystem inte ska ackrediteras.

Kravarbetet kan göras iterativt och frågan om eventuell ändring kan behöva återföras till FM, alternativt fastställas av Produktledare.

ITSS-D följer strukturen på FM ITSS (referens [3]) och innehåller såväl funktionella säkerhetskrav som assuranskrav. De funktionella säkerhetskraven utgör grund för Teknisk Specifikation (TS) medan assuranskraven utgör grund för Verksamhetsåtagandespecifikation (VÅS) inför eventuell upphandling.

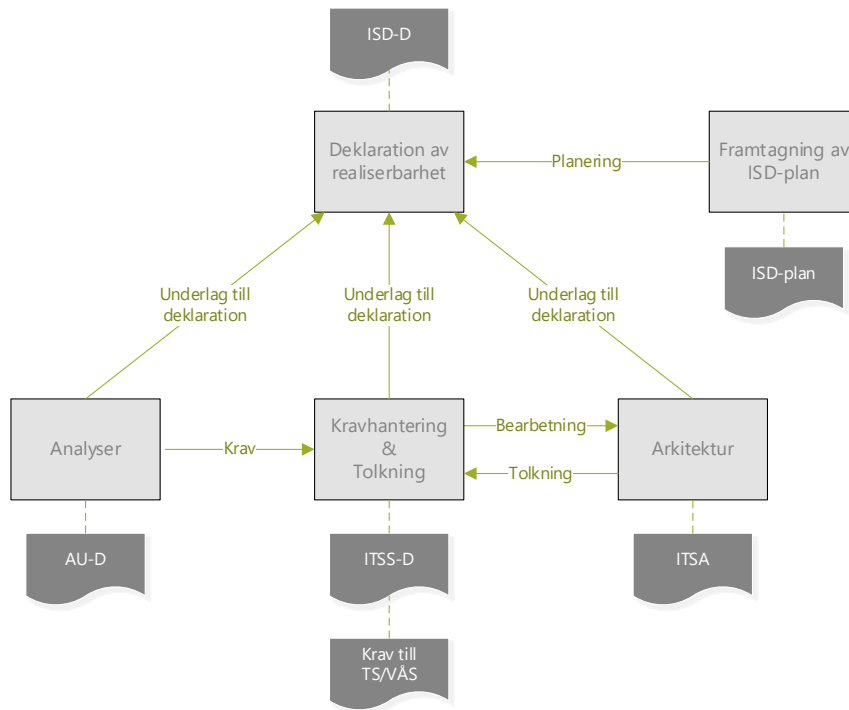
ISD-planen styr informationssäkerhetsarbetet i genomförandeprojektet.

Informationssäkerhetsarbetet planeras i form av omfattning, resurser, utmaningar, aktiviteter, tidplan och dokument. ISD-planen ska vara korrelerad med projektets övriga planer (t.ex proj -,

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	11(76)

SE-, ILS-, SysSÄK- och VoV-planer) för att säkerställa att ISD-arbetet synkroniseras med övriga aktiviteter i projektet.

Aktiviteter för Definiera beskrivs mer i detalj i kapitel 5.1.1.1. Figur 4 illustrerar de dokument som används för realiserbarhetsbedömning i Definiera-fasen, samt deras inbördes förhållande.



Figur 4 Realiserbarhetsbedömning i Definiera

### 3.3.3 Realisera

Realisera är genomförandeprojektets produktionskedje och innehåller också FMV leverans till FM. I Realisera är IT-systemet klart för leverans och en ackrediterbarhetsbedömning görs inför FMV VHL T4-beslut. Ackrediterbarhetsbedömning baseras på kravuppfyllnad, restriskanalys och sårbarhetsbedömning. Ackrediterbarhetsbedömning ska göras även om informationssystem inte ska ackrediteras.

Inför bedömningen görs relevanta analyser av leverantörens leverans och kravuppfyllnad, riskanalys på kvarvarande brister, samt utfall från evaluerarens (ISE) granskningsaktiviteter. Analyserna dokumenteras i AU-R och kravuppfyllnaden i ITSS-R.

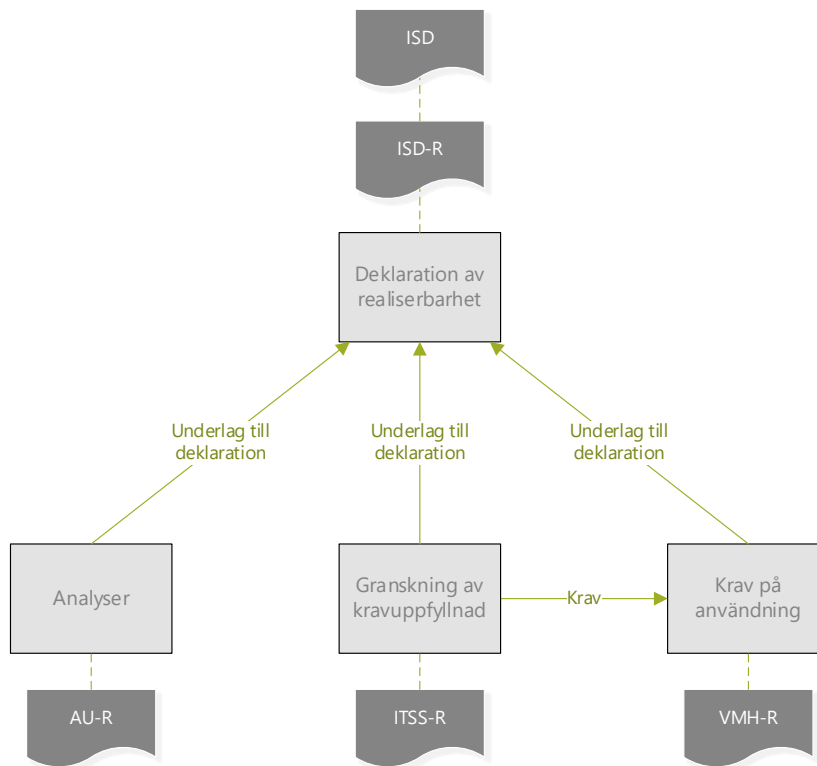
ISD-R, inklusive bilagor, utgör underlag inför överlämning till FM avseende IT- och informationssäkerhetsförmågor i systemet. Underlaget anger vilka krav som inte uppfylls av systemets IT-säkerhetslösning, utan ska uppfyllas av systemets omgivning vid driftsättning.

Inför T4-beslutet gör FMV den formella deklARATIONEN (ISD) till FM att systemet uppfyller

- FM ställda krav på IT-säkerhetsfunktioner,
- att avvikelser hanterats samt
- att ISD-processen har följts.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	12(76)

Aktiviteter i Realiserafasen beskrivs mer i detalj i kapitel 5.3 Figur 5 illustrerar de dokument som används för realiserbarhetsbedömning i Realiserafasen, samt deras inbördes förhållande.



Figur 5 Realiserbarhetsbedömning i Realisera

### 3.3.4 Vidmakthålla

I Vidmakthålla är systemet överlämnat och i operativ drift. För ett system i drift kan det ske förändringar vilket innebär att bedömningar av påverkan på informationssäkerhetslösningen behöver genomföras.

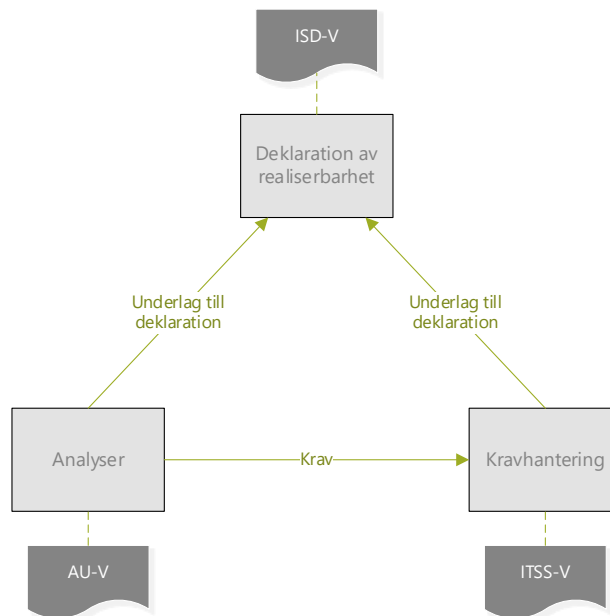
Bedömningens innehåll och omfattning beror på vilken typ av förändring som behövs göras. Det kan dels röra sig om planerade funktionsförändringar, eller hantering av materiel som når end-of-life, och dels om akuta åtgärder som t ex grundar sig i förändrad exponering eller ny hotbild baserad på nya driftsituationer.

ISD-V, med AU-V och ITSS-V, kan användas över tiden för att redovisa små förändringar och/eller förbättringar avseende uppfyllnad av IT-säkerhetskraven. Den tekniska förändringen av system genomförs i dessa fall genom Teknisk Order (TO) eller motsvarande.

VMH-R förtecknar förslag på säkerhetskrav som bör uppfyllas av den omgivande miljön för att informationssystemet ska kunna användas på ett säkert sätt.

Aktiviteter i Vidmakthållafasen beskrivs mer i detalj i kapitel 5.3. Figur 6 illustrerar de dokument som används för realiserbarhetsbedömning i Vidmakthållafasen, samt deras inbördes förhållande.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	13(76)



Figur 6 Realiserbarhetsbedömning i Vidmakthålla

### 3.3.5 Avveckla

Fasen *Avveckla* syftar till att säkerställa så informationssystem som tas ur drift kan avvecklas säkert och kontrollerat, med fokus på informationssäkerheten. FMV PrL är ansvarig för genomförandet.

Efter T5-beslut tagits om att informationssystemet ska avvecklas, finns en arbetsordning och vissa övergripande aktiviteter att ta hänsyn till.

*Exempel:*

1. Genomföra säkerhetsanalys och sekretessbedömning.
2. Planera genomförandet av avvecklingen och dokumentera hur det ska gå till.
3. Avveckla informationssystemet.
4. Färdigställa och signera rapport om avveckling (ISD-A) inför T6-beslut.

Avvecklingsrapporten består av ett huvuddokument och en bilaga. Huvuddokumentet ISD-A är rapporten som verkar som underlag för de beslut som sedermera resulterar i arkivering och destruktion.

Analysunderlaget (*bilaga AU-A*) innehåller analyser över vilken information som finns i informationssystemet med avseende på säkerhetsskyddsklass.

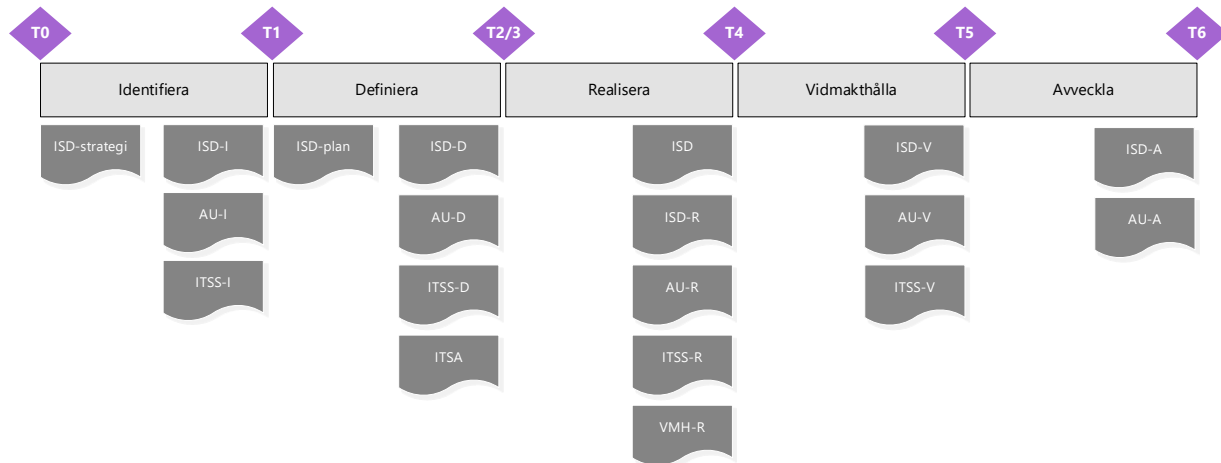
Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	14(76)

### 3.4 ISD-processens metodstöd

ISD-processen ger, utöver föreliggande processbeskrivning, metodstöd till informationssäkerhetsarbetet genom följande:

- Mallar som ger struktur och anvisningar för arbetet som krävs för att ta fram erforderlig information.
- Utbildningar som ger både översiktlig och fördjupad kunskap i ISD-processen och dess tillämpning för roller inom ISD-arbetet.
- Tillämpningsanvisningar för specifika delar i processen. Det är ett kontinuerligt arbete med att framställa dessa anvisningar.
- Av MetF arrangerade mötesfora (Infosäkforum, AG Säk) med syfte att stötta verksamhetens ISD-arbete.

I syfte att erbjuda ett stöd för framtagning av de dokument som krävs i ISD-processen har ett antal mallar tagits fram. Dessa mallar är knutna till respektive ISD-fas (Identifiera, Definiera, Realisera och Vidmakthålla och Avveckla) enligt Figur 7 nedan.



Figur 7 ISD 3.1 mallar

I Figur 7 framgår det att det finns vissa typer av dokument som återkommer i respektive fas, samtidigt som vissa dokument bara finns i en specifik fas.

Tabell 4 nedan avser att översiktligt beskriva de olika typerna av dokument. ISD 3.1 processtöd innehåller mallar för dessa dokument.

Artefakt	ISD-fas	Beskrivning/syfte
ISD-strategi	Identifiera	ISD-strategin är ett inriktningsdokument för FMV Produktledare (PrL) att använda för att ge genomförandeprojekt rätt förutsättningar avseende informationssäkerhet för produktområdet. ISD-strategin ska ge nödvändiga strategiska ingångsvärden för genomförandeprojekten vid utformning av ISD-I och ISD-plan, såsom beroenden till andra system och till andra organisationer, direktiv om återbruk, gemensamma säkerhetsfunktioner och krav FMV ställer.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	15(76)

Artefakt	ISD-fas	Beskrivning/syfte
ISD-plan	Definiera Realisera	ISD-planen styr projektets informationssäkerhetsarbete med målet att deklarerar IT-systemets informationssäkerhet. Primärt görs informationssäkerhetsdeklarationen för FM och deras ackreditering, men kan också användas för IT-system som inte ska överlämnas till FM (eller för IT-system som ska överlämnas till FM men inte ackrediteras). ISD-planen klargör förutsättningar, vilka aktiviteter som ska genomföras, i vilken omfattning ISD-processen ska användas och vilka roller som behövs.
ISD-I ISD-D ISD-R ISD-V	Identifiera Definiera Realisera Vidmakthålla	ISD-x dokumenterar bedömning av realiserbarhet (alternativt ackrediterbarhet) avseende informationssäkerhet för genomförandeprojektet och systemet. Syftet med dessa dokument är att utgöra ett sammanfattande beslutsunderlag inför T1, T2, T3 och T4.
AU-I AU-D AU-R AU-V	Identifiera Definiera Realisera Vidmakthålla	Syftet med AU-x är att ge ISM, ISA och/eller ISE möjlighet att t.ex. genomföra kompletterande analyser, eller dokumentera viktiga beslut/inriktningar som tagits avseende kravställning eller arkitektur. AU-x kan innehålla; fördjupad analys av förutsättningar, beskrivning av tillämpad metod för kravspårning, redovisning av genomförd kravspårning, motivering av ej tillämpliga krav, förteckning av krav som ska hanteras av evalueraren) samt analys av kravpåverkan från designregler. Strukturellt är AU-x fri att ändra efter behov. AU-x är en bilaga till ISD-x.
ITSS-I ITSS-D ITSS-R ITSS-V	Identifiera Definiera Realisera Vidmakthålla	Syftet med ITSS-x är att dokumentera de krav som ställs på systemet/produkten. I Identifiera förtecknas en grundläggande kravställning, vilken förfinas och tolkas i ITSS-D. I ITSS-R genomförs och dokumenteras hur kraven är uppfyllda samt evalueringen av de ställda kraven. ITSS-V används för att bibehålla en uppdaterad status avseende kravuppfyllnad. ITSS-V används för att spåra eventuella förändringar i kravbild eller i uppfyllanden av denna under vidmakthållfasen. ITSS-V ligger normalt till grund för nytt kravarbete efter T5/modifiering. Strukturen i dessa mallar följer FM ITSS (enligt referens [3]) och ska inte ändras. ITSS-x är en bilaga till ISD-x.
ITSA	Definiera	Syftet med ITSA (IT-säkerhetsarkitektur) är att producera och dokumentera en lämplig IT-säkerhetsarkitektur, vilken grundar sig på kravställningen i ITSS-D. ITSA tas med fördel fram i samarbete med projektets System Engineering. Om FMV avser att upphandla en eller flera leverantörer används ITSA som grund för att ta fram TS- och VÅS-krav. ITSA är en bilaga till ISD-D.
VMH-R	Realisera	VMH-R (Krav på vidmakthållande – Realisera) innehåller en lokal checklista vilken grundar sig på de krav på omgivningen som identifierats i ITSS-D och de krav som kan ha framkommit efter evalueringen i ITSS-R. VMH-R är en bilaga till ISD-R.



Ej sekretess

### ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	16(76)

Artefakt	ISD-fas	Beskrivning/syfte
ISD	Realisera	ISD används av FMV för att deklarerar att IT-systemet uppfyller FM krav på informationssäkerhet såsom specificerat i ITSS-D och är ur ett informationssäkerhetsperspektiv säkert att använda under identifierade förutsättningar. ISD baseras på slutsatserna i ISD-R.
ISD-A Rapport	Avveckla	Syftet med ISD-A Rapport är att redovisa hur avveckling skett.
AU-A	Avveckla	Syftet med AU-A är att göra en analys av vilken typ av information som kan finnas i systemet.

Tabell 4 – ISD-dokument där metodstöd (mallar) finns





Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	17(76)

### 3.5 Relation till FM-processer

Arbete inom ramen för ISD-processen är aktuellt då FMV utvecklar, eller vidmakthåller, informationssystem åt FM. Det är därför av betydelse att förstå hur en del av arbetet bedrivs på FM.

ISD-processen relaterar främst till två processer för IT-systemutveckling på FM:

- FM IT-process (se Referens[4])- Tillämpas för samtliga nya och förändrade IT-tjänster med tillhörande system oavsett leverantör
- FM BMTS (se Referens [5])- Försvarmaktens beslutsmodell för tekniska system

Avsikten med FM BMTS är att ta beslut om utveckling, produktion/anskaffning, användning och avveckling av tekniska system.

För närvarande tillämpas dock inte denna process fullt ut inom FM, men det är den som är beslutad och därför används denna process som referens till arbets sättet inom FM.

Figur 8 visar beslutspunkter i IT-processen och FM BMTS i relation till FMV VHL skeden, T-beslut och ISD-processens faser.



Ej sekretess

ISD 3.1 Processbeskrivning

Datum

Diarienummer

Ärendetyp

2021-05-18

20FMV5903-1:1

3.5

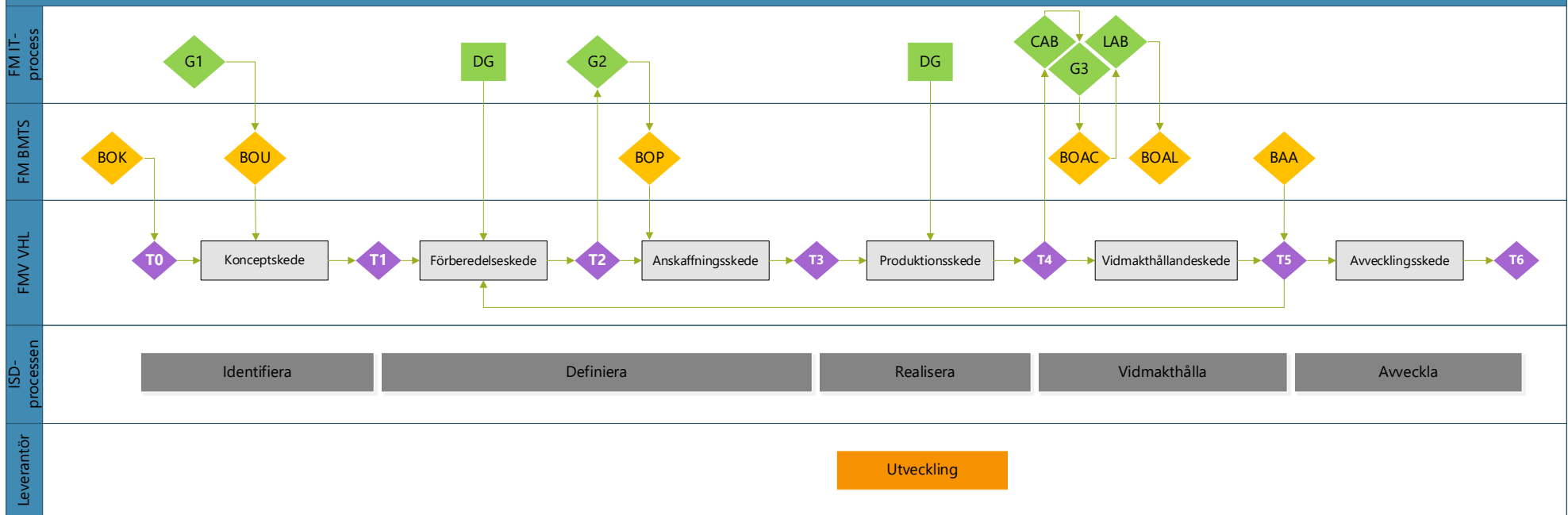
Dokumentnummer

Sida

3.1.0

18(76)

ISD i relation till FMV VHL, FM BMTS, FM IT-Process och FM ackrediteringsprocess



Figur 8 ISD-processen i förhållande till FMV VHL och FM processer

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	19(76)

Översta processraden i Figur 8 illustrerar FM IT-Process samt FM CIO ackrediteringsbeslut. Relevanta beslutspunkter är:

- **G1-beslut**  
FM har identifierat behov av nytt IT-system eller modifiering av befintligt IT-system. G1-beslutsdokument förväntas innehålla information om grundläggande behov och funktionalitet på IT-systemet. För system som redan ingår i Materielplanen kan FM anse att det motsvarar G1-beslut och att därmed inget explicit G1-beslut tas. G1-beslut ger inriktning om det är ett informationssystem, om ackrediterings ska ske, om MUST yttrande krävs samt vad FMV ska leverera inför G2-beslut.
- **DG – Designgenomgång**  
ISD-processen stödjer med skapande av säkerhetsarkitektur och kravställning avseende informationssäkerhetskrav för det IT-system som ska utvecklas. Vid ett eller flera tillfällen under förberedelse- och anskaffningskedet kan designgenomgångar med FM genomföras. En designgenomgång syftar till att lämna stöd och ge fortsatt inriktning inför realisering och ackreditering.
- **G2-beslut**  
Föreslagen lösning med sin nedbrutna kravställning och IT-säkerhetsarkitektur beslutas gälla. Genom beslutet tar Försvarmakten ansvar för föreslagen kravställning och arkitektur. G2-beslutet kan också innehålla krav som ska hanteras innan G3. Detta kan innebära att FMV bör uppdatera sin dokumentation (främst ITSS) i de tidigare faserna Identifiera och Definiera.
- **CAB – Beslut om central ackreditering**  
FM beslutar om central och/eller om lokal ackreditering baserat på bl.a. överlämnat ackrediteringsunderlag. Beslutet kan innehålla information som behöver beaktas av Projektledare, Produktledare och/eller ISM i vidmakthållande-fasen.
- **G3-beslut**  
FM beslutar om ett IT-godkännande, dvs att IT-systemet i framtaget systemet kan vidmakthållas. Beslutet kan innehålla information som behöver beaktas av Projektledare, Produktledare och/eller ISM vid FMV vid vidmakthållandefasen, om FMV fått uppdrag i ärendet, annars motsvarande roller inom Försvarmakten.
- **LAB – Beslut om lokal ackreditering**  
FM beslutar om lokal ackreditering baserat på bl.a. överlämnat ackrediteringsunderlag. Beslutet kan innehålla information som behöver beaktas av Projektledare, Produktledare och/eller ISM i vidmakthållande-fasen.

