ISD-PROCESSEN ISD 3.0

Innehåll

1 Basfakta

1.1 Syfte med detta dokument

Detta dokument beskriver ISD-processen version 3.0 (även benämnt ISD 3.0).

1.2 Revisionshistorik

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Första utgåva	DAOLO

Tabell 1 - Revisionshistorik

1.3 Terminologi och begrepp

Se Bilaga 1.

1.4 Bilageförteckning

Bilaga 1. Begrepp och Definitioner 18FMV6730-8:1.1
Bilaga 2. ISE Granskningsinstruktion 18FMV6730-8:1.2
Bilaga 3. SystGL granskningsinstruktion 18FMV6730-8:1.3

1.5 Referenser

Dokumenttitel	Dokumentbeteckning, datum	Utgåva nr
[1] Oberoende granskning	16FMV11109:2	1

Tabell 2 - Referenser

2 Inledning

2.1 Syfte

Syftet med ISD är att säkerställa FMVs uppgift att leverera och vidmakthålla realiserbara system till Försvarsmakten inom ramen för FMV designansvar, avseende IT- och informationssäkerhet. Detta görs genom att stödja samtliga roller inom FMV i informationssäkerhetsarbetet under ett systems hela livscykel; *identifiera, definiera, realisera, vidmakthålla och avveckla.*

Realiserbarhetsbedömningar i tidigt skede av produktprocessen ger effektivisering med avseende på kostnader och tid för genomförandeprojektet och därmed inför leveranser till FM.

Informationssäkerhetsarbetet följer produktprocessen med dess S-beslut och hanteras på samma sätt som övriga områden (t ex Systemsäkerhets och ILS) för utveckling av system.

Processen tydliggör aktiviteter för att realisera informationssäkerhetsaspekterna i System Engineerings (SE) som ska genomföras i genomförandeprojektet.

ISD-Processen 3.0 baseras på aktiviteter, där resultatet får dessa aktiviteter dokumenteras i artefakter.

2.2 Bakgrund

ISD-processen 3.0 är utökad från version 2.3 till att omfatta ett stöd för informationssäkerhetsarbetet för hela produktprocessen enligt FMV VHL, vilket underlättar integrering med FMV övriga processer. ISD version 2.3 styr informationssäkerhetsarbetet i VHL-faserna *Definiera* och *Realisera.* ISD version 3.0 täcker samtliga VHL-faser från *Identifiera* till och med *Avveckla.*

Historiskt sett har FMV genomförandeprojekt inte getts tillräckliga förutsättningar att genomföra informations-säkerhetsarbetet i fasen *Definiera,* vilket är grunden för att realisera systemet. ISD 3.0 omfattar därför hela systemlivscykeln från beställning från FM till avveckling med fasen *Identifiera* som nytt processteg i ISD 3.0 samt Kontrollpunkter i ISD processen kopplade till FMV VHL.

Bedömningar kring realiserbarhet behöver göras kontinuerligt, inte minst med tanke på FMV Designansvar. Även här spelar en högre integration med VHL in. Realiserbarhetsbedömningar följer S-besluten.

För att skapa ett ackrediterbart IT-system som uppfyller de funktionella kraven och IT-säkerhetskraven som en helhet är det därför viktigt att informationssäkerhetsarbetet integreras i System Engineerings-arbetet. Efter driftsättning ska informationssäkerhetsnivån upprätthållas i vidmakthållande fram till avveckling.

2.3 Övergripande förändringar

ISD-processen 3.0 bygger vidare på version 2.3. De största förändringarna är:

- Kontinuerlig realiserbarhetsbedömning för att kunna anpassa och reglera informationssäkerhetslösningen över hela livscykeln.

- Realiserbarhetsbedömningar i tidigt skede av produktprocessen ger effektivisering med avseende på kostnader och tid för genomförandeprojektet och därmed inför leveranser till FM.
- Genom att beskriva PrLs aktiviteter för informationssäkerhetsarbetet i *Identifiera* ges genomförandeprojektet de förutsättningar som krävs för att utveckla realiserbara IT-system.
- Informationssäkerhetsarbetet följer produktprocessen med S-besluten och hanteras på samma sätt som övriga områden för utveckling av system.