I nästa processrad i *Figur 8* illustreras FM BMTS. Denna process innehåller beslutspunkter som är länkade mot både FM IT-Process och FMV VHL. Relevanta beslutspunkter är:

- **BOK – Beslut om koncept**  
FM har identifierat behov av förmåga som ett tekniskt system ska lösa, där det ingår ett IT-system enligt G1-beslut. Detta behov kommuniceras till FMV som målsättningar, och med beställning på att ta fram och utvärdera en eller flera olika konceptlösningar. ISD-processen stödjer här med IT-säkerhetsaspekter i urvalet av konceptlösningar samt med realiserbarhetsbedömning av vald lösning.



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	20(76)

- **BOU – Beslut om utveckling**  
FM tar beslut på att föreslaget tekniskt system ska utvecklas och beställer uppdraget av FMV, som tillsammans med underlag från bl.a. ISD-processen tar T1-beslut för att initiera ett eller flera genomförandeprojekt.
- **BOP – Beslut om produktion**  
FM har fått underlag av FMV som är till belåtenhet och tar beslut om att tilltänkta leverantörer kan kontrakteras för att utveckla systemet. Detta beslut, tillsammans med bl.a. underlag från ISD-processen, används för att ta T3-beslut som initierar arbetet med utveckling och verifiering av informationssystemet. ISD-processen stödjer här med IT-säkerhetsaspekter under utveckling, samt säkerhetsvärdering av det framtagna IT-systemet. Resultatet av detta ISD-arbete utgörs av ett ackrediteringsunderlag som via T4-beslut överlämnas till FM.
- **BOAC – Beslut om central ackreditering**  
FM beslutar att systemet får användas inom FM under iakttagande av utfärdade instruktioner och angivna restriktioner. Beslutet kan innehålla information som behöver beaktas av Projektledare, Produktledare och/eller ISM i vidmakthållande-fasen.
- **BOAL – Beslut om lokal ackreditering**  
Efter att alla förutsättningar finns på plats tas beslut om användning lokalt på varje verksamhetsställe som operativt ska använda systemet. Besluten kan innehålla information som behöver beaktas av Projektledare, Produktledare och/eller ISM i vidmakthållande-fasen.

Mellersta processrad i Figur 8 visar FMV VHL med de tekniska T-beslut som är relevanta för ISD-processen. VHL innehåller också andra typer av beslutspunkter; investering (I-beslut), affärsbeslut (A-beslut) samt kundavtalsbeslut (K-beslut). I-, A- och K-beslut relaterar på olika vis mot T-besluten, men har ingen koppling till de tekniska T-beslut som ISD-processen relaterar till. Följande T-beslut är relevanta för ISD-processen 3.1:

- **T0 - Beslut om att fastställa förmågebehov som grund för FMV:s arbete**  
Detta beslut inleder ISD-fasen Identifiera.
- **T1 - Beslut om att fastställa Systemdefinition**  
ISD-I med dess bilagor är beslutsunderlag till T1. Genom T1-beslutet avslutas ISD-fasen Identifiera och ISD-fasen Definiera påbörjas.
- **T2 - Beslut om att fastställa tekniskt underlag för anskaffning**  
ISD-D med dess bilagor är beslutsunderlag till T2. Efter T2 kan det bli aktuellt med uppdatering av ISD-D inför T3.
- **T3 - Beslut om att fastställa tekniskt underlag för produktion**  
ISD-D (eventuellt reviderad efter T2) med dess bilagor är beslutsunderlag till T3. Genom T3-beslutet avslutas ISD-fasen Definiera och ISD-fasen Realisera påbörjas.
- **T4 - Beslut om att fastställa typunderlag inklusive fastställd konfiguration för överlämning**  
ISD deklarerar att FMV anser att IT-systemet som levereras till FM uppfyller de ställda informationssäkerhetskraven, och att informationssäkerhetsarbetet har genomförts i enlighet med produktområdets ISD-strategi samt att ISD-processen följts såsom specificerats i ISD-planen. ISD är en sammanfattning av ISD-R med dess bilagor(AU-R,



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	21(76)

ITSS-R och VMH-R), och är beslutsunderlag till T4. Genom T4-beslutet avslutas ISD-fasen Realisera. ISD-fasen Vidmakthålla påbörjas efter beställning från Försvarsmakten.

- **T5 - Beslut om konfiguration för genomförande av modifiering eller avveckling**

Utöver ovanstående T-beslut finns också T6 (Beslut om att avveckling är genomförd), som inte relaterar till denna version av ISD-processen.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	22(76)

### 3.6 Kravhantering i ISD-processen

Generellt är kravhantering (kravfångst, -formulering, sammanställning, allokering, spårning och verifiering) centralt i utveckling av säkra IT-system. Inledningsvis tas krav fram som systemet måste uppfylla för att bli säkert. Dessa krav ställs, efter bearbetning, till leverantör (-er) som utvecklar systemet. Leverantören redovisar kravuppfyllnad, vilken kompletteras med evaluerarens egen analys och redovisning av kravuppfyllnad avseende informationssäkerhet. Detta tillvägagångssätt, för att utveckla säkra IT-system, tillämpas av KSF 3.1. ISD-processen ger FMV stöd att efterleva detta i de olika VHL-skedena.

I KSF 3.1 specificeras ett dokument kallat IT-säkerhetsspecifikation (ITSS), till struktur och innehåll. ISD-processen använder samma begrepp på kravdokumentet ITSS-X, med ett suffix för att påvisa var i processen systemet befinner sig (Identifiera, Definiera, Realisera respektive Vidmakthålla). Syftet med detta är att FMV sak kunna använda FM ITSS som indata med rätt struktur, för att därefter vidare förädla samt granska kraven. FMV levererar i Realisera en ITSS-R, som till innehåll och struktur direkt kan användas av FM i vidare ackreditering och vidmakthållande.

ITSS i ISD-processen utvecklas i tre steg:

Steg ett är ITSS-I, där FM ITSS och krav från FMV kan vara indata, vilken innehåller:

- övergripande systembeskrivning
- Sammanställning av säkerhetskrav på både IT-systemet och driftsmiljön (IT-systemets omgivning).

Steg två är ITSS-D. Även i detta steg kan FM SM och ITSS vara indata i de fall konceptskedet inte har genomförts. ITSS-D innehåller:

- Utvecklad systembeskrivning
- Sammanställning av säkerhetskrav på både IT-systemet och driftsmiljön (IT-systemets omgivning)
- Tolkning av sammanställda säkerhetskrav på IT-systemet.

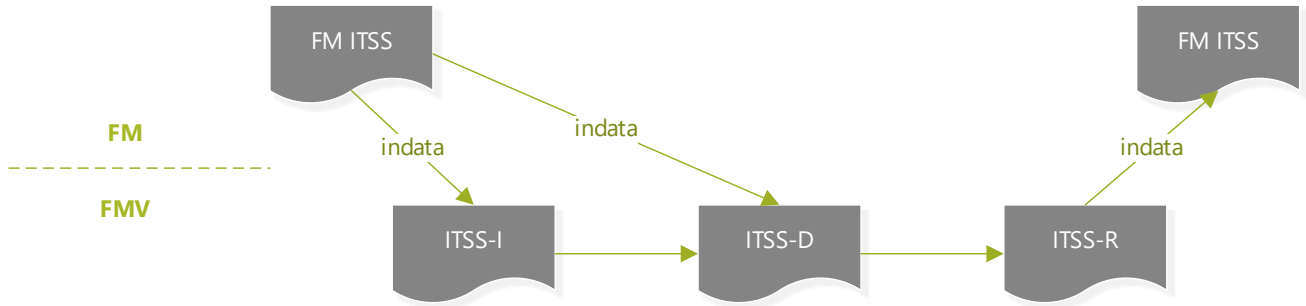
Syftet med detta steg är att utgöra underlag för utveckling av IT-systemet, genom att ligga till grund för de IT- och informationssäkerhetskrav som ska föras in i Teknisk Specifikation (TS) respektive Verksamhetsåtagandespecifikation (VÅS).

Tredje steget är ITSS-R. Denna innehåller:

- Slutlig systembeskrivning
- Sammanställning av säkerhetskrav på både IT-systemet och driftsmiljön (IT-systemets omgivning)
- Tolkning av sammanställda säkerhetskrav på IT-systemet
- Uppfyllnad av de säkerhetskrav som ställts på IT-systemet.

ITSS-R används som underlag inför FM beslut om ackreditering (BOAC/CAB) och kan både till struktur, såväl som innehåll, användas av FM som beslutsunderlag.

Figur 9 nedan illustrerar stegen i kravarbetet via respektive ITSS, både FM och FMV.



Figur 9 Kravflöde genom nyttjande av ITSS

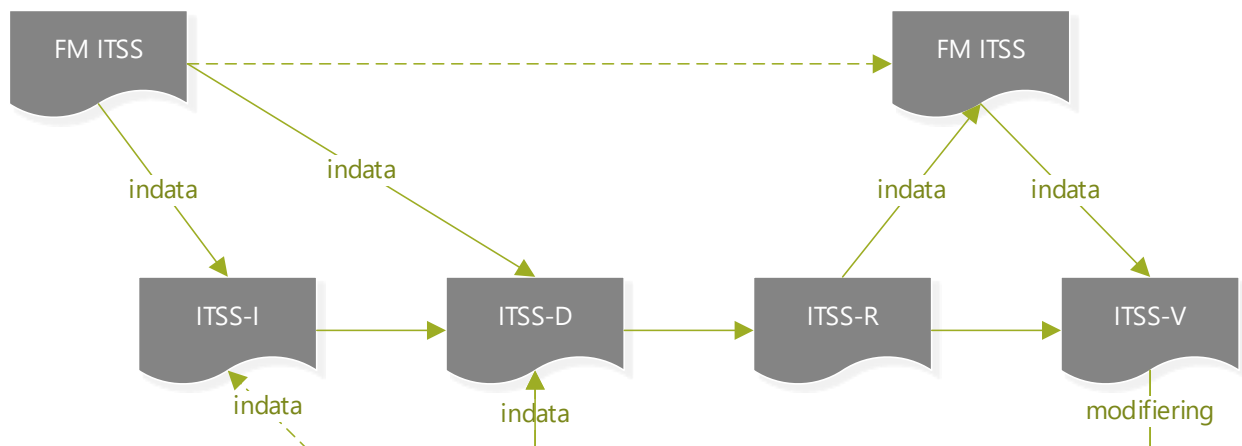
I de fall då FMV har ett åtagande att vidmakthålla systemet, kan ITSS-V nyttjas för att bibehålla spårbarhet i kravarbetet. I dessa fall utgår ITSS-V från den ITSS som FM tagit beslut om ackreditering på, och underhålls därefter av FMV.

ITSS-V innehåller då:

- Uppdaterad systembeskrivning
- Ev. modifierad sammanställning av säkerhetskrav på både IT-systemet och driftsmiljön (IT-systemets omgivning).
- Ev. modifierad tolkning av sammanställda säkerhetskrav på IT-systemet
- Ev. modifierad uppfyllnad av de säkerhetskrav som ställts på IT-systemet.

Vid behov av större modifiering av systemet används ITSS-V som indata till ny ITSS-I (i de fall det ska göras ett nytt konceptarbete) eller ITSS-D (då samma koncept gäller för den förestående modifieringen).

Figur 10 illustrerar detta flöde.



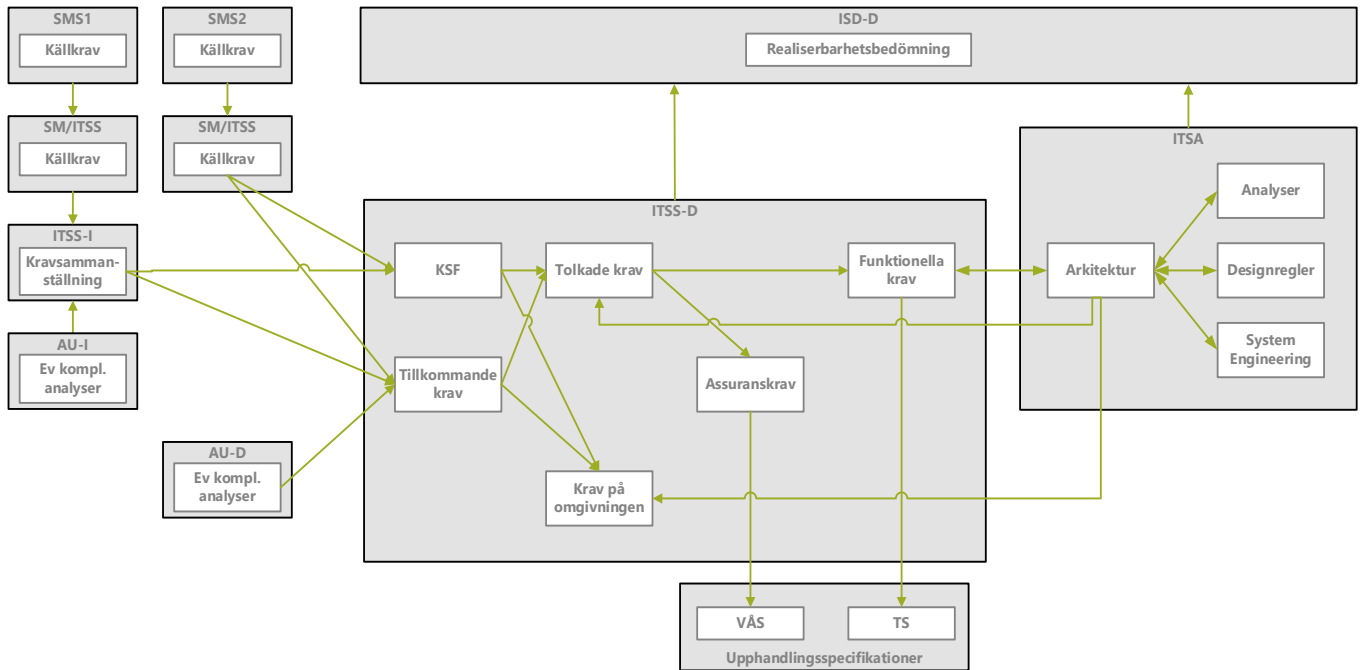
Figur 10 Kravflöde genom nyttjande av ITSS vid vidmakthållande och modifiering

Observera att Figur 9 och Figur 10 inte beskriver hur kraven förmedlas till leverantör (-er) via TS och VÅS.

Figur 11 nedan, illustrerar ett generellt kravflöde i Definiera-fasen. Ingående krav kommer från FM i form av ITSS innehållande SSB. Dessa kan komma att tas fram i konceptfasen, via FM

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	24(76)

SMS1, och kan då bearbetas i ITSS-I. I de fall ISD-arbetet inte föregås av en konceptfas, är det inte heller aktuellt med ISD Identifiera-fas. De relevanta delarna av ISD-I utförs då i Definiera där kraven från FM kommer i form av ITSS och SSB från FM SMS2.



Figur 11 Kravhantering i Definiera-fasen

I Definiera sammanställs källkraven i ITSS-D. Den första gallringen utgörs av de krav som omhändertas av säkerhetsfunktioner i systemet omgivning. Dessa krav på omgivningen hanteras vidare i dokumentet VMH-R i Realisera-fasen.

När gallringen av krav på omgivning har genomförts tolkas de sammanställda säkerhetskraven. Här särskiljs funktionella säkerhetskrav, som itereras mot den tänkta IT-säkerhetsarkitekturen i ITSA, och assuranskraven som anpassas mot VÅS (en eller flera).

De funktionella säkerhetskraven bearbetas och allokeras (ofta genom flera iterationer) gentemot arkitekturen och övriga relevanta krav i form av t.ex. designprinciper och designregler. I detta processteg är det viktigt att kraven anpassas mot den övrigripande systemlösningen som normalt hanteras inom System Engineering.

Från Definiera-fasens kravhantering kommer följande resultat:

- Realiserbarhetsbedömning av systemet, i ISD-D
- Teknisk kravställning och assuranskrav mot leverantör (TS respektive VÅS)
- Krav på omgivningen (indata till VMH-R)
- IT-säkerhetsarkitektur (ITSA)

Notera att ITSS-D eller andra ISD-underlag inte ska användas för upphandling. Det är TS/VÅS eller anpassade underlag som utgör underlag för upphandling/anskaffning. ISD-underlagen är





**Ej sekretess**

## **ISD 3.1 Processbeskrivning**

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	25(76)

projektledarens sätt att följa upp hur kravhantering, och i senare skede även hur evaluering av informationssäkerheten, framskrider i projektet.

Det är också av vikt att notera att den faktiska kravhanteringen med fördel sker i ett dedikerat verktyg för ändamålet, exempelvis Doors eller Enterprise Architect. Det är möjligt att genomföra enklare kravarbeten i t ex Excel, även om det inte är ett dedikerat kravhanteringsverktyg. Det är omfattningen och komplexiteten i projektet som styr valet av kravhanteringsverktyg.

Resultatet från kravarbetet ska dokumenteras i avsedda underlag, såsom ITSS-D och ITSA. Nödvändiga analyser, beslut och ställningstaganden som är av vikt för spårbarheten avseende kravarbetet ska dokumenteras i AU-R.

För att kravarbetet i ISD ska ge önskvärt resultat förutsätter det att informationssäkerhetsarkitekten (ISA) uppfyller de kompetenskrav som anges i kapitel 4.1.2



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	26(76)

### 3.7 ISD - definition av oberoende

I syfte att ge möjlighet för FMV att utge en ISD till FM för ett system, är det av vikt att kunna påvisa ett antal aspekter i genomförandeprojektet:

- Att FMV har genomfört informationssäkerhetsarbetet enligt ISD-processen
- Att det finns spårbarhet i kravhanteringen
- Att FMV evaluering är oberoende gentemot leverantör (-er)

Upprätthållandet av ISD-planen hanteras primärt av *Information Security Manager* (ISM, se kapitel 4.1.1). Spårbarheten i kravarbetet genomförs primärt av *Information Security Architect* (ISA, se kapitel 4.1.2).

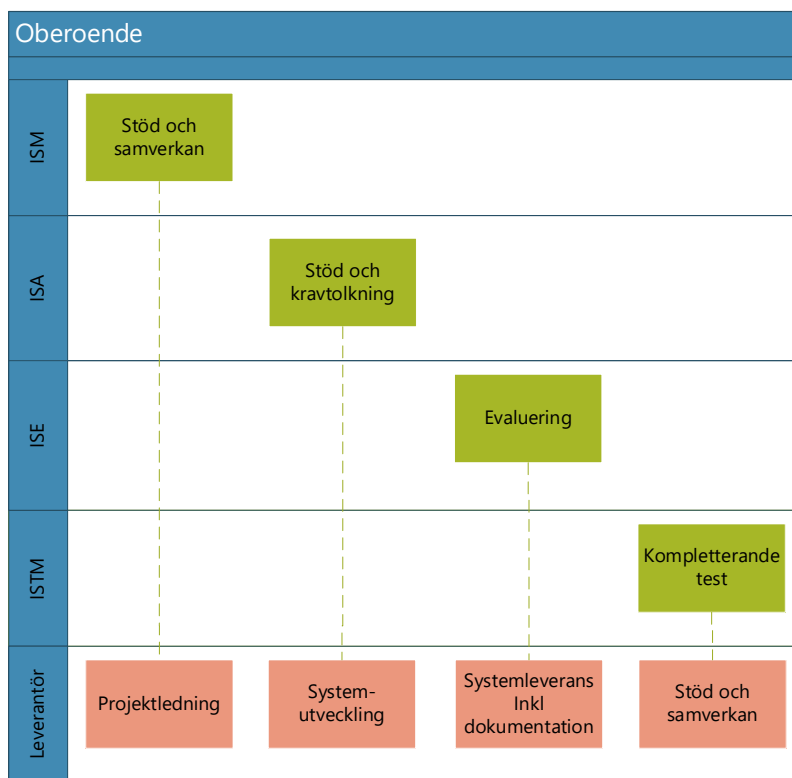
Oberoendet hanteras av *Information Security Evaluator* (ISE) och dennes granskning av leverantör (-ers) system- och assurancesunderlag. ISEs arbete kompletteras av *Information Security Test Manager* (ISTM) för att genom test verifiera systemleverantörs (-ers) systemunderlag.

Följande krav finns avseende ISD-roller mot leverantör (-er):

- ISM: kan t ex stödja leverantör i fråga om övergripande projektledning
- ISA: kan t ex stödja leverantör i fråga om kravtolkning och möjlig realisering (designbeslut)
- ISE: granskar leverantörens system- och assurancesunderlag samt evaluerar säkerhetslösningen i systemet
- ISTM: testar/verifierar leverantörs utlåtande om kravuppfyllnad

Ingen av rollerna ISM, ISA, ISE eller ISTM ska vara delaktiga, eller ha egna intressen, i realiseringen av systemet.

Figur 12 visar översiktligt interaktionen mellan FMV och ISD mot leverantör.



Figur 12 ISD oberoende mot leverantör

ISEs roll i ISD-processen är styrande för att FMV ska kunna hävda oberoende från leverantör gentemot FM och därigenom ge assurans till systemets säkerhetsfunktionalitet. ISE tar i sin tur stöd i ISTM arbete med verifiering för att kunna hävda oberoendet.

ISE kan, om behov finns, använda leverantörs utlåtande om kravuppfyllnad, men då endast som ingångsvärden för sin egen evaluering.

Värdet på assurans är svårt att kvantifiera, men stöd ges i de aktiviteter som krävs genom KSF. Dessa aktiviteter förtecknas i AU-D och redovisas i AU-R, och ligger därefter till grund för ackrediterbarhetsbedömning i ISD-R.

Den lägsta nivån på ISE evalueringsaktiviteter bestäms av definierad kravnivå, och omfattar bland annat granskning av leverantörs (-ers) dokumentation, egna analyser, kompletterande tester (ev. genom ITSM) samt restrisikanalyser och sårbarhetsanalyser.

Ansvarsområden och kompetenskrav på ISE och ISTM beskrivs i kapitel 4.1.3 respektive 4.1.4.

I de fall det finns ytterligare krav på oberoende granskning kan SystGL genomföra s.k. Oberoende systemgranskning (OSG) enligt särskild process. OSG kan både genomföras i Definierafasen och Realiserafasen. OSG är inte en del av ISD-processen, då denna ska kunna genomföras som en oberoende aktivitet (se kapitel 4.3.3).

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	28(76)

## 4 Roller

### 4.1 ISD-roller

ISD-processen definierar olika roller för att tydliggöra kompetensbehovet att utföra specifika aktiviteter i ISD-arbetet:

- ISM – Information Security Manager
- ISA – Information Security Architect
- ISE – Information Security Evaluator
- ISTM – Information Security Test Manager.

Underavsnitten som följer definierar respektive roll med ansvar och uppgifter samt dess kompetenskrav.

#### 4.1.1 ISM – Information Security Manager

ISM är den roll som är ansvarig för helheten avseende ISD-arbetet och utgör FMV Projektledares kontaktyta mot ISD-delprojektet.

Den som innehar ISM-rollen bör vara utsedd som delprojektledare och därmed även ingå i projektledningen.

ISM ansvar och uppgifter omfattar att:

- Ansvara för planering, koordinering och ledning av ISD-arbetet
- Producera och vidmakthålla ISD-plan (koordinerat med projektledaren och projektets SE-ansvarig samt representanter för övriga relevanta discipliner)
- Producera Informationssäkerhetsdeklaration (ISD)
- Identifiera och förmedla risker avseende ISD-arbetet och säkerheten i systemet
- Hantera risker utpekade av projektledaren
- Stödja framtagning av ISD-strategi och ISD-I (med bilagor)
- Genomföra realiserbarhetsbedömningar (ISD-I, ISD-D, ISD-R och ISD-V)
- Stödja framtagning av
  - Analysunderlag (AU-I, AU-D, AU-R och AU-V)
  - IT-säkerhetsarkitektur (ITSA)
  - ITSS (ITSS-I, ITSS-D, ITSS-R och ITSS-V)
  - Vidmakthållande (VMH-R)
- Stödja säkerhetstestning.

Kompetenskrav för person som har rollen som ansvarig ISM:

- Minst 5 års erfarenhet inom de kompetensområden som definierar denna roll
- Informationssäkerhet; certifierad CISM eller likvärdigt
- God kunskap om ISD-processen
- God kunskap om projektledning
- God dokumentationsteknik



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	29(76)

- Kännedom om FM KSF
- God kännedom om relevanta systemutvecklingsprocesser.

Dessutom är det lämpligt att den som arbetar som ISM även har kompetens inom följande områden:

- God kunskap om projektsäkerhetsskydd
- Kunskap om granskningsmetodik
- God kunskap om FMV verksamhetsledningssystem (VHL) och relevanta FM processer (t.ex. IT-processen, ackrediteringsprocessen och FM Beslutsmodell Tekniska system (FM BMTS))
- Teknisk domänkunskap inom FMV och FM (t.ex. IT-system, designregler, godkända komponenter och signalskydd)
- FM domänkunskap (t.ex. fysiska miljöer, personal, doktrin och verksamheter).

### 4.1.2 ISA – Information Security Architect

ISA är den roll som är ansvarig för krav- och designarbetet avseende säkerhetskrav och säkerhetsarkitektur.

ISA ansvar och uppgifter omfattar:

- Ansvar för att utforma IT-säkerhetsarkitekturen (ITSA) och att i detta arbete samarbeta med System Engineering
- Ansvar för kravnerbrytning och tolkning avseende informationssäkerhetskrav (ITSS-I, ITSS-D, ITSS-V och säkerhetskraven i TS/VÅS) och att i detta arbete samarbeta med System Engineering
- Att genomföra kompletterande analyser (AU-I och AU-D)
- Stödja framtagning av ISD-plan
- Stödja framtagning av ISD-strategi
- Stödja framtagning av realiserbarhetsbedömningar (ISD-I och ISD-D)
- Stödja utvärdering av leverantörsanbud
- Stödja leverantören med att svara på frågor och diskutera säkerhetslösningar.

Kompetenskrav för person som har rollen som ansvarig ISA:

- Minst 5 års erfarenhet inom de kompetensområden som definierar denna roll
- Informationssäkerhet motsvarande certifierad CISSP, CPRE
- Requirements Engineering inom IT (kravformulering, -hantering, -metodik och -verktyg)
- God kunskap om ISD-processen
- God dokumentationsteknik
- God kunskap om MUST KSF.

Dessutom är det lämpligt att den som arbetar som ISA även har kompetens inom följande områden:

- System Engineering inom IT (arkitektur, design, implementation och verifiering)



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	30(76)

- Teknisk domänkunskap inom FMV och FM (t.ex. IT-system, kommunikationsprotokoll, designregler, godkända komponenter och signalskydd)
- FM domänkunskap (t.ex. fysiska miljöer, personal, doktrin och verksamheter).

### 4.1.3 ISE – Information Security Evaluator

ISE är den roll som är ansvarig för evaluering av säkerheten i det utvecklade systemet.

ISE ansvar och uppgifter omfattar att:

- Ansvara för att utföra evaluering av både system och leverantörens arbete (AU-R, AU-V, ITSS-R och ITSS-V) och dokumentera detta
- Specificera säkerhetskrav för vidmakthållande (VMH-R)
- Stödja framtagning av ISD-plan
- Stödja framtagning av realiserbarhetsbedömningar (ISD-R och ISD-V)
- Ge inriktning/förslag till ISTM för vad som bör testas.

Kompetenskrav för person som har rollen som ansvarig ISE:

- Minst 5 års erfarenhet inom de kompetensområden som definierar denna roll
- Informationssäkerhet; certifierad CISA eller införskaffat motsvarande kompetens på annat sätt.
- God kunskap om ISD-processen
- God granskningsmetodik
- God dokumentationsteknik
- God kunskap om MUST KSF
- Kunskap om test och verifiering inom IT.

Dessutom är det lämpligt att person som arbetar som ISE även har kompetens inom följande områden:

- Requirements Engineering inom IT (kravformulering, -hantering, -metodik och -verktyg)
- Teknisk domänkunskap inom FMV och FM (t.ex. IT-system, kommunikationsprotokoll, designregler, godkända komponenter och signalskydd)
- FM domänkunskap (t.ex. fysiska miljöer, personal, doktrin och verksamheter).

### 4.1.4 ISTM – Information Security Test Manager

ISTM är den roll som är ansvarig för säkerhetstestning av det utvecklade systemet.

ISTM ansvar och uppgifter omfattar att:

- Ansvara för planering, koordinering, utförande och ledning av arbetet med säkerhetstestning
- Samverka med FMV T&E
- Ansvara för framtagningen av testplan och testspecifikationer
- Ansvara för rapporteringen av testresultat
- Stödja framtagning av ISD-plan.

Kompetenskrav för person som har rollen som ansvarig ISTM:



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	31(76)

- Minst 5 års erfarenhet inom de kompetensområden som definierar denna roll
- Informationssäkerhet; certifierad CISSP, CISA eller införskaffat motsvarande kompetens på annat sätt
- Mycket god kunskap om säkerhetstestning av IT-system (t.ex. sårbarhetsanalys, kodgranskning, penetrationstestning, metodik och verktyg)

Dessutom är det lämpligt att person som arbetar som ISTM även har kompetens inom följande områden:

- Kunskap om projektledning
- God dokumentationsteknik
- Mycket god kunskap om test och verifiering inom IT.

## 4.2 Tillsättning av ISD-roller

Arbetsuppgifterna som ingår i respektive ISD-roll kräver viss specifik kompetens enligt vad som definierades i föregående avsnitt. Tillsättning av rollerna i ett ISD-projekt ska göras enligt följande regler:

- Personen ska vara oberoende från leverantörerna av systemet
  - Oberoendet innebär att personen inte får ta designbeslut för leverantörs räkning
  - Det är däremot tillåtet att personen stödjer leverantör med att svara på frågor och diskutera lösningar under projektets gång
- En person som innehar tillräcklig kompetens kan tillsätta rollen
- En person kan tillsätta fler än en roll
- En roll kan tillsättas av flera personer. I detta fall måste det finnas en som är utpekad som ansvarig.

## 4.3 FMV-roller med anknytning till ISD-processen

### 4.3.1 Produktledare (PrL)

Produktledare har inom FMV designverksamheten ett, från C VerkO delegerat, designansvar för specificerat område eller produkt med befogenheter enligt dokumenterat delegat. Se arbets- och delegeringsordning för aktuellt VerkO avseende beskrivning av uppgifter och ansvar.

Produktledare har ansvaret för det initiala ISD-arbetet som sker under ISD-processens Identifiera-fas. Stöd för ISD-arbetet kan då erhållas från:

- ISD-rollerna ISM och ISA
- Metodföreträdaren för IT-säk (MetF IT-säk)
- Kravföreträdaren för IT-säk (KravF IT-Säk)
- Systemgranskningsledare IT-säk (SystGL IT-säk).

### 4.3.2 Projektledare (PL)



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	32(76)

Projektledare utses per genomförandeprojekt och vidmakthållandeprojekt. Uppdraget styrs av projektdirektiv.

Projektledaren har ansvaret för att genomförandet av ISD-arbetet sker enligt ISD-processen. Stöd för genomförande av ISD-arbetet fås från ISD-rollerna ISM, ISA, ISE och ISTM.

### 4.3.3 Systemgranskningsledare IT-säk (SystGL IT-säk)

SystGL IT-säk finns utsedd på vissa VerkO med uppdrag att bl.a. kvalitetssäkra ISD-arbetet oberoende från projektarbetet. Se arbets- och delegeringsordning för aktuellt VerkO avseende beskrivning av uppgifter och ansvar.

Avseende ISD-processen kan SystGL IT-säk vara stöd till projektet i frågor rörande ISD, IT-säkerhet och informationssäkerhet. SystGL IT-säk kan även genomföra oberoende systemgranskning (OSG) i syfte att godkänna dokument från genomfört ISD-arbete inför deras fastställande.

## 4.4 Övriga roller

### 4.4.1 FM MOA

Materielområdesansvarig (MOA) för aktuellt materielområde är beställarens representant. Det är MOA som tillhandahåller beställningen med dokumentationen som specificerar vad det är FMV ska leverera.

Vidare är det MOA som avgör vilka kontakter projektet ska ha med andra på FM, t.ex. med handläggare på FM CIO och MUST. Det är till MOA som FMV ställer krav på kompletterande information rörande indata och direktiv för beställt system.

### 4.4.2 Leverantör

Leverantör är den organisation som utvecklar hela eller delar av systemet. Under ett genomförande- eller vidmakthållandeprojekt kan det finnas en eller flera leverantörer som utvecklar olika delar av systemet. Leverantör kan vara ett företag, flera företag eller del av FMV.

Leverantör kallas även för systemutvecklare.

Leverantör av systemet skall utse kontaktperson för informations säkerhetsrelaterade frågor. Beroende på omfattningen av projektet bör leverantör också utse följande roller:

- Systemarkitekt
- Testledare

I de fall FMV är integratör gäller motsvarande krav.

## 4.5 Ansvarsfördelning för ISD-arbete

Tabell 5 definierar ansvarsfördelningen för ISD-relaterade dokument och information. Följande ansvar fördelas i tabellen:

X = Beslutande

Ytterst ansvarig för innehållet och medger att dokumentet får formell status. Godkänner dokumentet inför fastställande.



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	33(76)

F = Föredragande

Tar fram dokumentet själv eller med hjälp av andra. Den som står för innehållet kan muntligen föredra för beslutande vid behov. Bekräftar med sin signatur att det är framtaget enligt tillämpliga FMV-processer.

S = Samråd

Granskar dokumentets innehåll och säkerställer att innehållet tagits fram på rätt sätt och att rätt sakkunskap har använts. Kan ta hjälp med granskning vid behov.

ISD-rollerna ISM, ISA, ISE och ISTM är avskilda av ett tjockare kolumnstreck i Tabell 5. Detta illustrerar att det beror av var processarbetet betraktas och därmed vilket ansvar som tilldelats. T.ex. kan ISM vara föredragande inför Projektledaren inom ISD-arbetet, medan det är Projektledaren som är föredragande i projektet inför beslutande roll. ISM dock alltid ansvarig för ISD dokument inför Produktledare eller Projektledare.

ISD-fas	Artefakt/information	Enl. del. ordn. <sup>2</sup>	PrL	PL	ISM	ISA	ISE	ISTM
Identifiera	ISD-strategi	X	F		F	S		
Identifiera	ISD-I	X	F		F	S		
Identifiera	AU-I	X	F		S	F		
Identifiera	ITSS-I	X	F		S	F		
Definiera	ISD-plan	X		F	F	S		
Definiera	ISD-D	X		F	F	S		
Definiera	AU-D	X		F	S	F		
Definiera	ITSA	X		F	S	F		
Definiera	ITSS-D	X		F	S	F		
Definiera	Säkerhetskrav till TS/VÄS	X		F	S	F		
Realisera	ISD-plan	X		F	F		S	S
Realisera	ISD	X		F	F		S	
Realisera	ISD-R	X		F	F		S	
Realisera	AU-R	X		F	S		F	
Realisera	ITSS-R	X		F	S		F	
Realisera	VMH-R	X		F	S		F	
Realisera	Testdokumentation säkerhetstestning	X		F	S		S	F
Vidmakthålla	ISD-V	X		F	F		S	
Vidmakthålla	AU-V	X		F	S		F	
Vidmakthålla	ITSS-V	X		F	S		F	
Vidmakthålla	Testdokumentation säkerhetstestning	X		F	S		S	F

Tabell 5 – Ansvarsmatrix

<sup>2</sup> Enligt gällande delegeringsordning på aktuellt Verksamhetsområde (VerkO) på FMV eller, om det inte är definierat där, av Teknisk Chef (TC).

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	34(76)

## 5 Fördjupad processbeskrivning

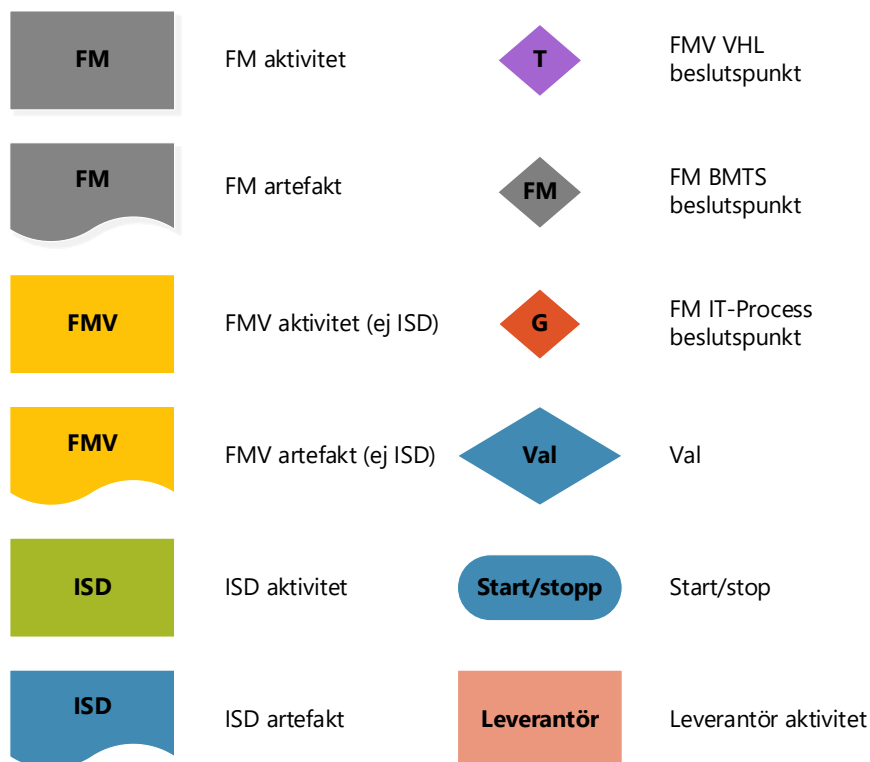
ISD-Processen är aktivitetsbaserad, vilket innebär att för varje skede i produktprocessen beskrivs de aktiviteter som bör göras i informationssäkerhetsarbetet, samt vilka roller som bör utföra dem. Rollerna är angivna som en indikation på var ansvaret för aktiviteterna finns.

Notera att de övergripande och detaljerade processbeskrivningarna i detta kapitel utgår från ISD-processens perspektiv. Dessa processbeskrivningar avser inte att beskriva FMV VHL i sin helhet, och inte heller FM:s olika beslutsprocesser.

De T-beslut som utgör kopplingen mellan FMV VHL och ISD-processen, är de anknytningspunkter som är väsentliga för att dessa två processer ska fungera tillsammans.

Notera också att processbeskrivningarna i detta kapitel är av en generell natur, då det inte är möjligt att här påvisa olika möjligheter att justera processen för specifika genomförandeprojekt. Det åligger ISM att i dennes planering utgå från dessa processbeskrivningar och anpassa ISD-planeringen för det aktuella genomförandeuppdraget. Denna anpassade projektbeskrivning ska dokumenteras i ISD-planen, som också ska uppdateras vid behov.

I detta kapitel används följande symboler<sup>3</sup>:



Figur 13 Symbolförklaring

<sup>3</sup> Processbeskrivningen kan med fördel läsas i färg, men det är inget krav då beskrivningarna inte bygger på symbolernas färgmarkering. Aktiviteter och dokument framgår av respektive roll.



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	35(76)

## 5.1 Identifiera

I Identifiera genomför Produktledare aktiviteter med stöd av en ISD-kompetens motsvarande ISM. Produktledare från olika VerkO styrs av det VerkO som har huvudprojektet och dess delegeringsordning. ISD-arbetet ska resultera i att förutsättning och inriktning kan ges till ett (eller flera) genomförandeprojekt. Tack vare den första realiserbarhetsbedömningen säkerställs att inga genomförandeprojekt startar utan att rätt förutsättningar finns. Samverkan i gränstorna mellan FM och FMV Produktledare, samt mellan Produktledare och Projektledare, är viktiga för det fortsatta arbetet för att säkerställa att samtliga parter har förstått varandras behov.

### 5.1.1 Övergripande fasbeskrivning

ISD-fasen Identifiera sammanfaller med FMV VHL Konceptskede. ISD-arbetet kan starta genom två olika T-beslut.

I de fall FM beställer ett konceptarbete av FMV startar ISD Identifiera genom beslut T0.

Det kan också finnas fall då FMV tagit T5-beslut om Modifiering, som är av sådan art att ett nytt konceptarbete behöver genomföras. I dessa fall startar ISD Identifiera efter T5-beslutet.

Indata från FM i fallet då ISD startar i T0 är normalt sett FM Systemmålsättning 1 (SMS1) och SSB. Denna kan, beroende på mognadsgrad, innehålla en ITSS vilken då styr FMVs ISD-arbete i denna fas. Indata som krävs från FM är även om det är ett informationssystem, om det ska ackrediteras och vad som är ackrediteringsobjektet. G1 beslut innehåller normalt dessa uppgifter.

Identifiera avslutas genom FMV T1-beslut, där ISD-I är ett beslutsunderlag.

I Konceptskedet kan ett antal förslag på systemdesign tas fram. Dessa presenteras för FM som genom beslut BOU väljer vilket koncept som ska gälla. I samband med BOU tar FM även fram SMS2 vilken innehåller den gällande kravbilden på systemet. FMV stödjer FM inför beslut BOU, där även ISD bidrar med information.

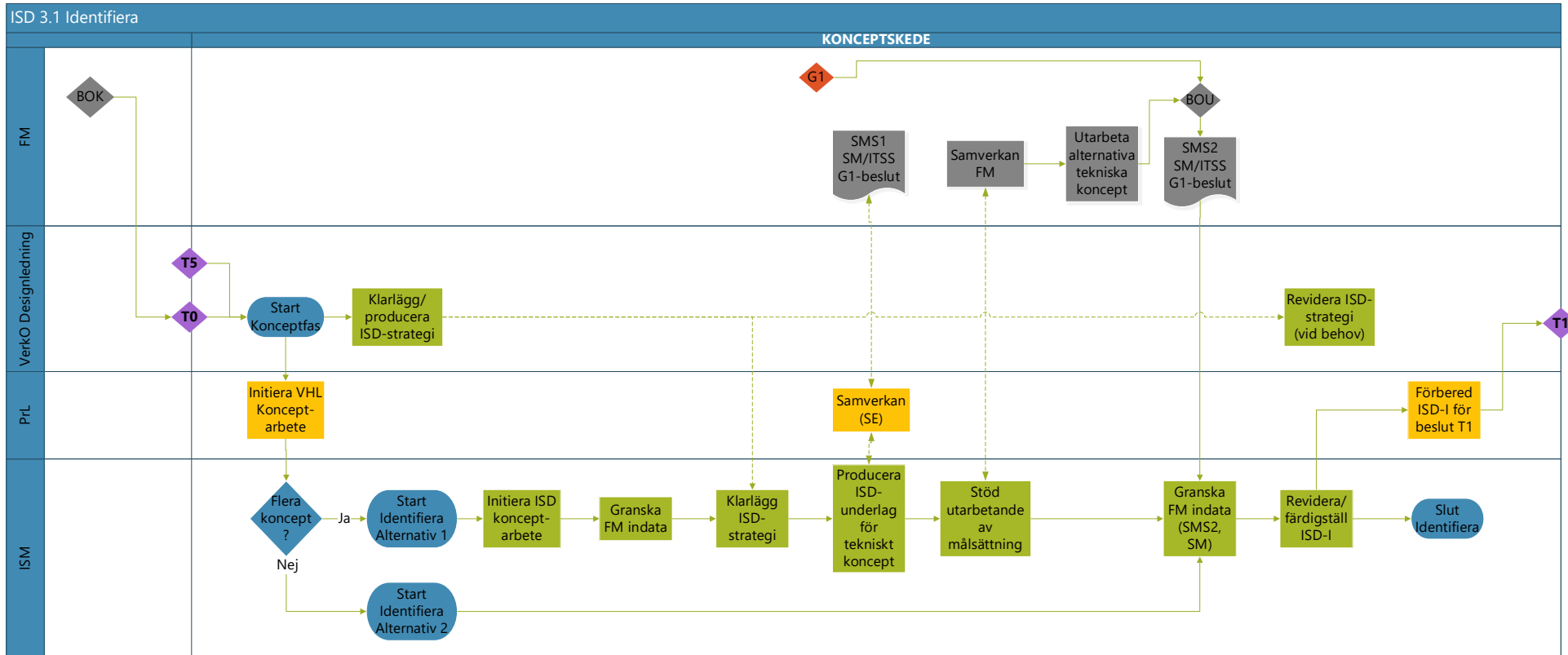
Inom Identifierafasen klarlägger också Produktledare om det finns en tillämplig ISD-strategi för det genomförandeprojekt som planeras. Finns ingen tillämplig ISD-strategi tas denna fram av Produktledare. Figur 14 nedan visar översiktligt aktiviteterna i Identifiera-fasen.