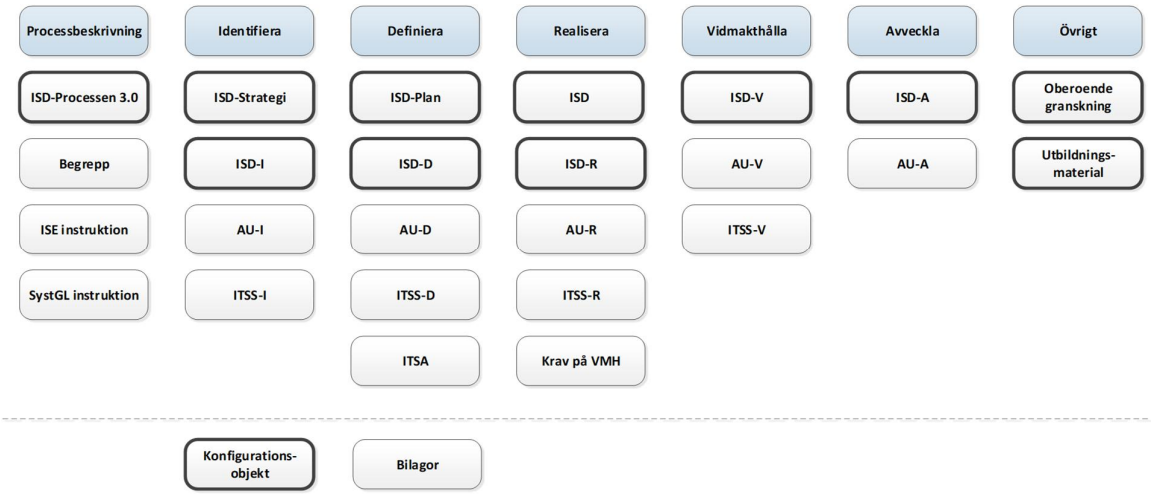
2.4 ISD-Processen 3.0 stöd

Stödet till ISD-Processen är i huvudsak uppbyggt på mallar. I dessa mallar finns det vägledande texter.

I varje mall finns följande stödinformation:

- Mallinformation – revisionshistorik avseende mallen
- Mallinstruktion – hur arbetet med mallen ska bedrivas
- Omfattning – beskrivning av hur mallen ska användas
- Att tänka på – stöd vid användning av mallen

Följande figur illustrerar stödet kring ISD-Processen.



Figur 1 Omfattning ISD-Processen inklusive processtöd

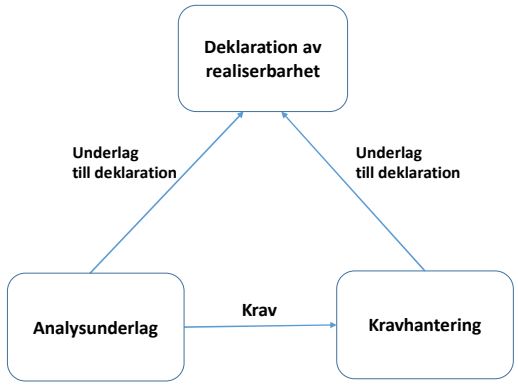
3 ISD-Processen

3.1 Övergripande beskrivning

Realiserbarhet är den röda tråden i ISD-Processen och bedömningen görs inför varje S-beslut med utgångspunkt från:

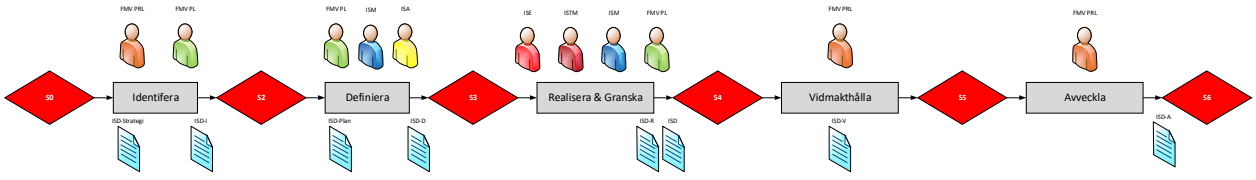
- Ackrediterbarhet – kravuppfyllnad mot FM krav
- Kostnadseffektivitet – krav på informationssäkerhet vägs mot bedömd kostnad för informationssäkerhetslösningen.
- Projektrisker
- Integration med SE – informationssäkerhetsarbetets integration med SE för avvägning av krav mm