Ej sekretess

ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	36(76)



Figur 14 Översikt av aktiviteter i Identifiera-fasen

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	37(76)

Tabell 6 sammanfattar ISD Identifiera-fas.

Identifiera	VHL T0 till T1
Syfte	Säkerställ FMV åtagande inför genomförandeprojekt
ISD-aktiviteter	Klarlägg/producerera ISD-strategi Initiera ISD konceptarbete Granska FM indata (SMS1) Klarlägg ISD-strategi Genomför konceptarbete för informationssäkerheten Producerera ISD-underlag för tekniskt koncept Stöd utarbetande av FM målsättning Granska FM indata (SMS2) Revidera/färdigställ ISD-I Revidera ISD-strategi (vid behov)
ISD dokument <sup>4</sup>	ISD-strategi ISD-I AU-I ITSS-I
Indata	FM krav (SMS1, SMS2, SM, ITSS, TTEM, SYD, mm)
Utdata	ISD-strategi ISD-I AU-I ITSS-I
Aktiva roller	FM Verko Designledning PrL ISM

Tabell 6 – Sammanställning ISD Identifiera

## 5.1.2 Detaljerad fasbeskrivning

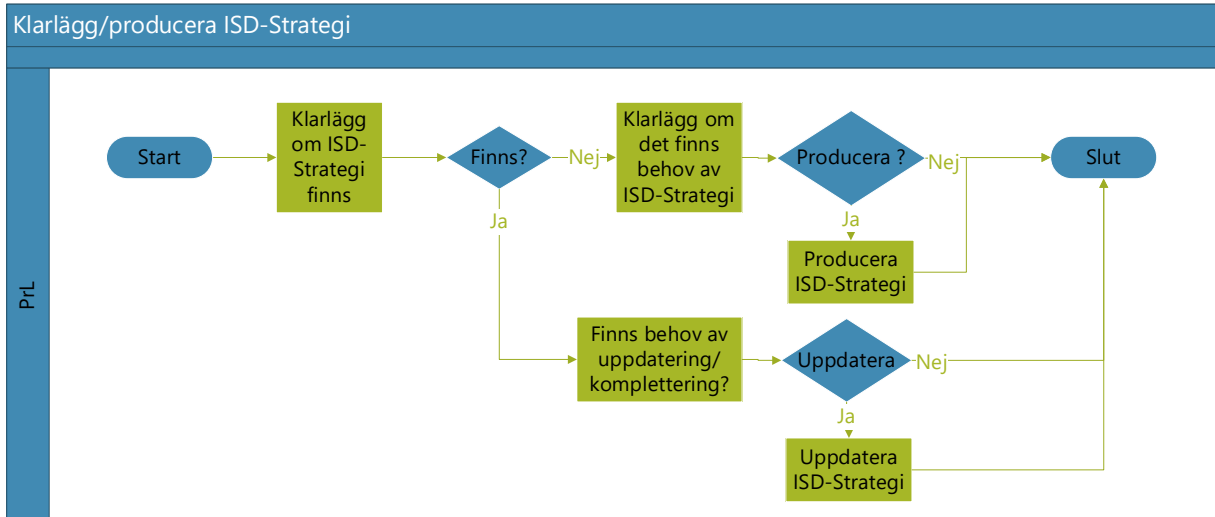
### 5.1.2.1 Klarlägg/producerera ISD-strategi

Det första steget i Identifiera är att klarlägga om det finns en ISD-strategi. Ansvarig för denna aktivitet är Produktledare. Om det finns en tillämplig ISD-strategi är denna underprocess slut. Finns ingen ISD-strategi, eller om befintlig ISD-strategi behöver uppdateras genomförs detta av Produktledare.

ISM kan stödja Produktledare i denna uppdatering.

Figur 15 visar aktiviteterna i detta processavsnitt.

<sup>4</sup> Avser ISD-underlag som produceras i denna fas



Figur 15 Klarlägg/producerera ISD-strategi

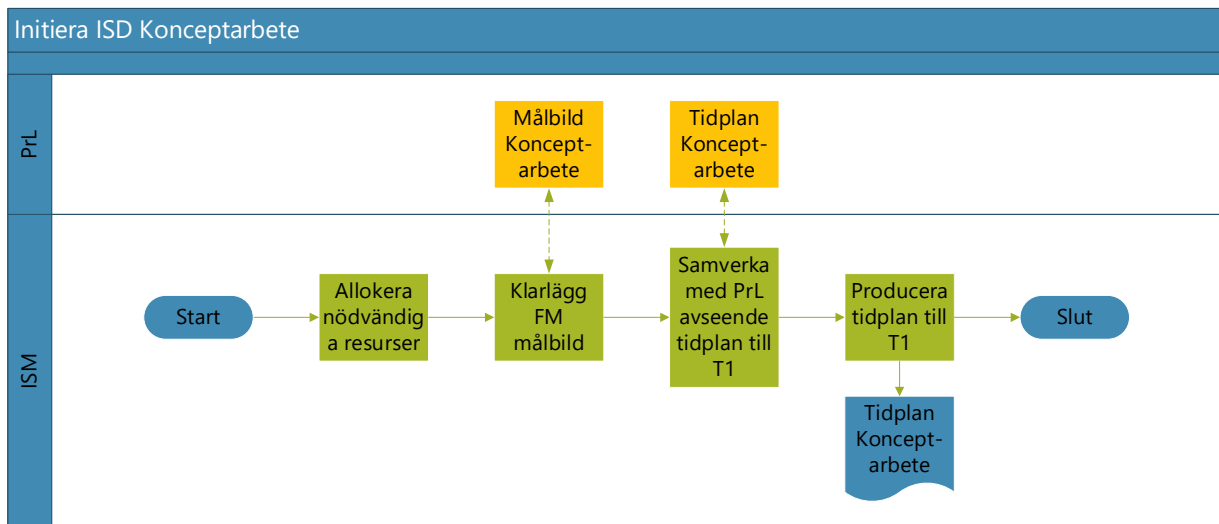
Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	39(76)

### 5.1.2.2 Initiera ISD konceptarbete

I processavsnittet Initiera ISD konceptarbete påbörjar ISM arbetet i ISD Identifiera-fasen. Beroende på konceptarbetets omfattning kan ISM behöva allokera ytterligare resurser, t ex i form av stöd i ISM eller ISA, om det krävs fördjupat krav- och/eller arkitekturarbete.

Nästa aktivitet är att klarlägga FM målbild med konceptstudierna, för att därefter ta fram en uppskattning avseende tidplan för Identifiera-fasen. Tidplanen kommuniceras med Produktledare.

Figur 16 visar aktiviteterna i detta processavsnitt.



Figur 16 Initiera ISD Konceptarbete

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	40(76)

### 5.1.2.3 Granska indata (SMS1)

I denna del av Identifiera granskar ISM indata från FM i syfte att klarlägga om denna är tillfyllest. FMs indata kan bestå av olika typer av dokument, men typiskt är SMS1, FM ITSS innehållande SSB. Även G1-beslut kan vara en del av FM indata.

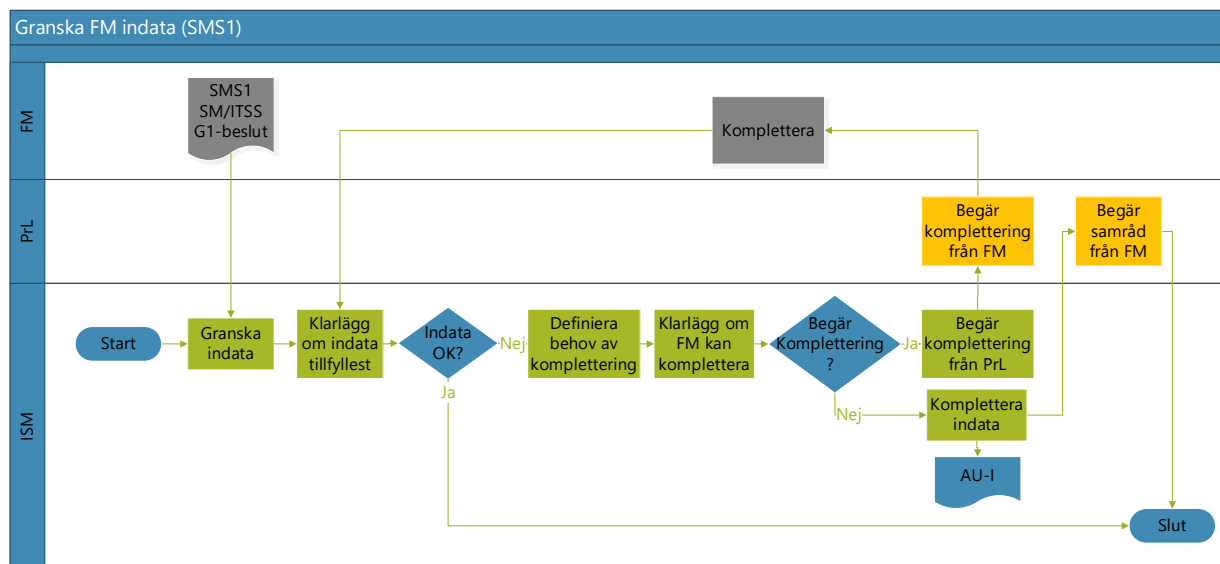
I de fall det rör sig om en modifiering, dvs då Identifiera startar om efter FMV T5-beslut, kan FM indata bestå av uppdaterad ITSS, eller om FMV haft vidmakthållandeuppdrag, av en ITSS-V.

Anser ISM att relevant indata är tillfyllest är denna aktivitet slutförd.

I de fall ISM inte anser att FM indata är tillräckligt, krävs beslut om hur vidare kompletteringar ska göras. Ett alternativ är att FM beställer uppdatering/komplettering av indata, men om detta inte är möjligt ska Produktledare returnera behovet till FM för deras komplettering.

I det fall då FMV på beställning från FM kompletterar indata, bör Produktledare inhämta samråd från FM innan beslut tas.

Figur 17 visar aktiviteterna i detta processavsnitt.



Figur 17 Granska FM indata (SMS1)



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	41(76)

### 5.1.2.4 Klarlägg ISD-strategi

Efter att ISM har erhållit en aktuell och relevant kravbild för konceptarbetet, ska ISM identifiera om det finns en ISD-strategi som kan ha påverkan på det fortsatta ISD-arbetet. Detta görs i samråd med Produktledare.

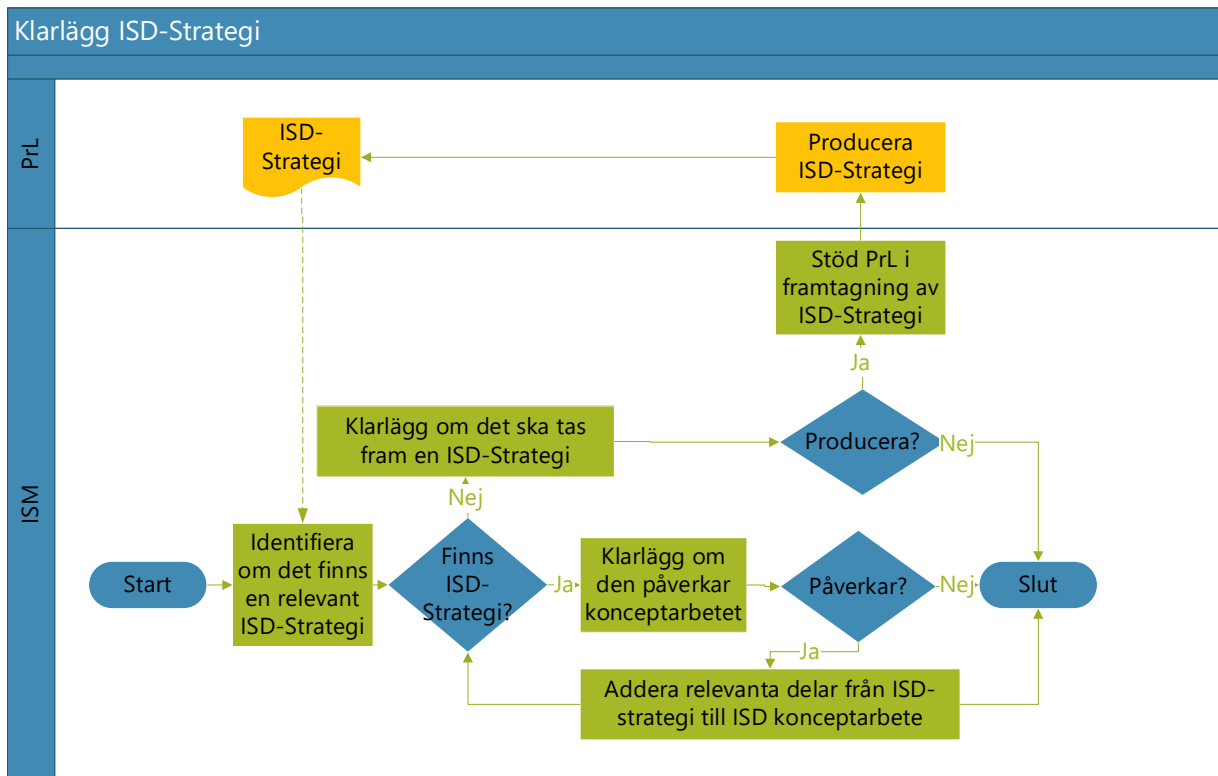
Om det visar sig att det inte finns någon ISD-strategi, ska det klargöras om det finns behov av att producera en sådan. Om så är fallet går denna uppgift till Produktledare, där ISM kan stödja produktionen.

I de fall det inte finns någon ISD-strategi, och det inte heller finns behov av att producera en sådan, är denna delaktivitet avslutad.

Visar det sig att det finns en relevant och aktuell ISD-strategi, ska ISM klargöra om denna strategi kan komma att påverka arbetet med framtagning av ISD-I (inklusive bilagor).

Om befintlig strategi inte visar sig påverka vidare ISD-arbete är denna delaktivitet avslutad. I de fall ISD-strategin visar sig påverka vidare ISD-arbete, ska ISM identifiera relevanta delar och använda dessa i det fortsatta konceptarbetet.

Figur 18 visar aktiviteterna i detta processavsnitt.



Figur 18 Klarlägg ISD-strategi

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	42(76)

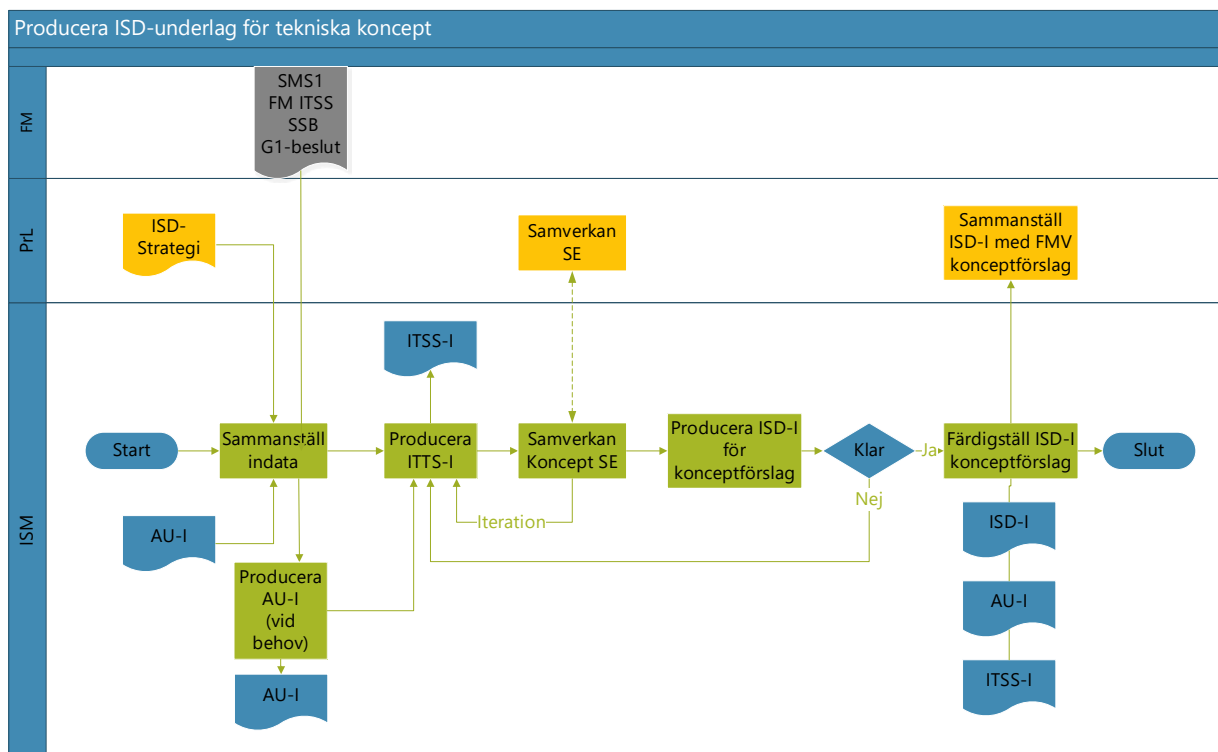
### 5.1.2.5 Producera ISD-underlag för tekniskt koncept

Inför denna delaktivitet är FM indata klarlagda (avseende konceptlösning), liksom FMV ISD-strategi.

ISM inleder arbetet med att sammanställa all indata, för att därefter dokumentera dessa i ITSS-I. I detta läge är det inte nödvändigt att i detalj beskriva samtliga krav, men alla relevanta kravkällor ska vara identifierade. I arbetet med ITSS-I ska samverkan ske med de SE-resurser inom FMV som arbetar med konceptframtagningen. AU-I används för att dokumentera eventuella beslut, analyser och ställningstaganden som gjorts i konceptarbetet.

När ISM tillsammans med SE tagit fram en (eller flera) konceptförslag att presentera för FM inför BOU, färdigställer ISM ISD-I, ITTS-I och AU-I för Produktledarens leverans till FM.

Figur 19 visar aktiviteterna i detta processavsnitt.



Figur 19 Producera ISD-underlag för tekniskt koncept

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	43(76)

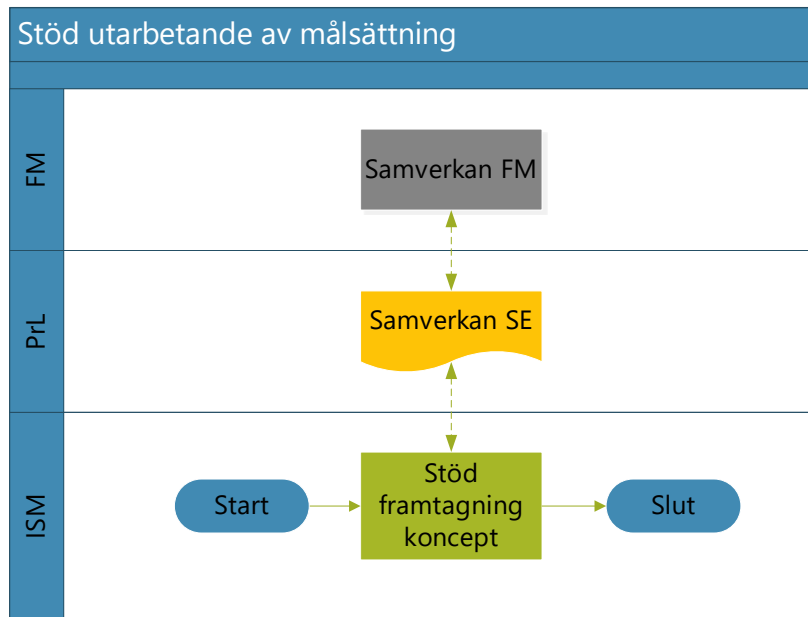
### 5.1.2.6 Stöd utarbetande av målsättning

Denna avgränsade delaktivitet syftar till att ge ISM möjlighet att stötta Produktledare och FM i framtagning av slutligt koncept.

En viktig faktor i denna delaktivitet är att omhänderta och säkerställa att FMs indata (SMS2) återspeglar de eventuella kompletteringar/modifieringar som gjorts tidigare i detta skede.

Samverkan med FMV SE, ledd av Produktledare, är av vikt för att FM ska kunna erhålla en eller flera godtagbara konceptlösningar.

Figur 20 visar aktiviteterna i detta processavsnitt.



Figur 20 Stöd utarbetande av målsättning

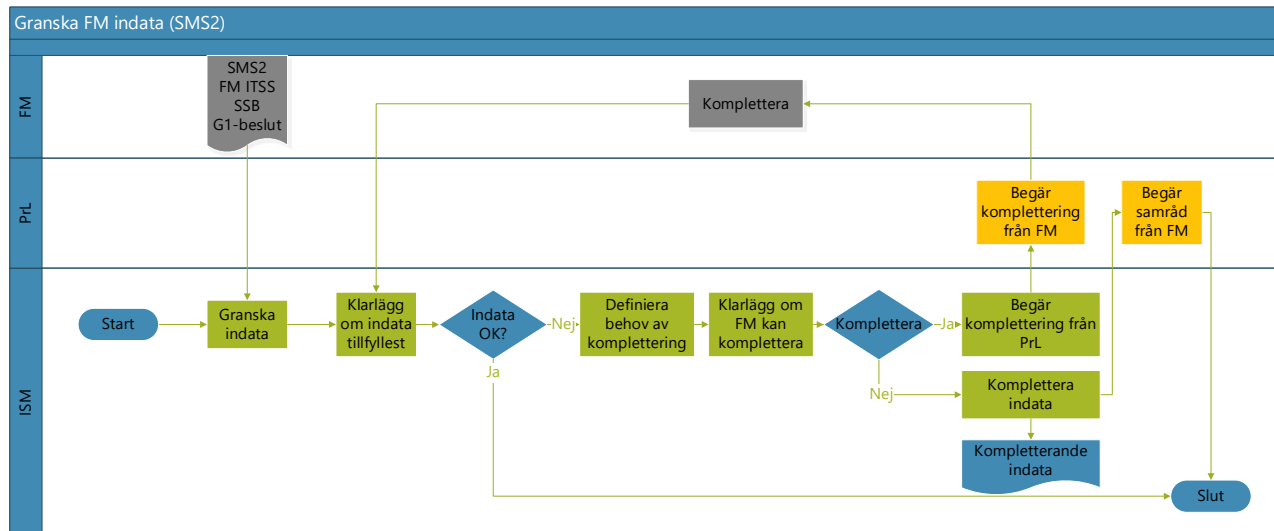
Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	44(76)

### 5.1.2.7 Granska indata (SMS2)

Aktiviteter i detta processavsnitt motsvarar i princip de som är beskrivna i kapitel 5.1.1.3, med skillnaden att indata här utgörs av SMS2, FM ITSS och dess SSB. SMS2 färdigställs efter FM beslut BOU, och innehåller då en specificerad mål- och kravställning på det valda konceptet.