Realiserbarhetsbedömningen deklareras i en informationssäkerhetsdeklaration, i processtödet benämnt ISD-x där x är namnet på aktuellt skede i produktprocessen. Deklarationen baseras på analyser (AU-x) och krav (ITSS-x). Med realiserbarhet i detta sammanhang syftas till informationssäkerhet. Ackrediterbarhet är en betydande faktor, men även aspekter som projektrisker och kostnadseffektivitet spelar in.



Figur 2 Struktur Deklaration av realiserbarhetsbedömning

Hela ISD-processen, med huvudsakliga artefakter och aktörer beskrivs i följande figur.



Figur 3 Översiktlig ISD-processen

3.1.1 Identifiera

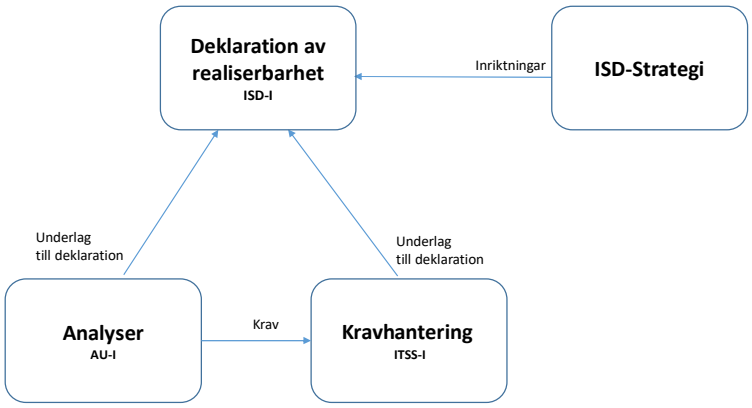
Realiserbarhetsbedömningen i *Identifiera* inför FMV VHL S2-beslut baseras huvudsakligen på att relevant indata (främst Säkerhetsmålsättning, men även andra relevanta kravdokument) från FM har erhållits så att genomförandeprojektet har förutsättning att leverera ackrediterbart IT-system.

Bedömningen görs med utgångspunkt från analyser på hur IT-systemet ska användas, verksamhetsmässig exponering, informationsklassning, verksamhetens sårbarheter och konsekvenser mm.

Indata från FM kan vara systemmålsättning, säkerhetsmålsättning och FM ITSS. Arbetet med analyserna kan göras iterativt för att FM och FMV ska förstå varandras behov. Resultatet från analyserna dokumenteras i AU-I och de kravkällor som framkommer i analyserna dokumenteras i ITSS-I.

ISD-strategin är ett viktigt indata för att klargöra förutsättningarna för genomförandeprojektet. Strategin klargör ackrediteringsobjektet, pekar på utmaningar främst med avseende på system av system, ger inritningar avseende återbruk av komponenter, relationer till andra projekt och fördelar krav som finns på system av system.

Aktiviteter för Identifiera beskrivs mer i detalj i avsnitt 5.1.