Om det funnits möjlighet till bra samverkan mellan FM och FMV avseende informationssäkerhetskravställningen bör detta processavsnitt snabbt kunna hanteras. I övriga fall genomförs samma kontroller som för SMS1, med syfte att ge FMVs genomförandeprojekt korrekta förutsättningar att påbörja ISD Definiera.

Figur 21 visar aktiviteterna i detta processavsnitt.



Figur 21 Granska FM indata (SMS2)

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	45(76)

### 5.1.2.8 Revidera/färdigställ ISD-I

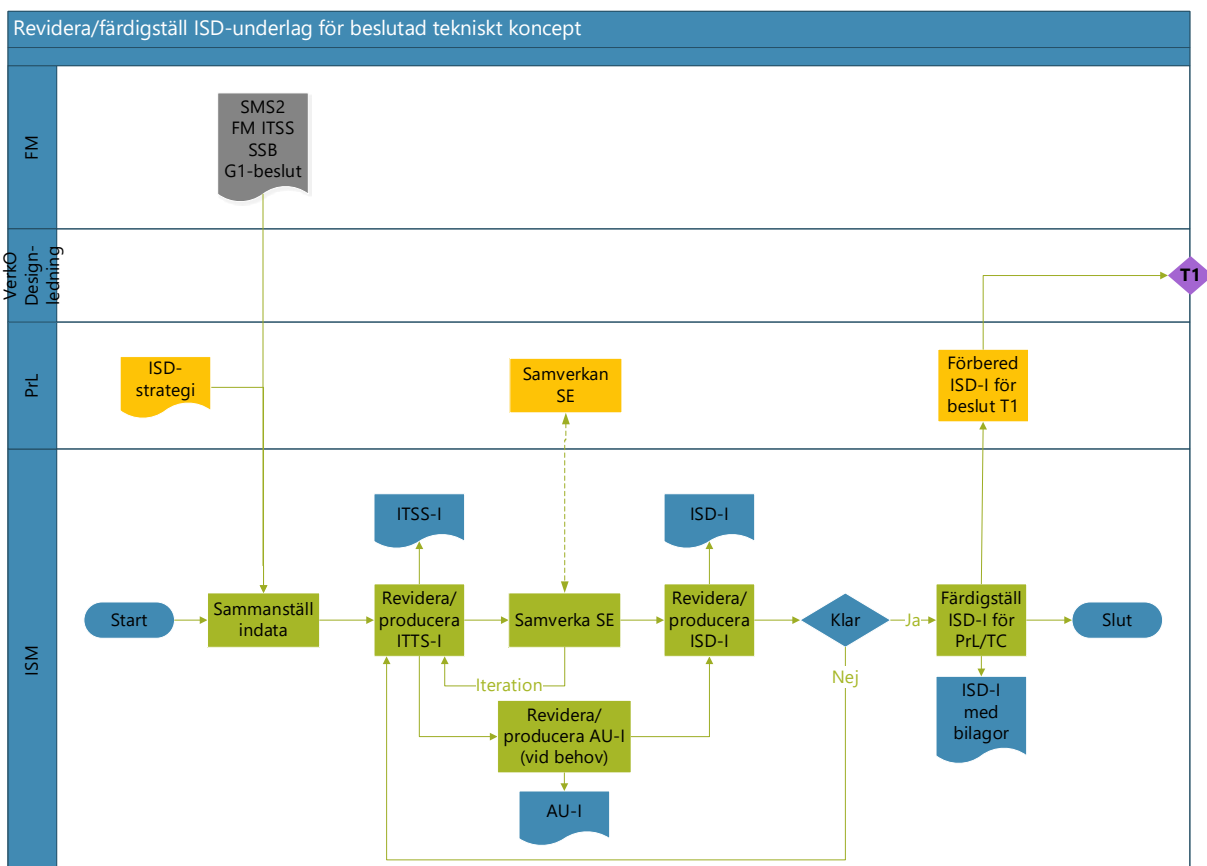
Denna delaktivitet motsvarar aktiviteterna i kapitel 5.1.1.5, med den skillnaden att ISD-I underlagen nu bygger på av BOU vald teknisk lösning med tillhörande SMS2/ITSS.

Om behov finns ska samverkan ske med SE. Processen är iterativ tills ett tillräckligt bra underlag har producerats. Kriterierna för definition av "tillräckligt" är att underlaget ska kunna användas som indata till ISD Definiera-fas då FMV genomförandeprojekt startar. När ISD-I är färdigställd ska den övergripande kravställningen vara fullständig. Kraven/kravkällorna i ISD-I ska i efterkommande fas brytas ned, tolkas och allokeras mot definierad systemarkitektur.

Observera att konceptarbetet i detta skede kan komma att initiera mer än ett genomförandeprojekt inom FMV, och att ISD-I underlagen då ska kunna ge stöd till samtliga av dessa projekt.

ISD-I, med dess bilagor AU-I och ITSS-I, är efter denna delaktivitet underlag till FMV T1-beslut.

Figur 22 visar aktiviteterna i detta processavsnitt.



Figur 22 Revidera/färdigställ ISD- underlag för beslutad tekniskt koncept

### 5.1.2.9 Revidera ISD-strategi

Efter konceptfas ska ISD-strategin vid behov uppdateras för berörda produktområden.



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	46(76)

## 5.2 Definiera

Definiera är första fasen i genomförandeprojektet där planering av informationssäkerhetsarbetet, kravarbete (inkl. IT-säkerhetsarkitektur) och framtagning av upphandlingsunderlag är huvudaktiviteterna.

ISD-fasen Definiera sammanfaller med FMV VHL Förberedelse- och Anskaffningsskede. ISD-arbetet kan starta efter två olika T-beslut;

- 1) T1 - I de fall FM beställer ett konceptarbete av FMV startar ISD Definiera genom beslut T1.
- 2) T5 - I de fall FMV tagit T5-beslut om Modifiering som är av sådan art att ett nytt konceptarbete inte behöver genomföras.

Indata från FM i fallet då ISD startar i T1 är normalt sett SMS2 med FM ITSS innehållande SSB. Denna SMS är då också omsatt och bearbetad i ISD-I.

Identifiera avslutas genom FMV T3-beslut, där ISD-D är ett beslutsunderlag.

Aktiviteterna resulterar i att Projektledare bedömer att systemet är realiserbarhet inför FMV VHL T3-beslut för upphandling. I denna fas tar Projektledare stöd av rollerna ISM och ISA.

Förutsättningarna för att kunna bedöma realiserbarheten, och ge förutsättningar till upphandling och realisering, är att ett förberedande arbete som har genomförts i Identifiera. Det är viktigt att Projektledare gör en bedömning av mognadsgraden på indata från Produktledare, och begär komplettering i de fall det bedöms att informationen inte är tillräcklig.

Projektledare planerar arbetet/projektet och tar tillsammans med ISM fram en ISD-plan.

Aktiviteter som kravfångst, och eventuellt ett kompletterande av analyser från Identifiera-fasen, sker av ISM. Resultatet av detta använder ISA till att genomföra kravtolkning och framtagning av ITSA.

ISM genomför, tillsammans med ISA, en ny realiserbarhetsbedömning samt producerar indata till upphandlingsunderlag i form av VÅS och TS.

Aktiviteter som kravtolkning, kravnedbrytning och framtagning av ITSA kräver kompetens enligt ISA kravprofil i kapitel 4.1.2. IT-säkerhetskraven från kravnedbrytningen fördelas på IT-säkerhetsarkitekturen. Detta arbete sker iterativt.

Arbetet med TS och VÅS sker i samverkan med SE för att säkerställa realiserbarhet med övriga systemområden. I slutskedet av arbetet kan oberoende granskning av SystGL, samt samråd med FM MUST i form av designgenomgång (DG) och FM G2 beslut, ge inriktningar.

FMV lämnar fastställt underlag efter FMV VHL T2 (beslut om att fastställa tekniskt underlag för anskaffning) till FM för designgenomgång. När FM tagit BOP kan FMV ta T3-beslut (beslut om att fastställa tekniskt underlag för produktion.).

Inför FMV VHL T3 sammanställs, vid behov uppdaterad, deklARATION av realiserbarhet och upphandlingsunderlag.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	47(76)

### 5.2.1 Övergripande fasbeskrivning

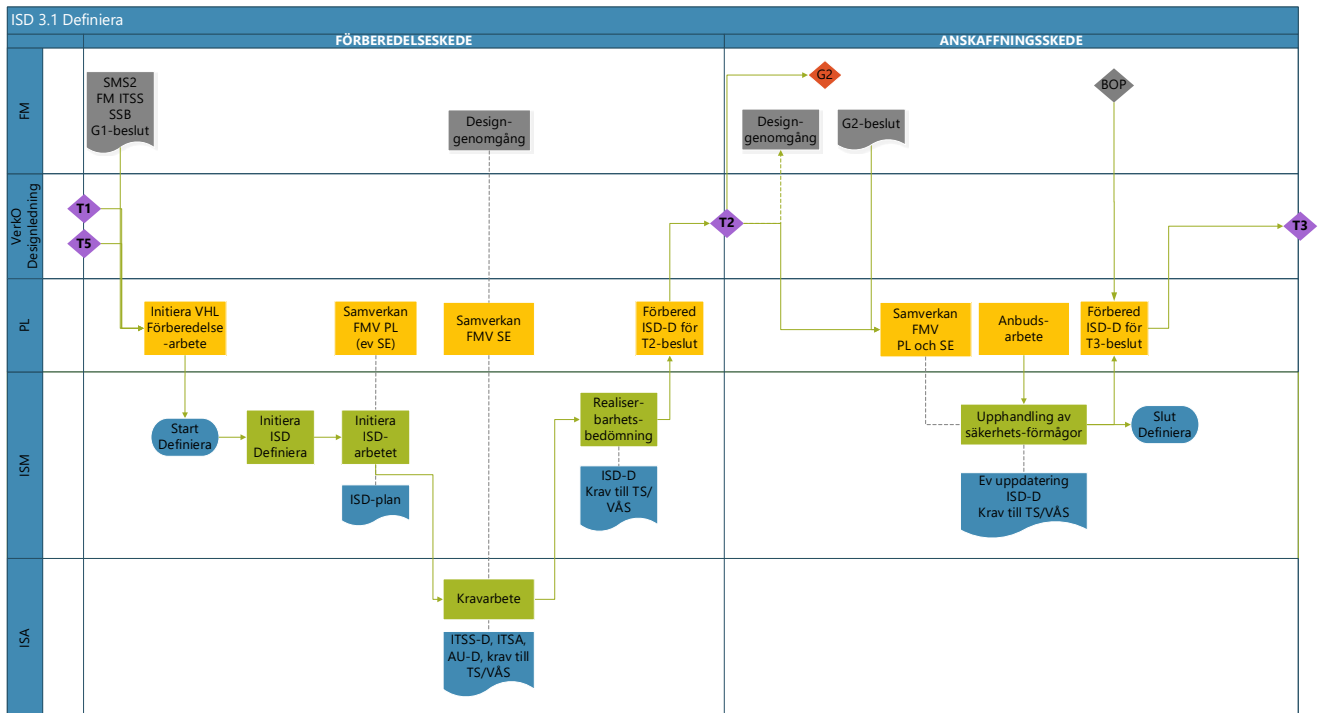
I de fall FM beställer ett konceptarbete av FMV startar ISD Definiera genom beslut T1.

Det kan också finnas fall då FMV tagit T5-beslut om Modifiering, som är av sådan art att ett nytt konceptarbete inte behöver genomföras. I dessa fall startar ISD Definiera efter T5-beslutet.

Definiera kan också starta utan genomfört konceptarbete och initieras då direkt med SMS2, SM och ITSS.

Definierafasen avslutas genom FMV T3-beslut, där ISD-D är ett beslutsunderlag.

Figur 23 nedan visar översiktligt aktiviteterna i Definiera-fasen.



Figur 23 Översikt av aktiviteter i Definiera-fasen



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	48(76)

Tabell 7 sammanfattar ISD Definiera-fas.

Definiera	VHL T1 till T3
Syfte	Definiera och tolka krav, framtagning av säkerhetsarkitektur samt informationssäkerhetskrav till TS/VÅS samt bedömning av realiserbarhet Ta fram underlag för upphandling och produktion.
Aktiviteter	Initiera ISD Definiera-fas Initiera ISD-arbete Kravarbete Realiserbarhetsbedömning Upphandling av säkerhetsförmågor
ISD dokument	ISD-plan ISD-D AU-D ITSS-D ITSA
Indata	ISD-strategi ISD-I AU-I ITSS-I
Utdata	ISD-plan ISD-D AU-D ITSS-D ITSA
Aktiva roller	FM VerkO Designledning PL ISM ISA

Tabell 7 – Sammanställning ISD Definiera



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	49(76)

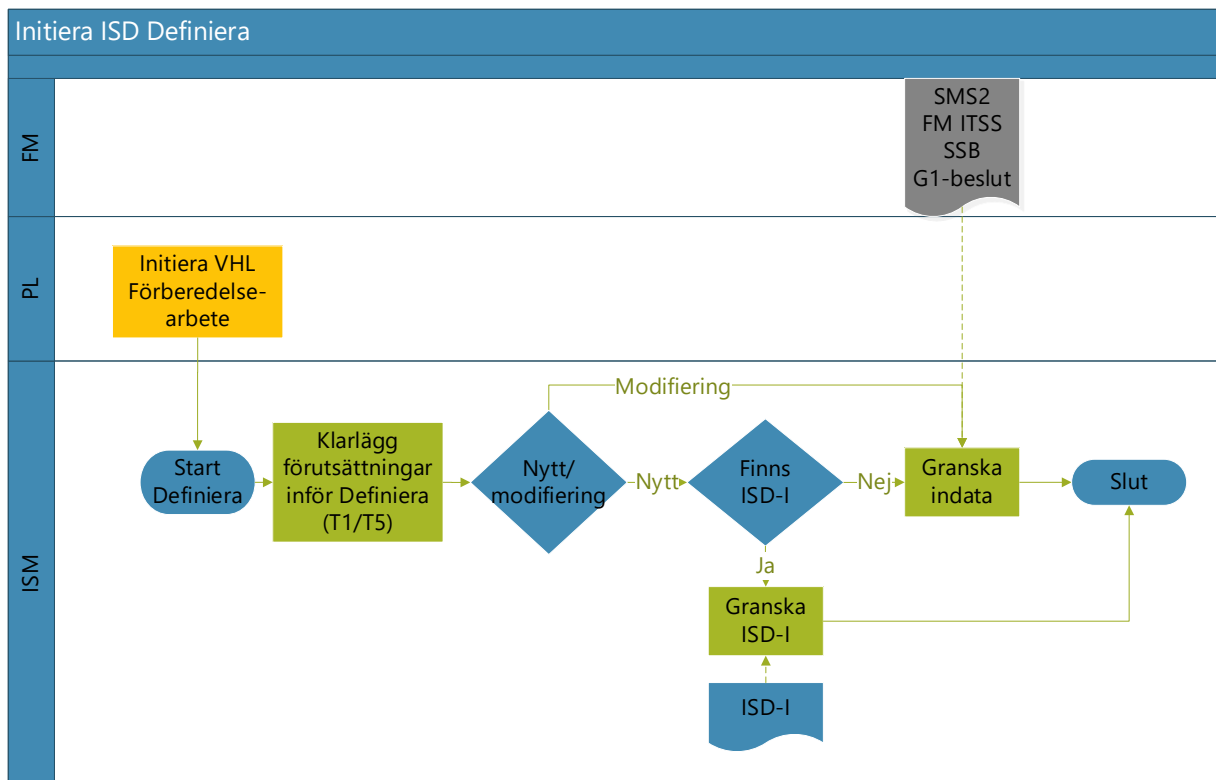
## 5.2.2 Detaljerad fasbeskrivning

### 5.2.2.1 Initiera ISD definiera

Arbetet med Initiera ISD Definiera börjar med att ISM klarlägger förutsättningarna för ISD-arbetet i denna fas.

Oavsett hur Definiera startar, ska ISM säkerställa att förutsättningarna för fortsatt arbete är klarlagda.

Figur 24 visar aktiviteterna i detta processavsnitt.



Figur 24 Initiera ISD Definiera

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	50(76)

### 5.2.2.2 Initiera ISD-arbete

I detta processavsnitt initieras ISD-arbetet i Definierafasen, genom ISM's produktion av ISD-plan. ISD-planen syftar till att beskriva arbetet i Definiera och Realisera för att systemet ska kunna bli tillräckligt säkert och därigenom ackrediterbart.

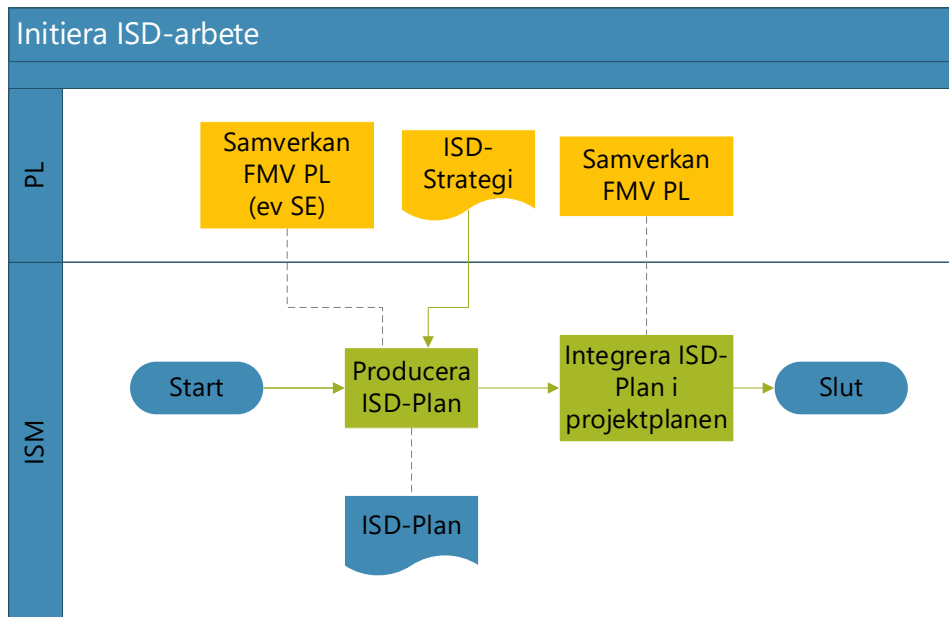
ISD-planen styr projektets informationssäkerhetsarbete med målet att deklarerat IT-systemets informationssäkerhet (under specificerade förutsättning).

ISD-planen klargör förutsättningar, vilka aktiviteter som ska genomföras, i vilken omfattning ISD-processen ska användas och vilka roller som behövs. ISD-planen ska synkroniseras med FMV Projektledares projektplan.

ISD-planen innehåller bland annat:

- Styrande förutsättningar
- Avgränsningar
- Förteckning över kravkällor
- Beskrivning av informationssystemet
- Utmaningar
- Tillsättning av ISD-roller samt identifiering av samverkansparter
- ISD-relaterade aktiviteter samt tidplan

Figur 25 visar aktiviteterna i detta processavsnitt.



Figur 25 Initiera ISD-arbete

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	51(76)

### 5.2.2.3 Kravarbete

I detta processavsnitt startar ISAs primära arbete med att sammanställa kravunderlag, tolka kraven och framtagning av IT-säkerhetsarkitektur. ISA kravarbete beskrivs översiktligt kapitel 3.6.

Arbetet med att producera ett kravunderlag är ett iterativt arbete där samverkan med SE är av största vikt. Arbetet inom ISD-processen är inte en fristående aktivitet som pågår parallellt med systemdesignen utan ett integrerat arbete där flera olika discipliner måste samverka. Dessa kan t.ex. vara ILS, test och systemsäkerhet. Samtliga discipliner måste samverka för att FMVs kravbild ska kunna formuleras som en helhet i beslutsunderlaget inför T2 och T3.

Som tidigare beskrivits bör kravarbetet ske i ett dedikerat kravhanteringsverktyg, och resultatet dokumenteras i ITSS-D.

Nödvändiga analyser, beslut och ställningstaganden dokumenteras i AU-D med syftet att bibehålla spårbarheten i kravarbetet.

När ISA, ISM och FMV Projektledare finner det lämpligt bör samråd ske med FM i form av Designgenomgång (DG). Syftet med DG är att dels ge FM en bild av systemdesignen (inklusive IT-säkerhetsarkitekturen), och dels ge FM möjlighet att styra FMVs arbete med systemet och IT-säkerhetsarkitekturen.

Då ISM, ISA, FMV Projektledare och FMV SE (samt FM genom DG) anser att IT-säkerhetsarkitekturen är tillfyllest, fastställs ISD-D, AU-D, ITSS-D och ITSA i sin första utgåva.

I de fall FMV ska upphandla IT-systemet via TS och VÅS används primärt den tolkade kravbilderna i ITSS-D som underlag för säkerhetskraven.

Funktionella säkerhetskrav allokeras normalt mot TS, medan assuranskrav normalt sett allokeras mot VÅS.

Normalt ska assuranskraven synkroniseras, med övriga krav, i samband med kravarbetet. Om detta inte är gjort är det av vikt att notera att assuranskrav bör synkroniseras här med övriga krav i VÅS.

Om genomförandeprojektet omfattar mer än en leverantör, ska kraven i ITSS-D fördelas på respektive leverantörs TS och VÅS. Denna fördelning genomförs utanför ISD-underlagen, och då lämpligen i ett kravhanteringsverktyg.

Oavsett om genomförandeprojektet omfattar en eller flera leverantörer, är ITSS-D källan till de krav som ställs via TS och VÅS. Väsentligt här är att spårbarheten mellan ITSS-D och respektive TS och VÅS bibehålls, så att det är möjligt att redovisa detta i Realiserfasen.