Figur 4 Realiserbarhetsbedömning Identifiera

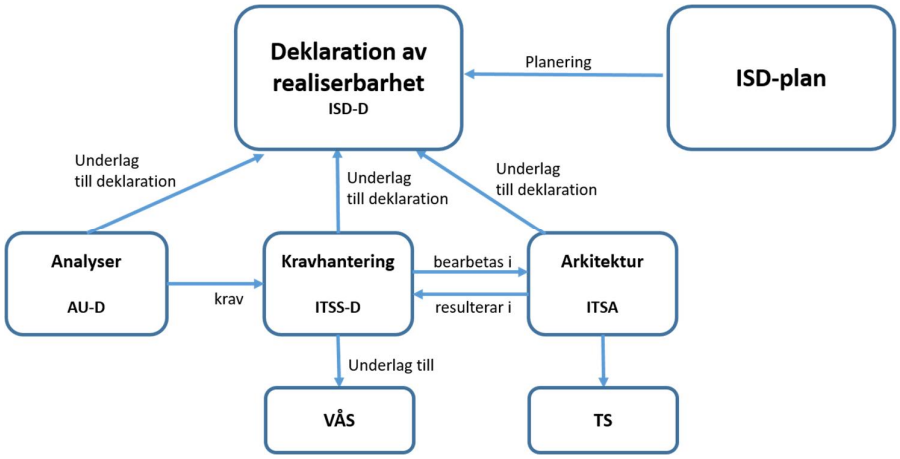
3.1.2 Definiera

Realiserbarhetsbedömningen i *Definiera* inför FMV VHL S3-beslut baseras huvudsakligen på framtagen IT-säkerhetsarkitektur som visar på balansen mellan verksamhetens behov (funktionalitet) och säkerhetsfunktioner kopplat till kravnivå.

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

ITSS-D följer strukturen på FM ITSS och innehåller såväl funktionella säkerhetskrav som assuranskrav. De funktionella säkerhetskraven föder Teknisk Specifikation (TS) medan assuranskraven föder Verksamhetsåtagandespecifikation (VÅS) inför upphandling.

ISD-planen, som tas fram av ISM i denna fas, styr informationssäkerhetsarbetet i genomförandeprojektet. Informationssäkerhetsarbetet planeras i form av omfattning resurser, utmaningar, aktiviteter, tidplan och artefakter. Projekt-, SE- och VoV-planer ska korreleras med ISD-planen för att säkerställa att ISD-planen är integrerad i dessa.



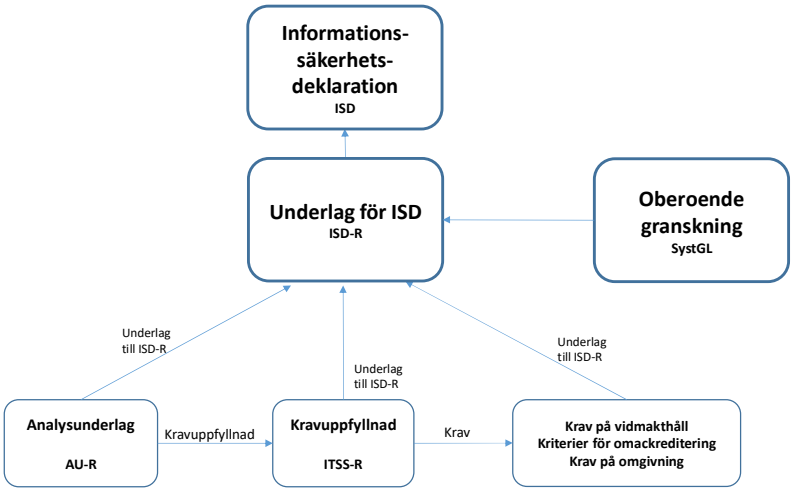
Figur 5 Realiserbarhetsbedömning Definiera

3.1.3 Realisera

Realisera är genomförandeprojektets produktionsskede och leverans. I *Realisera* är IT-systemet klart för leverans och en ackrediterbarhetsbedömning görs inför FMV VHL S4-beslut. Ackrediterbarhetsbedömning baseras på kravuppfyllnad, riskbedömning och yttrande från oberoende granskning. Inför bedömningen görs relevanta analyser såsom analys 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 det fastställda underlaget inför ackreditering på FM.
I underlaget finns angivet vilka krav som inte uppfylls av systemets IT-säkerhetslösning utan ska uppfyllas av systemets omgivning. Det är FMs ansvar att se till att de kraven uppfylls innan hemställan om FM MUST yttrande.

ISD-R omfattar också vilka kriterier som gäller vid förändring i samband med vidmakthåll och när förändring leder till omackreditering.

I S4-beslutet gör FMV den formella deklarationen (ISD) till FM att systemet uppfyller FM krav på IT-säkerhetslösning med tolererbar risk, att avvikelser hanteras, fastställd ISD-plan har följts samt att ITSS-R följer FMV norm.