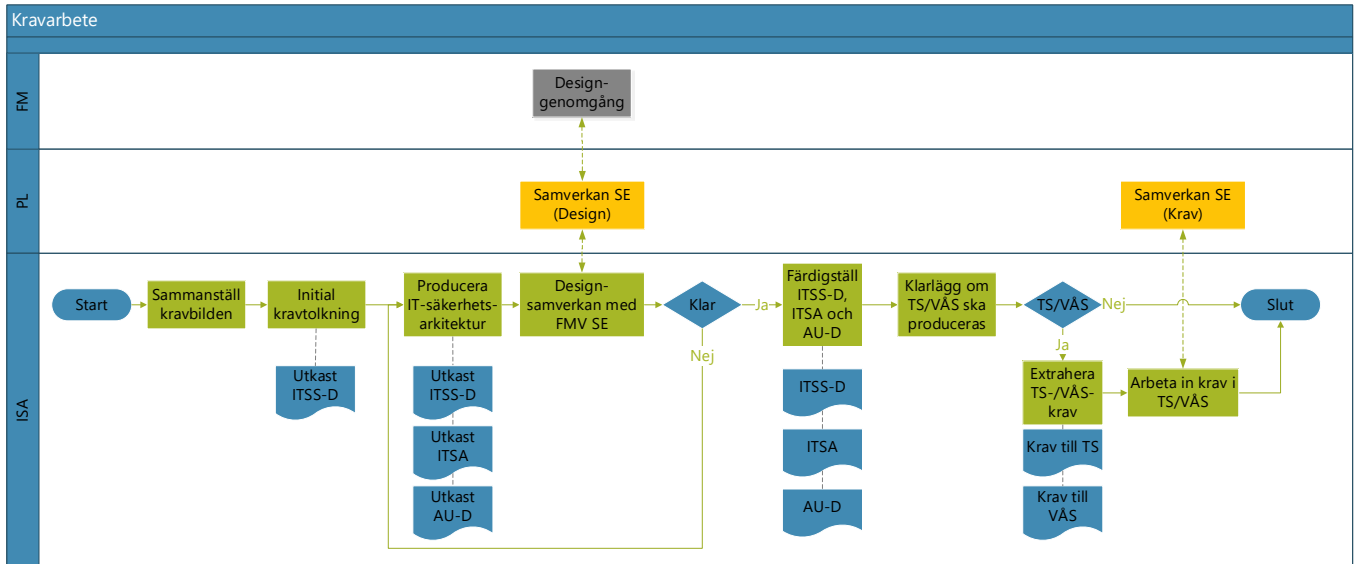
TS och VÅS är kommersiella upphandlingsunderlag som används mot en eller flera leverantörer, och är också den samlade kravställning som ställs mot dessa. I VÅS ska det framgå hur leverantör (-er) ska redovisa sin kravuppfyllnad, bland annat som stöd för ISEs evaluering.

Notera att ISD-underlagen, där ITSS-D innehåller den samlade kravställningen, är interna FMV-underlag som inte ska delges leverantör (-er).

I de fall FMV Projektledare och SE agerar integratör utgör ITSS-D det kravunderlag som nyttjas för att kravställa de systemkomponenter som ingår i systemet.

Figur 26 visar aktiviteterna i detta processavsnitt.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	52(76)



Figur 26 Kravarbete

#### 5.2.2.4 Realiserbarhetsbedömning

När den första utgåvan av ISD-D är klar, gör ISM en bedömning av realiserbarheten i system avseende informationssäkerheten.

Detta ISD-D underlag är indatat till FMV VHL T2-beslut, vilket i sin tur ligger till grund för FM BOP-beslut, Beslut om produktion.

#### 5.2.2.5 Upphandling av säkerhetsförmågor

ISD-D skickas till FM för G2 beslut och BOP. Innan FMV skickar offertförfrågan till någon leverantör ska FMV fått ta del av Försvarmaktens G2 beslut och uppdaterat kravställningen i enlighet med beslutet. FMV ska i samband med detta även erbjuda Försvarmakten en designgenomgång där det bl.a. framgår hur IT-arkitekturen och IT-säkerhetsarkitekturen ser ut, hur kravställningen tolkats och brutits ner samt vilka krav som faller på Försvarmakten att uppfylla.

Efter G2-beslut kan det finnas behov av att ändra kravställningen. När kravställningen uppfyller Försvarmaktens krav kan FMV påbörja upphandlingen. Efter anbudsförfrågan görs anbudsutvärdering, och en eller flera leverantörer väljs. ISM stöttar FMV Projektledare i anbudsutvärderingen tillsammans med ISA.

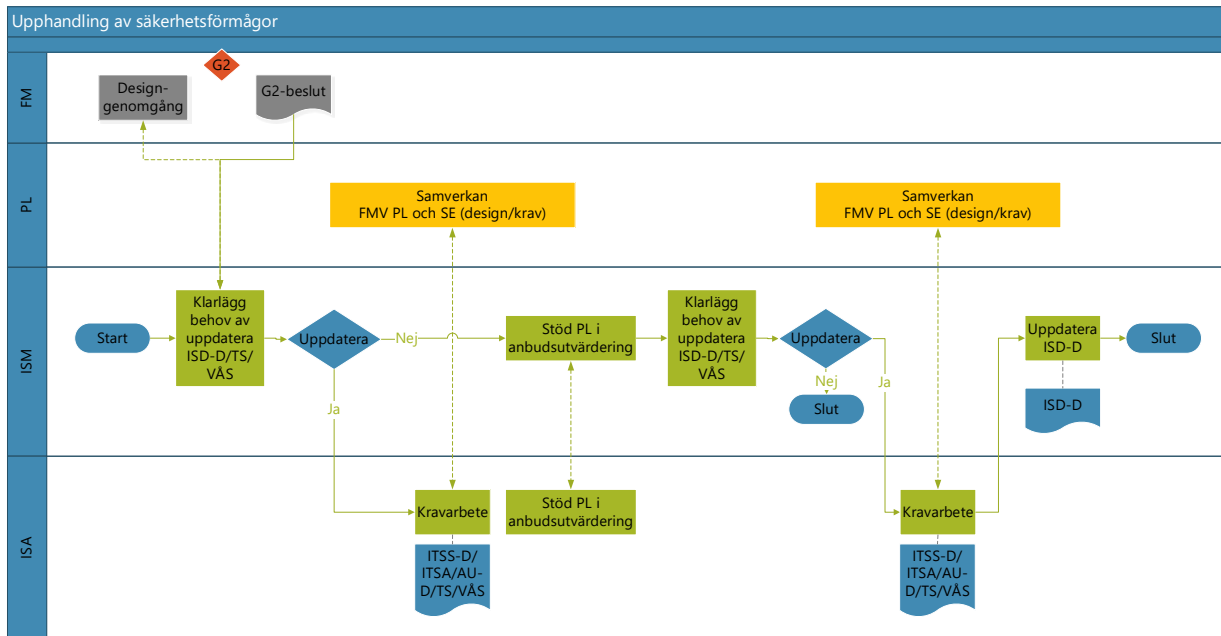
Efter att FMV slutfört anbudsutvärderingen, och tagit beslut om leverantör (-er), ska ISM analysera huruvida ISD-D med dess bilagor (samt TS och VÅS) behöver uppdateras. Om analysen visar att underlagen inte behöver uppdateras är detta processavsnitt avslutat. ISD-D kan då nyttjas som beslutsunderlag.

I de fall analysen visar att ISD-D behöver uppdateras återgår ISD-D till ISA, och kravarbete i enlighet med kapitel 5.2.2.3 vidtar. Beroende på uppdaterings omfattning kan det uppstå behov av kompletterande DG med FM. Samverkan med FMV SE ska alltid ske.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	53(76)

Efter uppdatering av ISD-D och eventuellt även TS/VÅS kan dessa nyttjas som beslutsunderlag för FMV VHL T3-beslut och beställning hos leverantör.

Figur 27 visar aktiviteterna i detta processavsnitt.



Figur 27 Upphandling av säkerhetsförmågor



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	54(76)

## 5.3 Realisera

I Realiserafasen genomförs leverantörens produktion med evaluering av leverantör (-er), systemdokumentation, systemrealisering och assurancesunderlag tillsammans med kompletterande tester av systemet.

ISD-fasen Realisera sammanfaller med FMV VHL Produktionsskede. ISD-arbetet startar genom T3-beslut, och avslutas i T4.

Inför T4 genomförs en ackrediterbarhetsbedömning vilken, tillsammans med resultat från evaluering, restrisikalanlys och kompletterande tester sammanfattas i ISD, Informationssäkerhetsdeklarationen.

### 5.3.1 Övergripande fasbeskrivning

ISD Realisera påbörjas i princip samtidigt som FMV beställer anskaffning/produktion från leverantör (-er) och inleds med att ISM planerar för denna fas, i enlighet med ISD-planen. Om behov uppstår kan ISD-planen behöva uppdateras. ISM etablerar kontakt med relevant (-a) leverantör (-er).

Då leverantör startar upp systemutvecklingen har ISA möjlighet att ge stöd avseende kravspecifikationer, designriktningar och systemlösningar. Viktigt att observera är att ISA ska bibehålla sitt oberoende i förhållande till leverantör, och endast erbjuda stöd. Framtagning av system- och assurancesdokumentation, samt implementation av säkerhetsfunktioner och -mekanismer, ska genomföras av leverantör.

Evalueringen genomförs i två steg, där det första steget bland annat omfattar leverantörens säkerhetsskydd i utvecklingsmiljön, konfigurationsledning och bristhantering. Det andra steget omfattar evaluering av den implementerade säkerhetslösningen, samt system- och övrig assurancesdokumentation. I samband med evaluering kan vid behov kompletterande tester genomföras.

Då evaluering och tester är klara genomför ISE en sårbarhetsanalys samt en sammanfattande restrisikalanlys.

Den sista aktiviteten i Realisera är ISMs ackrediterbarhetsbedömning, innan ISD och ISD-R med bilagor är klara som beslutsunderlag inför FMV VHL T4.

Efter T4 vidtar FMs beslutspunkter inför driftsättningen; CAB, G3, BOAC, LAB och BOAL.

Figur 28 nedan visar översiktligt aktiviteterna i Realisera-fasen.



Ej sekretess

ISD 3.1 Processbeskrivning

Datum

2021-05-18

Diarienummer

20FMV5903-1:1

Ärendetyp

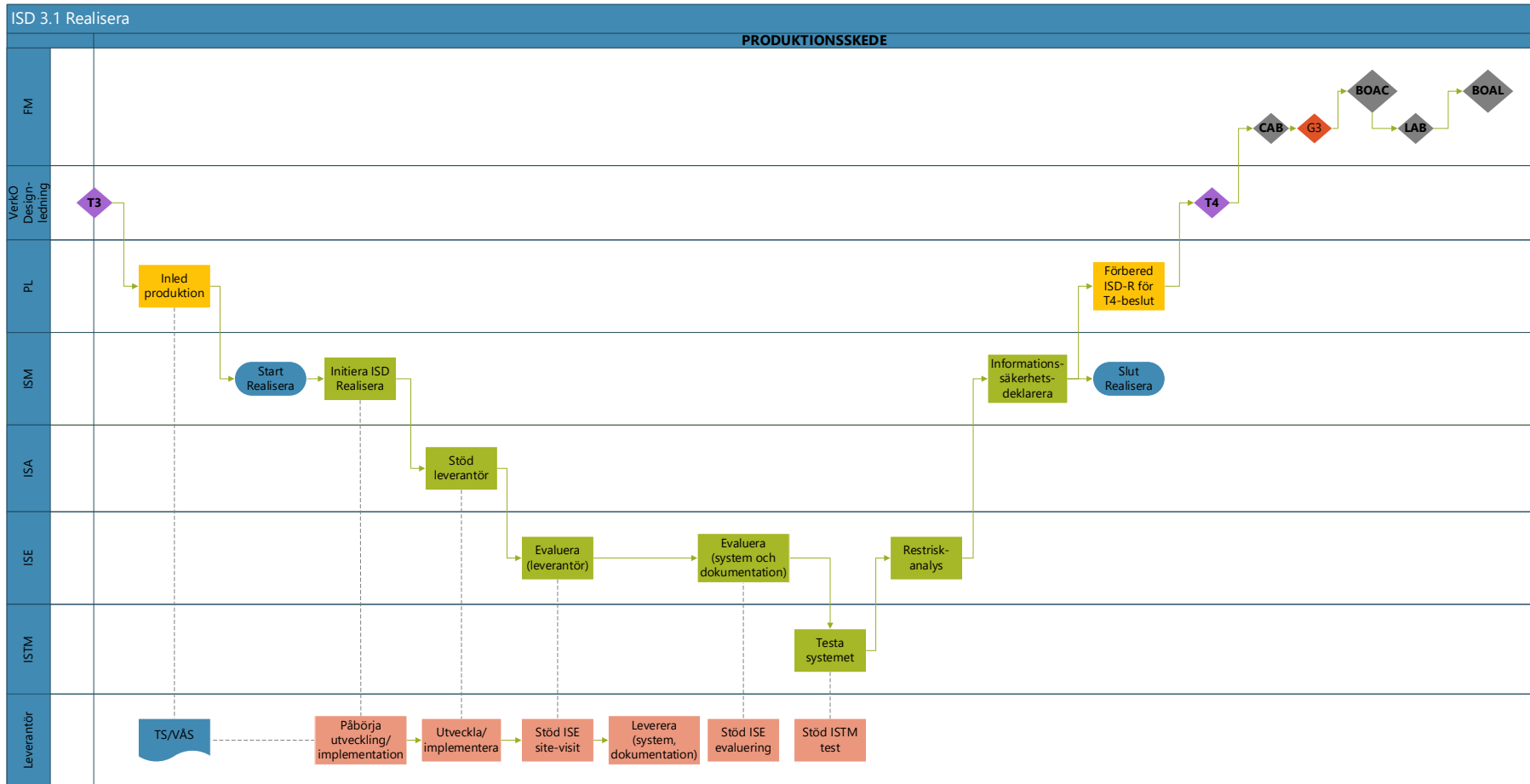
3.5

Dokumentnummer

3.1.0

Sida

55(76)



Figur 28 Översikt av aktiviteter i Realisera-fasen



Ej sekretess

ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	56(76)

Tabell 8 sammanfattar ISD Realisera-fas.

Realisera	VHL T3 till T4
Syfte	Evaluera systemutvecklare och säkerheten i systemet, samt skapa underlag för ackreditering och deklarerar informationssäkerheten
Aktiviteter	Initiera ISD Realisera Stöd leverantör Evaluering av leverantör Evaluering av system och dokumentation Test av systemet Restriskanalys Informationssäkerhetsdeklaration
ISD dokument	ISD ISD-R AU-R ITSS-R VMH-R ISTM Testdokumentation
Indata	ISD-plan ISD-D AU-D ITSS-D ITSA TS (en/flera) VÅS (en/flera)
Utdata	ISD ISD-R AU-R ITSS-R VMH-R
Aktiva roller	FM VerkO Designledning PL ISM ISA ISE ISTM Leverantör (-er)

Tabell 8 – Sammanställning ISD Realisera



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	57(76)

### 5.3.2 Detaljerad fasbeskrivning

#### 5.3.2.1 Initiera ISD Realisera

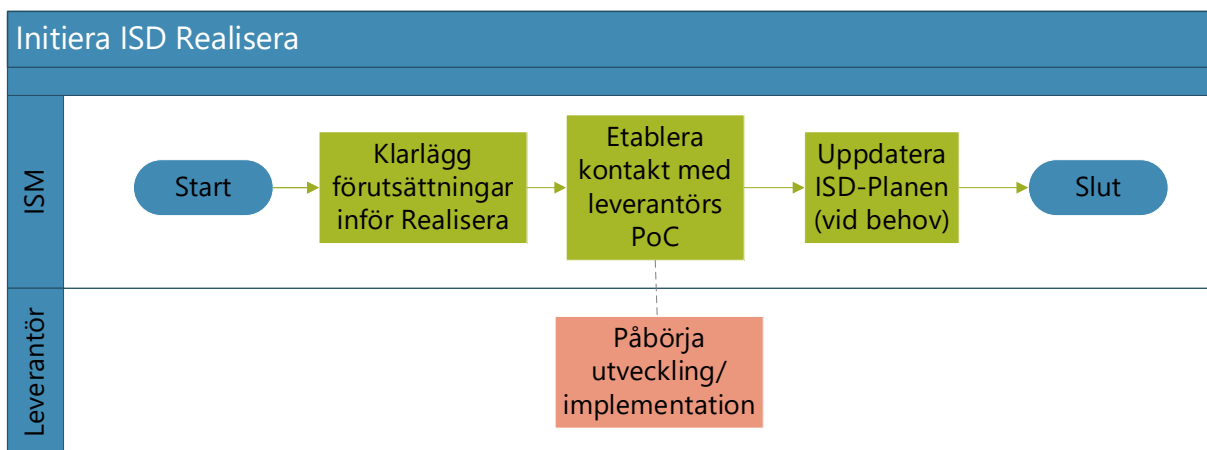
Arbetet i Realiserafasen inleds i processavsnittet Initiera ISD Realisera, där ISM påbörjar att klargöra förutsättningarna för ISD-arbetet i denna fas.

Klarläggandet innefattar, men är inte begränsat till, att identifiera ISD-underlag från Definiera samt (om det finns flera) samtliga relevanta TS- och VÅS-underlag.

Efter detta etablerar ISM kontakt med leverantör (-ers) PoC för att kunna ha en kommunikationskanal avseende stöd i informationssäkerhetsfrågor.

Vid behov ska ISM också uppdatera ISD-planen, då det kan ha skett förändringar i t ex tidplanen i samband med anbudsarbetet.

Figur 29 visar aktiviteterna i detta processavsnitt.



Figur 29 Initiera ISD Realisera



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	58(76)

### 5.3.2.2 ISA stöd till leverantör

När leverantör (-er) har startat upp sitt arbete kan ISA erbjuda stöd i design- och realiseringsfrågor. ISA bör därför etablera kontakt med leverantörs PoC.

ISA (och även ISM) kan med fördel delta på leverantörens progressmöten i syfte att hantera eventuella frågeställningar i god tid. Dessa progressmöten ska vara kravställda i VÅS, och kan typiskt innehålla följande typer av möten beroende på vilken typ av utvecklingsmodell som respektive leverantör använder:

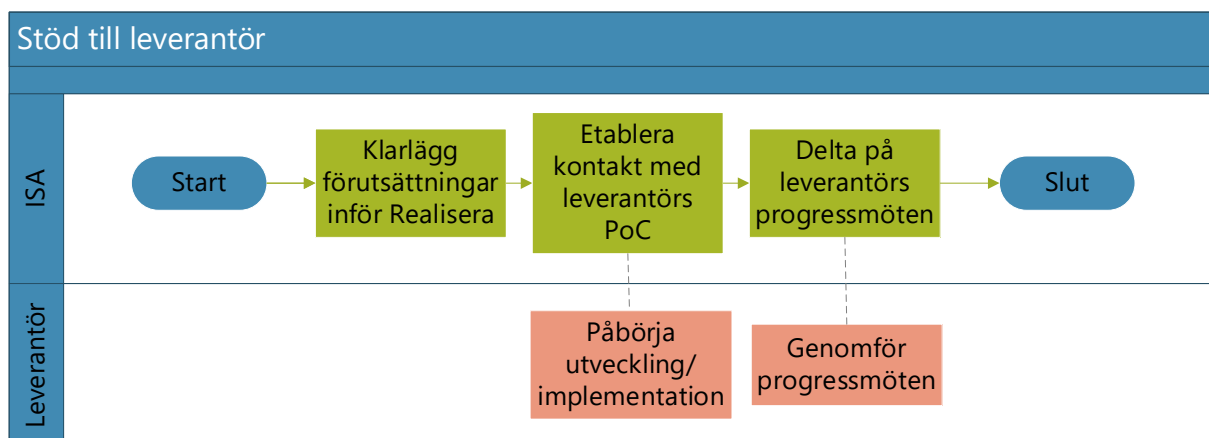
- **SRR - System Requirements Review**  
Innebär en formell granskning som genomförs i syfte att säkerställa att ett systems, eller en produkts, totala kravbild har identifierats och att en gemensam tolkning (förståelse) finns mellan FMV och leverantören kring kravbild. Granskningen säkerställer att initial, och preliminär, systemdesign kan ta vid. Dessutom säkerställs att system- och prestandakrav är nedbrutna utifrån fastställda målsättningsdokument, samt att de är definierade, verifieringsbara och att de ryms inom kostnadsram, tidplan och acceptabel risknivå m.m.
- **SDR - System Design Review**  
Granskningen syftar till att säkerställa att framtagen funktionell kravnivå (baseline) är inom rimliga förväntningar, samt att budget och tidplan kan möta kravställning på högre systemnivå. SDR innebär att en systemnedbrytning från toppnivå är genomförd och jämför systemspecifikationen med funktionell specifikation. Efter genomförd SDR påbörjas arbetet med att utforma en preliminär design för aktuellt system.
- **PDR - Preliminary Design Review**  
Är en teknisk granskning som syftar till att fastställa ett systems principiella utformning för att säkerställa systemets funktionalitet, att systemfunktioner och prestandakrav är allokerade korrekt, att gränssytor är definierade m.m. PDR genomförs innan detaljerat designarbete påbörjas och är ofta första tillfället för FMV att granska leverantörens förslag på systemdesign. FMV kan välja att komma med invändningar, eller presentera sådan information, så att leverantören måste ompröva sin tidigare inriktning och ta fram en alternativ systemlösning.
- **CDR - Critical Design Review**  
CDR är en teknisk granskning som syftar till att säkerställa att utarbetad detaljerad design uppfyller funktions-, förmåge- och prestandakrav som de är fastställda i TS och att den befinner sig inom de kostnads- och tidsramar som angivits, samt med acceptabel risk. Genomförd CDR innebär att detaljkonstruktion kan slutföras och att produktionsunderlag kan utarbetas.
- **PRR - Production Readiness Review**  
PRR syftar till att säkerställa att samtliga förutsättningar för att påbörja produktion är etablerade. Vid PRR kontrolleras produktionsunderlag och att en adekvat produktionsplanering har genomförts.
- **TRR - Test Readiness Review**  
TRR genomförs i syfte att säkerställa att ett system är klart att gå vidare till formell testning och verifiering. Detta görs genom granskning av att testobjektet har relevant utformning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	59(76)

och egenskaper, samt att testprocedurer är kompletta och möter verifieringsplan och beskrivning. TRR genomförs normalt innan varje större delsystem och/eller funktion ska verifieras. Vid TRR redovisas vilka åtgärder som genomförts i syfte att kvalitetssäkra att verifieringsaktiviteten kan utföras i sin helhet. Detta innefattar redovisning av föregående verifieringsaktiviteter. Innan TRR avslutas tas ställning till om verifieringsaktiviteten kan starta eller om det krävs ytterligare åtgärder.

- SVR - System Verification Review  
SVR är en granskning som syftar till att utifrån genomförd verifiering fastställa om systemet eller produkten anses uppfylla ställda krav.

Figur 30 visar aktiviteterna i detta processavsnitt.



Figur 30 ISA stöd till leverantör

Notera att leverantörens utvecklingsprocess med milstolpar i exemplet ovan inte kravställs från ISD-processen, men oavsett vilken process som ska följas så ska detta specificeras i VÅS. ISM och ISA anpassar därefter sina aktiviteter för att stödja leverantör.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	60(76)

### 5.3.2.3 ISE evaluering (leverantör)

Processavsnittet inleds med att ISE samlar in all relevantt assuransdokumentation som ska omfattas av evalueringen i detta steg.

Evalueringsaktiviteterna som ISE ansvarar för kan med fördel delas upp i två områden:

- Evaluering av leverantör
- Evaluering av system (se kapitel 5.3.2.4)

Evaluering av leverantör kan genomföras relativt tidigt i Realisera och syftar till att granska de assuranskrav som normalt sett är förutsättningar för att leverantören ska kunna producera och leverera ett säkert system.