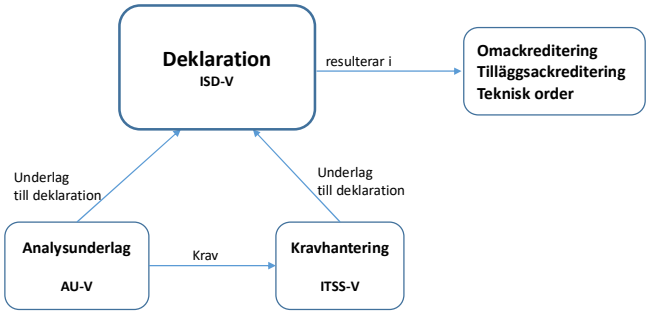
Figur 6 Ackrediterbarhetsbedömning Realisera

3.1.4 Vidmakthålla

I *Vidmakthålla* är systemet överlämnat och i drift. För ett system sker förändringar kontinuerligt som innebär att deltaanalys med avseende på grad av påverkan på informationssäkerhetslösningen behöver genomföras. Deklaration i *Vidmakthålla* är en bedömning av stor eller liten ändring avseende på informationssäkerhet. Första bedömning utgår från ISD-R från *Realisera* där krav på vidmakthåll och kriterier för omackreditering inhämtas. Från andra bedömningen sker versionshantering av ISD-V.

Resultatet av bedömningen avgör om och vilken form av ackreditering som behöver genomföras. Är förändringen liten eller en förbättring av informationssäkerheten realiseras den med hjälp av Teknisk Order eller motsvarande. Är förändringen stor startar projektet i *Identifiera* eller *Definiera* med ett systemutvecklingsarbete som ska mynna ut i en omackreditering (ny ackreditering) eller tilläggsackreditering (komplettering av gällande ackreditering med att ackreditera de tillägg man identifierat och värderat).

.



Figur 7Deklaration vidmakthålla

3.1.5 Avveckla

I *Avveckla* genomförs en sekretessbedömning i enlighet med FMV VHL *Avveckla*.

3.2 Kravhantering

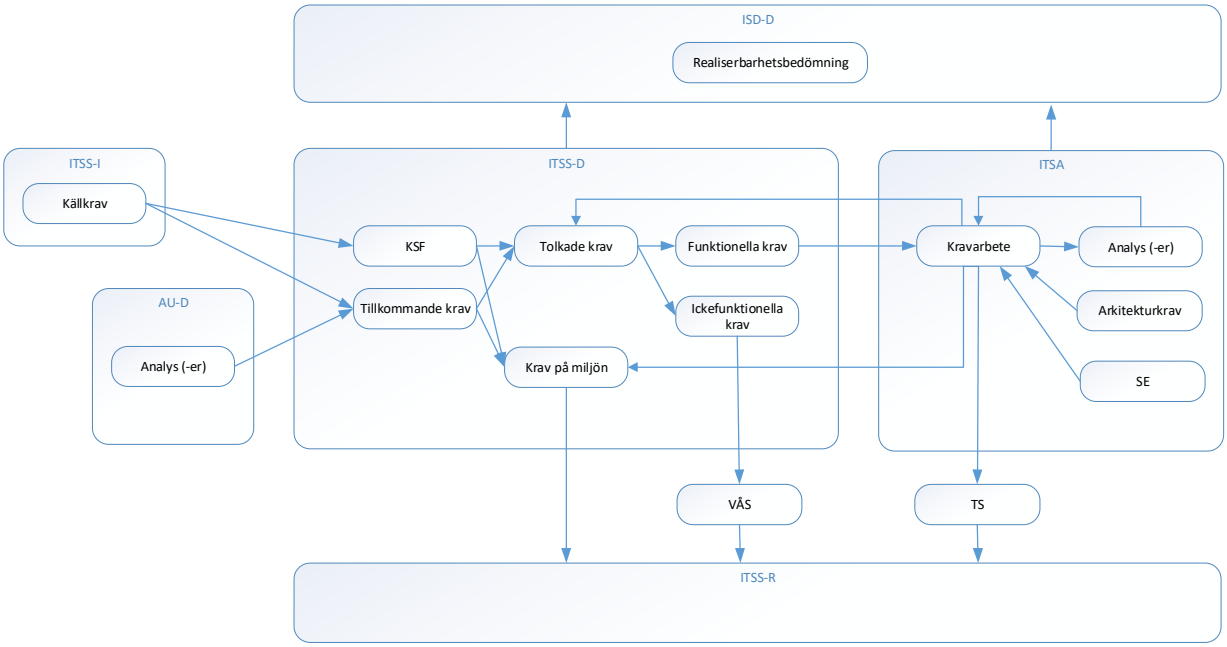
Kravhantering utgör det gemensamma språket mellan FM, FMV och Leverantör och är även det som gör det möjligt att realisera ett ackrediterbart system.