Dessa aktiviteter omfattar normalt:

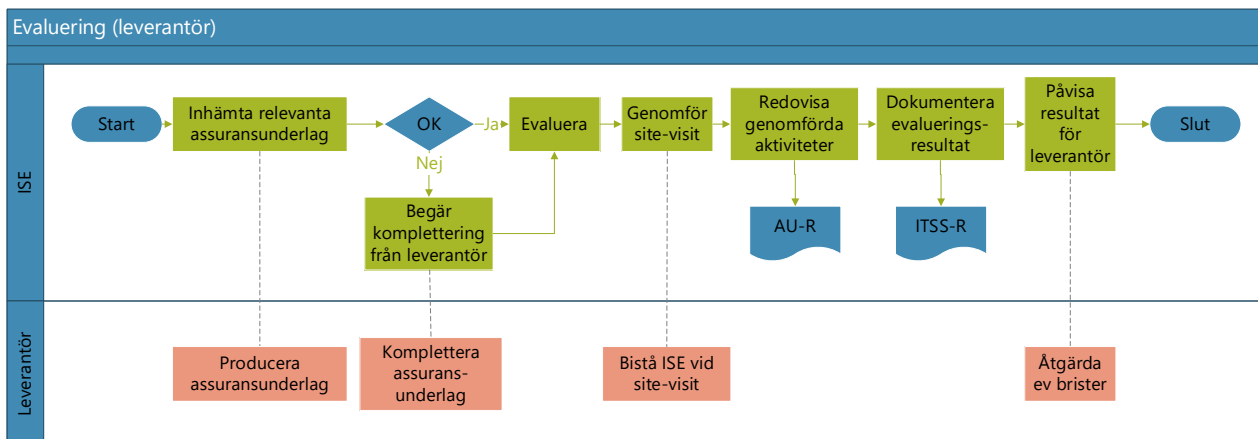
- Evaluering av leverantörens säkerhetsskydd i utvecklingsmiljön
- Evaluering av leverantörens konfigurationsledningssystem
- Evaluering av leverantörens bristhanteringsystem
- Evaluering av leverantörens anskaffnings- och integrationsprocesser

Flera av ISE granskningsaktiviteter kräver ett eller flera besök hos leverantör, s.k. site-visit, i syfte att på plats verifiera att t.ex. konfigurationsledningssystem finns implementerat, och faktiskt används i produktionen. Detsamma gäller ISEs verifiering av leverantörens säkerhetsskydd i utvecklingsmiljön.

Resultatet från ISE granskning av leverantören, samt utfall från site-visit, redovisas i AU-R respektive ITSS-R.

I den mån det är möjligt ska leverantör ges möjlighet att åtgärda eventuella brister som identifieras i detta processavsnitt.

Figur 31 visar aktiviteterna i denna detta processavsnitt.



Figur 31 ISE evaluering (leverantör)



Ej sekretess

## ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	61(76)

### 5.3.2.4 Evaluering (system, dokumentation)

Detta processavsnitt syftar till att evaluera den implementerade säkerhetslösningen i systemet, samt att evaluera all relevant systemdokumentation och tillhörande assuransdokumentation.

Processavsnittet inleds med att ISE samlar in all relevant dokumentation och granskar denna. Om ISE anser att det behövs, ska leverantör erbjudas möjligheten att komplettera denna. Därefter vidtar själva evalueringen. Resultatet från evalueringen dokumenteras i AU-R respektive ITSS-R, beroende på vilket krav som evalueras.

Om det är möjligt bör leverantören ges möjlighet att komplettera dokumentation efter första evalueringen, och AU-R respektive ITSS-R ska då uppdateras efter komplettering.

När evalueringen är klar tas VMH-R fram. VMH-R innehåller de krav på omgivningen som tidigare definierats i ITSS-D, och som även finns i ITSS-R. Den omhändertar även eventuellt tillkommande krav på omgivningen vilka har identifierats i samband med evalueringen.

VMH-R byggs med fördel upp som en checklista, vilken kan användas inför lokal ackreditering.

ISE klargör också huruvida det finns behov av kompletterande säkerhetstester. Dessa tester specificeras på en övergripande nivå och specifikationen lämnas till ISTM för vidare planering och utförande av tester.

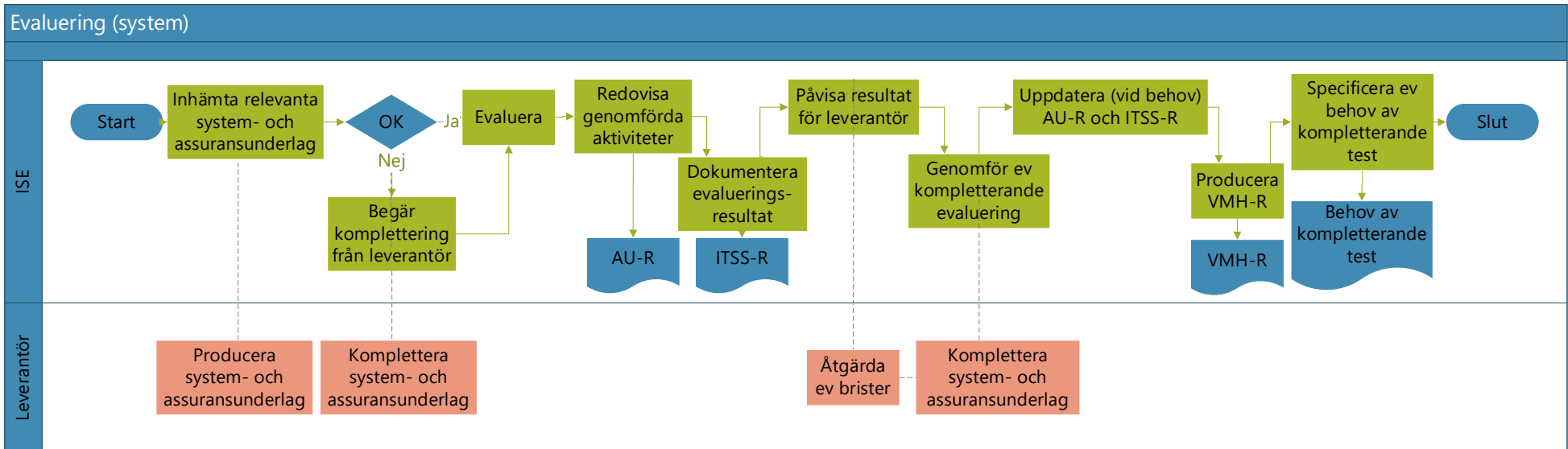
Figur 32 visar aktiviteterna i detta processavsnitt.



Ej sekretess

### ISD 3.1 Processbeskrivning

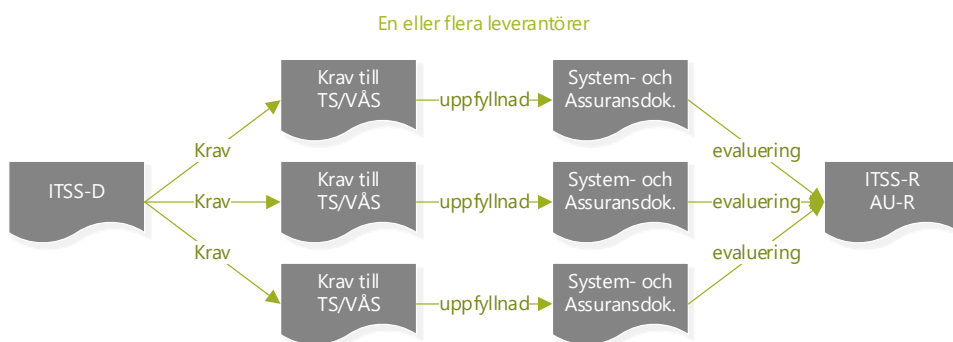
Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	62(76)



Figur 32 ISE evaluering (system)

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	63(76)

I detta processavsnitt är det viktigt att notera att om det finns flera leverantörer som producerar olika delsystem som ska integreras till det system som definierats som ackrediteringsobjektet, så är det bara inom ISD som den totala säkerhetslösningen finns beskriven och kravställd. Det är således viktigt att ISE tar in system- och assurancesunderlag från samtliga leverantörer för att kunna evaluera den totala säkerhetslösningen (enligt Figur 33), både avseende funktionalitet och assurance.



Figur 33 ISE evaluering vid mer än en leverantör

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	64(76)

### 5.3.2.5 Test av systemet

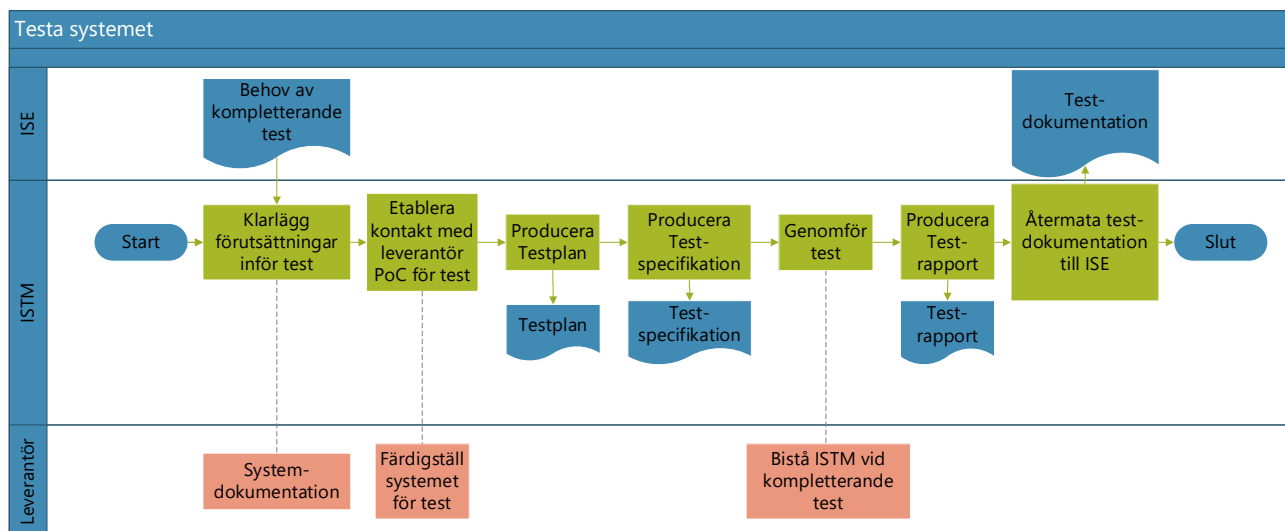
Efter, eller i samband med, evalueringen kan om ISE så anser vara påkallat begära att kompletterande tester ska genomföras. Dessa tester, beroende på komplexitetsgrad och behov av olika testverktyg, bör då göras av ISTM. Enklare tester i form av stickprov kan göras av ISE.

Efter att ISTM samlat in relevanta underlag för genomförande, inklusive ISE eventuella behov av kompletterande test, tar ISTM kontakt med leverantör inför genomförande av test.

Leverantör ska kunna tillhandahålla systemet i ett testbart skick, men om det av praktiska orsaker inte är möjligt ska leverantören ge ISTM möjlighet att testa systemet hos leverantören.

ISTM producerar testplan och testspecifikation innan genomförande av test och dokumenterar resultatet i en testrapport. Denna testrapport ges sedan till ISE som indata för dennes restrisikanalyser.

Figur 34 visar aktiviteterna i detta processavsnitt.



Figur 34 ISTM test av systemet

ISTM kan vid behov delta på leverantörs tester för att erhålla förståelse för systemet. Beroende på system, kan dessa tester exempelvis vara:

- TRR - Test Readiness Review
- FAT – Factory Acceptance Test
- SIAT – Site Acceptance Test
- SAT – Sea Acceptance Test
- FRR - Flight Readiness Review
- HAT – Harbour Acceptance Test

ISTM deltagande i leverantörs testverksamhet kan med fördel regleras i VÅS.



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	65(76)

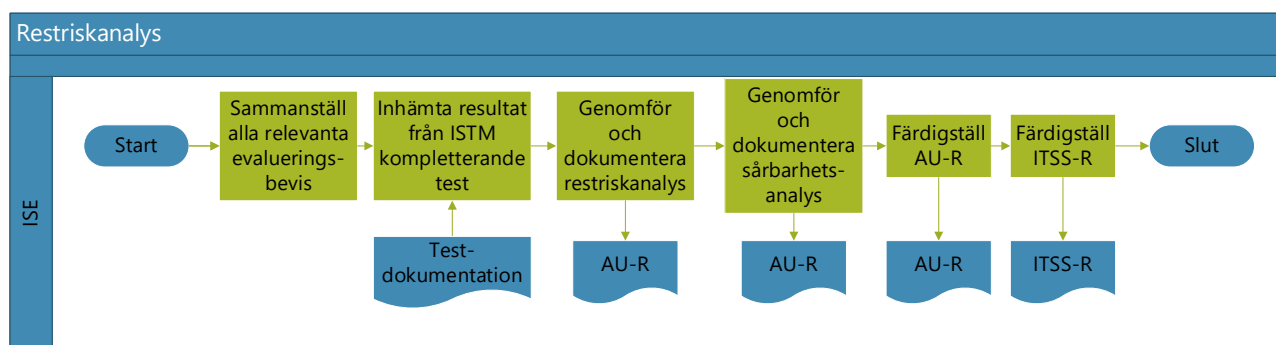
### 5.3.2.6 Restriskanalys

Efter ISE evaluering av leverantör och systemet (eller fler i det fall det finns multipla leverantörer) samt ISTM tester av det kompletta systemet, ska ISE genomföra restriskanalys samt sårbarhetsanalys.

Resultatet från båda dessa analyser dokumenteras i AU-R.

I detta processavsnitt är det också lämpligt att ISE färdigställer AU-R och ITSS-R för ISM ackrediterbarhetsbedömning.

Figur 35 visar aktiviteterna i detta processavsnitt.



Figur 35 ISE Restriskanalys

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	66(76)

### 5.3.2.7 Informationssäkerhetsdeklaration

Det sista processavsnittet i Realisera är att deklarerat att systemet (ackrediteringsobjektet) uppfyller FM:s krav på informationssäkerhet och att det, utifrån ett informationssäkerhetsperspektiv, är säkert att använda givet specificerade förutsättningar.

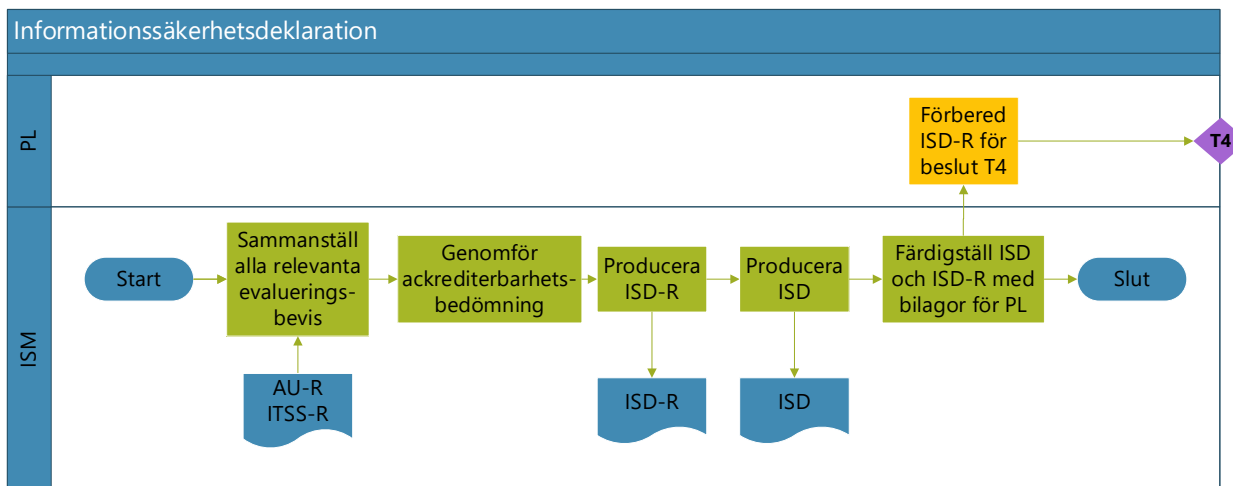
FMV deklARATION dokumenteras i ISD, Informationssäkerhetsdeklaration.

Denna deklARATION bygger på ackrediterbarhetsbedömningen i ISD-R, vilken vilar på utvärderingsresultaten i AU-R och ITSS-R.

Krav på användning är förtecknad i VMH-R.

ISM färdigställer samtliga ISD-R underlag samt ISD färdigställs av ISM för vidare beredning av Projektledare, inför FMV VHL T4-beslut.

Figur 36 visar aktiviteterna i detta processavsnitt.



Figur 36 ISD Informationssäkerhetsdeklaration



Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	67(76)

## 5.4 Vidmakthålla

Efter FMV VHL T4-beslut överlämnar FMV systemet till FM, tillsammans med erforderlig dokumentation. När FM tagit beslut BOAC och BOAL kan systemet driftsättas. Efter driftsättning ansvarar FM för vidmakthållande och beställer erforderligt stöd från FMV.

Under vidmakthållandeskedet av tekniska system kommer modifieringar i många fall att genomföras flera gånger. Beroende på modifieringens karaktär och omfattning delas denna upp i följande kategorier:

- Prestandahöjande modifiering
- Mindre prestandahöjande modifiering
- Modifiering syftande till livstidsförlängning

När det rör sig om prestandahöjande modifiering, så utför FMV denna typ av modifieringar på uppdrag av FM. För att förberedelseskedet ska kunna slutföras och upphandling av modifieringen ska vara möjlig, krävs att FM överlämnar detaljerad information om den typkonfiguration av systemet som ska modifieras. Detta görs lämpligtvis genom en sk. Konfigurationsöverlämning (KÖL). När så skett, fastställer FMV informationen som ingångsvärde för att genomföra modifieringsarbetet genom att fatta designbeslut T5. Fastställd målsättning som beskriver målet med modifieringen och som ska ligga till grund för upphandling, fastställs genom designbeslut T2. Inför anskaffningsskedet för en modifiering finns således ett T5-beslut som beskriver den konfiguration som ska modifieras, så att den överensstämmer med målsättningen som fastställts i T2-beslutet.

När det gäller mindre prestandahöjande modifieringar ansvarar FM för planering, förberedelser och genomförande. FM kan beställa stöd från FMV för detta arbete. Behovet av att fastställa ingångsvärden, i form av typkonfiguration som ska modifieras och vilken målsättning som gäller, är detsamma som för prestandahöjande modifieringar (enligt ovan). Då FMV inte har designansvar, kan dessa ingångsvärden dock inte fastställas i formella designbeslut (T2 och T5) på samma sätt.

Modifieringar som sker inom ramen för vidmakthållandet gäller primärt livstidsförlängande åtgärder, och inte sådana som syftar till att tillföra ny funktionalitet eller att höja prestandan i systemet. FM ansvarar för att planera, förbereda och genomföra denna kategori av modifieringar. FM kan beställa stöd från FMV för detta arbete. Behovet av att fastställa ingångsvärden, i form av typkonfiguration som ska modifieras och vilken målsättning som gäller, är detsamma som för Prestandahöjande modifieringar (enligt ovan). Då FMV inte har designansvar, kan dessa ingångsvärden dock inte fastställas i formella designbeslut (T2 och T5) på samma sätt.

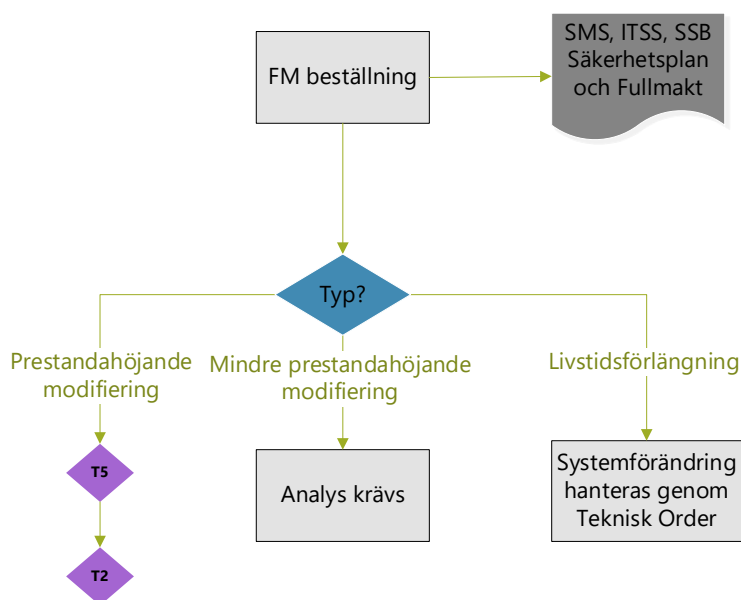
### 5.4.1 Övergripande fasbeskrivning

ISD-fasen Vidmakthålla inleds via FM beställning till FMV. Fasen befinner sig dock alltid mellan T4 och T5 enligt FMV VHL.

Beroende på vilken typ av beställning FM lägger på FMV, kan ISD-arbetet genomföras på olika sätt. Figur 37 illustrerar de olika sätt som ISD-arbetet kan genomföras på. Försvarsmakten överlämnar nödvändig information, och FMV fastställer informationen som ingångsvärde för att genomföra modifieringsarbetet genom att fatta designbeslut T5. Fastställd målsättning, som

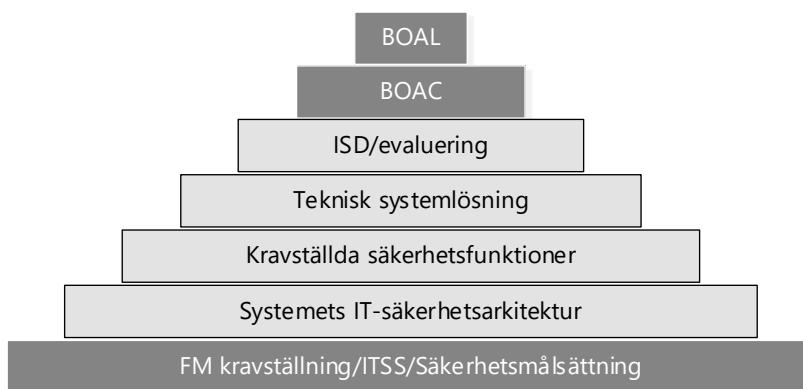
Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	68(76)

beskriver målet med modifieringen och som ska ligga till grund för upphandling, fastställs genom designbeslut T2. Inför anskaffningskedet för en modifiering finns således ett T5-beslut, som beskriver den konfiguration som ska modifieras så att den överensstämmer med målsättningen som fastställts i T2-beslutet. Forsvarsmakten utfärdar en fullmakt till FMV viken redogör för vilka befogenheter som FMV tilldelas för modifieringens genomförande, liksom en säkerhetsplan för modifieringen.



Figur 37 Varianter på modifiering i Vidmakthålla

Oavsett omfattning på FM modifiering, ska FMV alltid genomföra en analys av beställd modifiering utifrån ett informationssäkerhetsperspektiv. En generell utgångspunkt för denna analys illustreras i Figur 38.