Kravhantering i ISD-Processen är uppbyggt så att det finns en spårbarhet från Identifiera till Vidmakthålla. Kraven från varje skede dokumenteras i ITSS, och kravunderlagen är uppbyggda på samma sätt så att de kan utvecklas successivt fram till Realisera.

Figur 8 visar kravflödet från *Identifiera* till *Realisera*. Efter leverans är kravhanteringen beroende på förändringar i systemet med avseende på informationssäkerhet, där spårbarhet sker genom versionshantering av ISD-V.

Verksamhetens krav (säkerhetsmål) med avseende på informationssäkerhet från ITSS-I ligger till grund för tolkning av KSF och tillkommande krav i ITSS-D. För att få fram rätt kravnivå för upphandling sker iterativt arbete där funktionella krav bearbetas med IT-säkerhetsarkitekturen. Funktionella informationssäkerhetskrav dokumenteras inför upphandling/anskaffning i TS och icke funktionella krav i VÅS .

I ITSS-R fångas kravuppfyllnad från leverantören (från TS och VÅS) samt krav på miljön.



Figur 8 Kravflöde i ISD-Processen

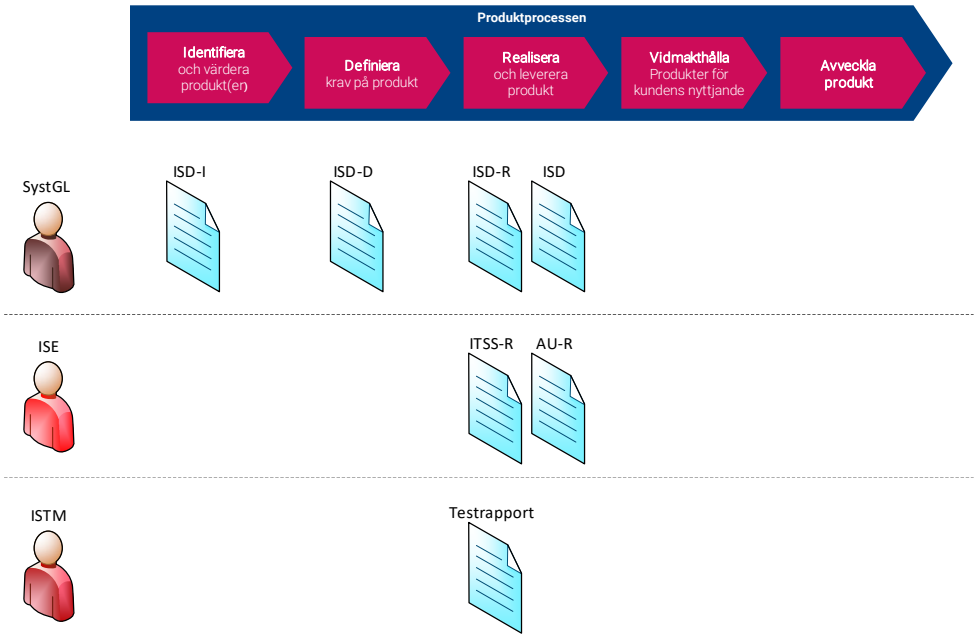
3.3 Oberoende granskning

ISD-processens definition av oberoende granskning är ”Med oberoende granskning avses granskning av ett objekt (som kan vara system eller specifik produkt/lösning) ur ett IT-säkerhetsperspektiv. Granskningen ska alltid ske av en instans med korrekt kompetens för uppgiften och som är oberoende, det vill säga utan tidigare åtagande eller ekonomiskt intresse avseende utvecklingen av granskningsobjektet.”.