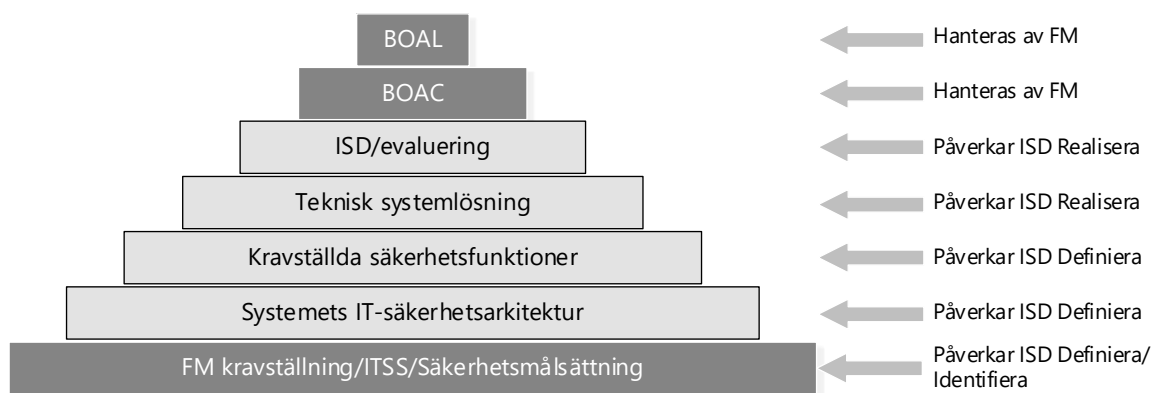
Figur 38 Bedömningsmodell avseende modifiering ur ett informationssäkerhetsperspektiv

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	69(76)

Syftet med denna bedömning är att klargöra omfattningen av ISD-arbetet som kan komma att behöva genomföras givet den beställda modifieringen. Säkerheten i det driftsatta systemet (BOAL) byggs upp av flera lager beslut och analyser. Varje lager är beroende av grunden som läggs i underliggande lager.

De mörkare rutorna i Figur 38 åskådliggör FM ansvar avseende grundläggande kravställning, samt förändrade centrala eller lokala driftsättningsbeslut. Då det gäller förändrade centrala, eller lokala, driftsförutsättningar är inte ISD-processen tillämplig, men om analysen påvisar att de grundläggande förutsättningarna för FMV krav- och evalueringsaktiviteter påverkats, ska ISD-processen användas i tillämplig omfattning för att uppdatera ISD.

De ljusare rutorna i Figur 38 åskådliggör FMV ansvar avseende IT-säkerhetsarkitektur, kravställning och evaluering.



Figur 39 Påverkan av modifiering ur ett informationssäkerhetsperspektiv

Figur 39 visar, ur ett generellt perspektiv, hur modifieringar kan påverka FMVs behov av att tillämpa ISD-processen. Genom att identifiera det lägsta lager som modifieringen berör, är det möjligt att erhålla en uppfattning om var i ISD det är lämpligt att påbörja förnyat informationssäkerhetsarbete. Detta lager och alla ovanliggande blir då också mer eller mindre berörda. Respektive lagars påverkan på ISD/FM kan utläsas till höger i bilden.

Aspekter på modifiering som bör beaktas kan exempelvis vara:

- Nya eller ändrade regelverk, lagar eller kravdokument
- Förändringar i hotbild
- Funktionsförändring (ny, förändrad eller borttagen intern eller extern funktion)
- Gränsyteförändring (ny, förändrad eller borttagen intern eller extern gränsyta)
- Förändrade användningsfall (t ex ny operativ driftmiljö)
- Förändringar i systemets omgivning
- Tidigare identifierade brister som har justerats
- Tidsatt beslut har löpt ut
- Systemuppdatering eller säkerhetsuppdateringar (patch motsv)



Ej sekretess

ISD 3.1 Processbeskrivning

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	70(76)

Tabell 8 sammanfattar ISD Vidmakthålla-fas.

Vidmakthålla	VHL T4 till T5
Syfte	Vidmakthålla, uppdatera och styra förändringsarbetet
Aktiviteter <sup>5</sup>	Initiera ISD modifiering Bedömning Evaluering/uppdatering av ISD-underlag
ISD dokument	ISD-V AU-V ITSS-V
Indata	FM krav (SMS, SM, ITSS, TTEM, SYD, m.m.) ISD-R AU-R ITSS-R VMH-R
Utdata	ISD-V AU-V ITSS-V
Aktiva roller	FM Verko Designledning Produktledare ISM ISA ISE ISTM Leverantör (-er)

Tabell 9 – Sammanställning ISD Vidmakthålla

<sup>5</sup> Beror på typ av modifiering

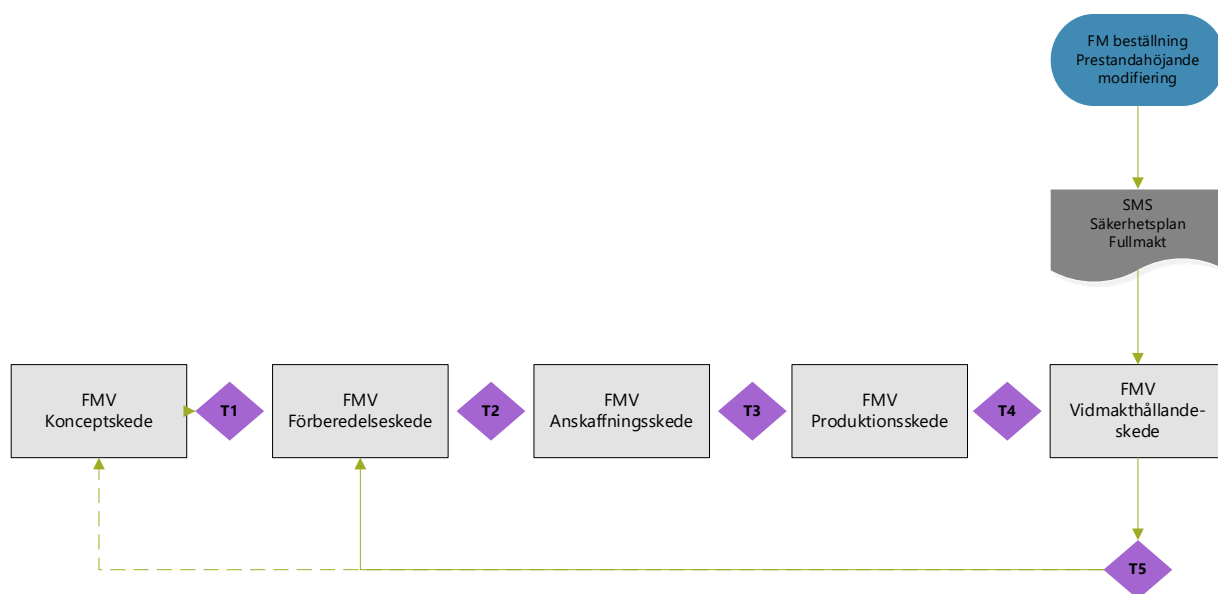
Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	71(76)

## 5.4.2 Detaljerad fasbeskrivning

### 5.4.2.1 Prestandahöjande modifiering

I fallet med prestandahöjande modifiering tar FMV T5-beslut med stöd av FM indata. ISD-processen, liksom genomförandeprojektet, startar om i ISD Definiera (FMV VHL Förberedelseskede). Det kan finnas möjlighet att modifieringen är av sådan art att ISD och VHL behöver återgå till Identifiera respektive Konceptskede.

Figur 40 visar hur prestandahöjande modifiering hanteras i FMV VHL.



Figur 40 Prestandahöjande modifiering (T5 till T2)

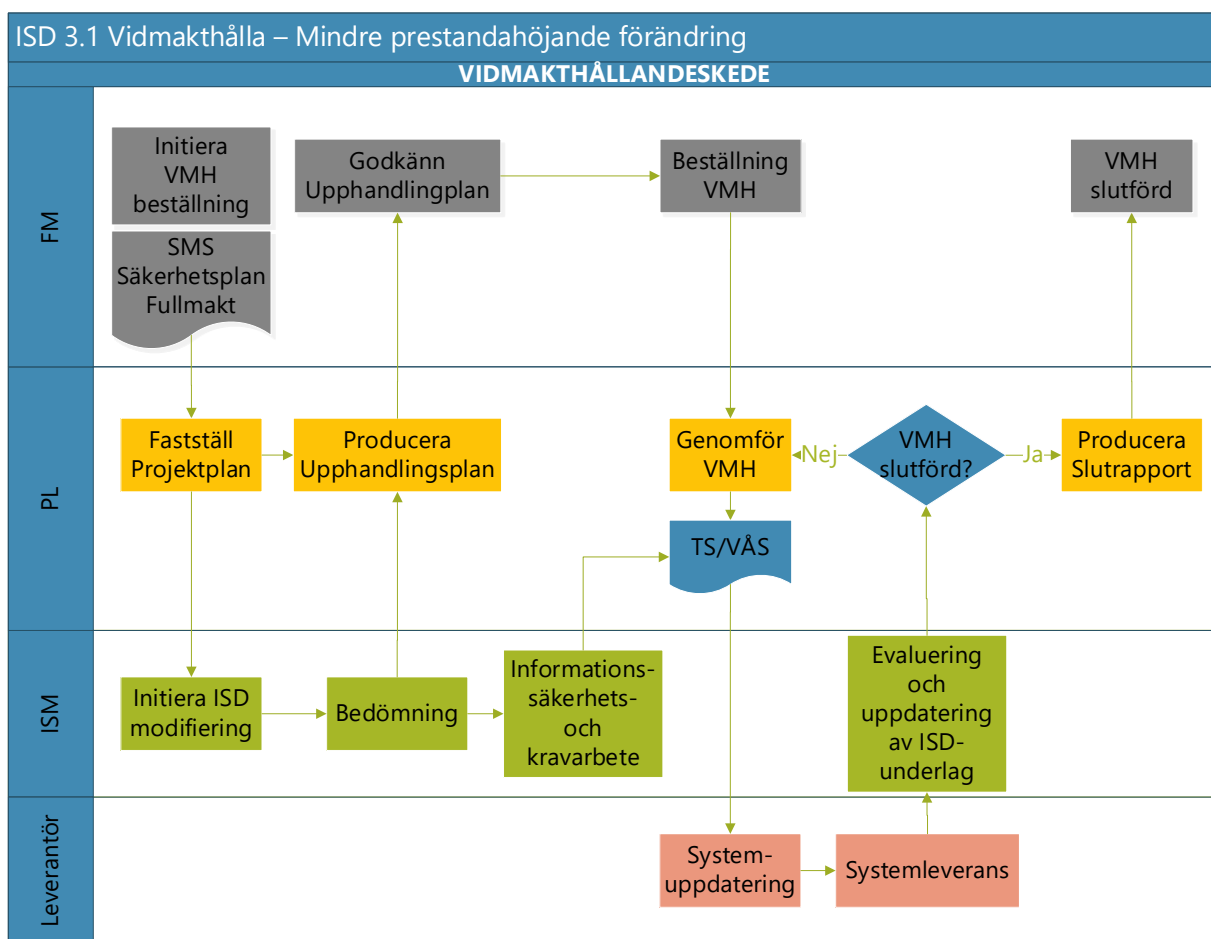
I detta fall genomförs de ISD-aktiviteter som tidigare beskrivits i kapitel 5.2 (Definiera) och kapitel 5.3 (Realisera). Modifieringen kan också medföra att ISD-arbetet återstartas i Identifiera, enligt beskrivningar i kapitel 5.1. FM indata för beställd modifiering ligger till grund för analys av säkerhetspåverkan. Resultatet från denna analys avgör omfattning på kommande ISD-arbete, vilket dokumenteras i ISD-plan.

### 5.4.2.2 Mindre prestandahöjande modifiering

Modifieringar av typen Mindre prestandahöjande, innebär inte per automatik att T5-beslut tas och att ISD-processen återstartas i Definiera. Däremot är det av vikt att analysera förändringen ur ett informations säkerhetsperspektiv för att klargöra vilken påverkan modifieringen får.

Vägledande i denna analys är bedömningsmodellen i Figur 39.

Figur 41 visar översiktligt aktiviteterna för mindre prestandahöjande modifiering.



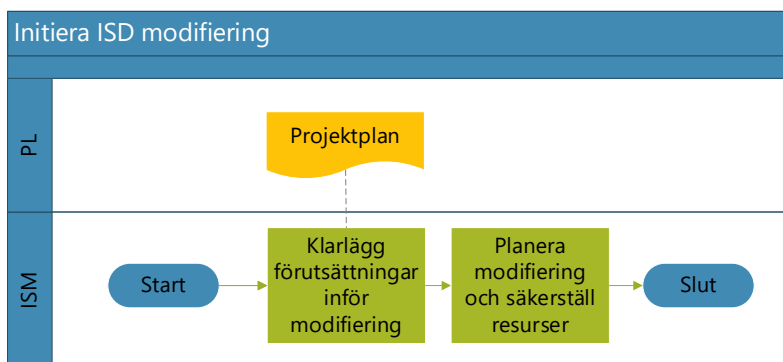
Figur 41 Mindre prestandahöjande modifiering

Efter det att projektplanen är fastställd, klargör ISM förutsättningarna för ISD-arbetet i Vidmakthålla. ISM inhämtar relevanta ISD-underlag i form av ISD-R (om föreliggande modifiering är den första efter den initiala driftsättningen), eller ISD-V (om föreliggande modifiering inte är den första efter driftsättning). ISM kan också ge stöd till FMV Projektledare i framtagning av Projektplan.

När ISM har klarlagt förutsättningarna genomförs ISD-planering och resurstillsättning i samråd med FMV Projektledare.

Figur 42 visar aktiviteterna i detta processavsnitt.



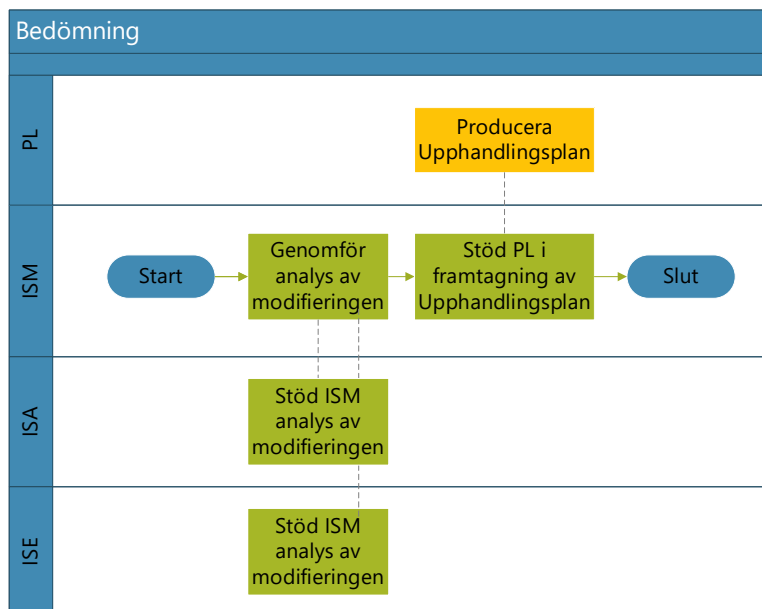


Figur 42 Initiera ISD modifiering

I processavsnittet Bedömning genomför ISM analys av den modifiering FM beställt. Analysen grundar sig på de bedömningspunkter som beskrivs i kapitel 5.4.1. ISA och ISE kan vid behov stötta ISM i denna analys.

Efter genomförd analys kan ISM stötta FMV Projektledare i framtagning av upphandlingsplan.

Figur 43 visar aktiviteterna i detta processavsnitt.

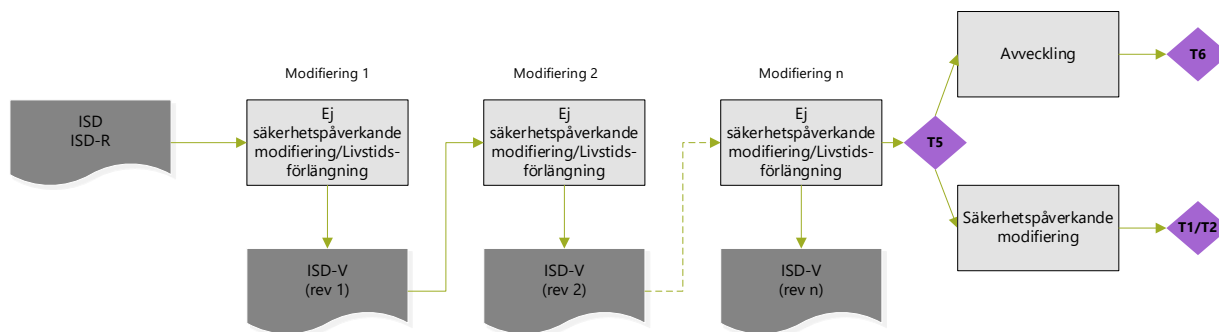


Figur 43 Bedömning

Processavsnittet Evaluering/Uppdatera ISD-underlag startar när FM har upphandlat modifieringen av FMV. Inledningsvis klarlägger ISM huruvida den gällande kravställningen har förändrats. Om så är fallet, tar ISA över vidare analyser och uppdaterar ITSS-V vid behov. Finns inte ITSS-V sedan tidigare, används ITSS-R som källa och ITSS-V uppdateras med bibehållen struktur.

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	74(76)

Figur 44 illustrerar nyttjandet av ISD-V för spårbarhet i ISD under systemets vidmakthållande. ISD-V följer systemet till prestandahöjande modifiering (som då beslutas via T5), eller till FM beslut om avveckling<sup>6</sup>. Avvecklingen avslutas i och med T6-beslut.



Figur 44 Användning av ISD-V under systemets vidmakthållande

Om kravbilden är densamma som gäller för ITSS-R/V, klarlägger ISM om det finns behov av kompletterande evaluering. Om så är fallet tar ISE över arbetet, och om denne anser att det finns behov av kompletterande säkerhetstester så genomförs dessa av ISTM. Leverantör stöttar ISE och ISTM arbete med system- och assurancesunderlag, samt säkerställer tillgång till systemet för kompletterande tester.

Efter genomförd evaluering, med eventuella kompletterande tester, uppdaterar ISE ITSS-V och AU-V (eller skapar dessa underlag om de inte fanns tidigare).

Slutligen producerar ISM ISD-V (utifrån AU-V och ITSS-V) samt bistår FMV Projektledare med modifieringens slutrapport.

Figur 45 visar aktiviteterna i detta processavsnitt.

<sup>6</sup> Notera att avveckling inte behandlas i ISD version 3.1.



Ej sekretess

ISD 3.1 Processbeskrivning

Datum

Diarienummer

Ärendetyp

2021-05-18

20FMV5903-1:1

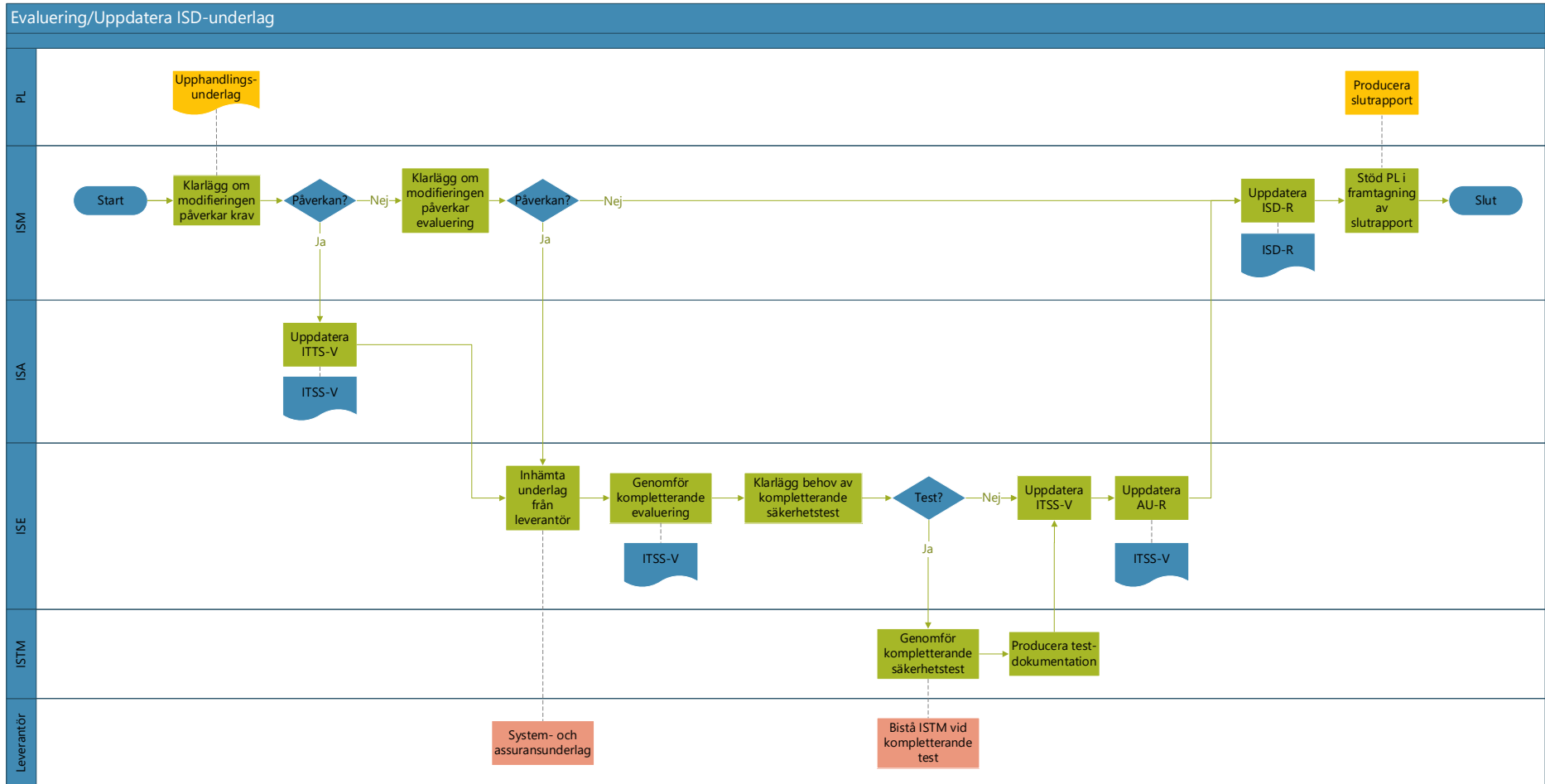
3.5

Dokumentnummer

Sida

3.1.0

75(76)



Figur 45 Uppdatera ISD-underlag



**Ej sekretess**

## **ISD 3.1 Processbeskrivning**

Datum	Diarienummer	Ärendetyp
2021-05-18	20FMV5903-1:1	3.5
	Dokumentnummer	Sida
	3.1.0	76(76)

### **5.4.2.3 Modifiering syftande till livstidsförlängning**

Aktiviteter avseende modifiering syftande till livstidsförlängning är, ur ett ISD-perspektiv, detsamma som mindre prestandahöjande modifieringar.

Detta innebär att, oavsett vilken typ av livstidsförlängning som FM beställer, så ska motsvarande analyser genomföras utifrån ett informationssäkerhetsperspektiv.