Oberoende granskning genomförs av SystGL enligt Bilaga 3, och initieras av genomförande-projektet när ISD-processen är mogen för denna typ av granskning. Oberoende granskning på denna nivå är reglerad i FMV-beslutsmatris.

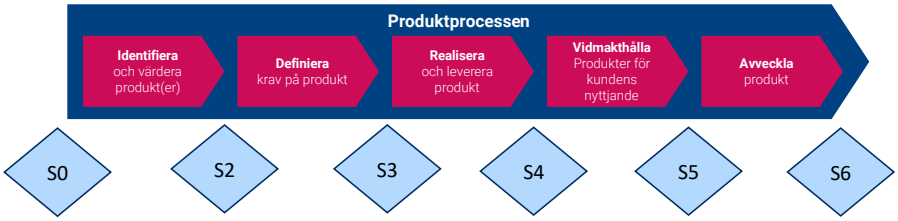
Genomförandeprojektet genomför också två interna granskningar:

- ISE genomför granskning av kravuppfyllnad, enligt Bilaga 2
- ISTE kan genomföra egna kompletterande tester, eventuellt baserade på leverantörens tester på levererat system.. Resultatet delges ISE inför granskning av kravuppfyllnad.



Figur 9 Granskning i olika nivåer

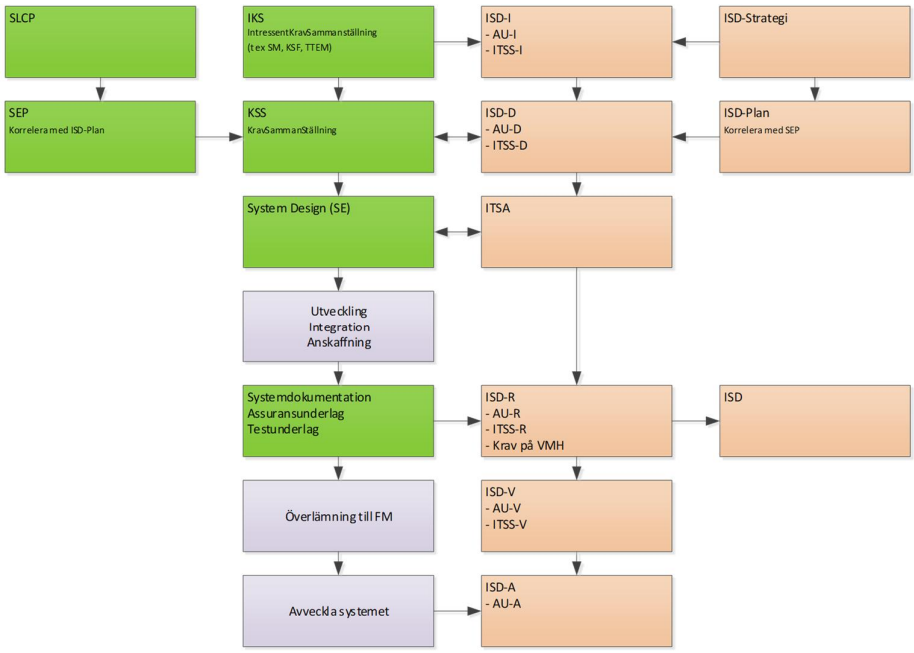
3.4 Angränsande processer



Figur 10 FMV VHL Produktprocess

3.4.2 Samverkan ISD och SE

Figur 11 Informationssäkerhetskrav i förhållande till kravområden i SE visar vilka delar i ISD-Processen som motsvarar samma arbete för andra kravområden i SE. De två kolumnerna till vänster visar SE-arbetet medan de två kolumnerna till höger motsvarar ISD-arbetet. Kravområdena måste samarbeta och synkroniseras för att systemet ska utvecklas i en helhet.

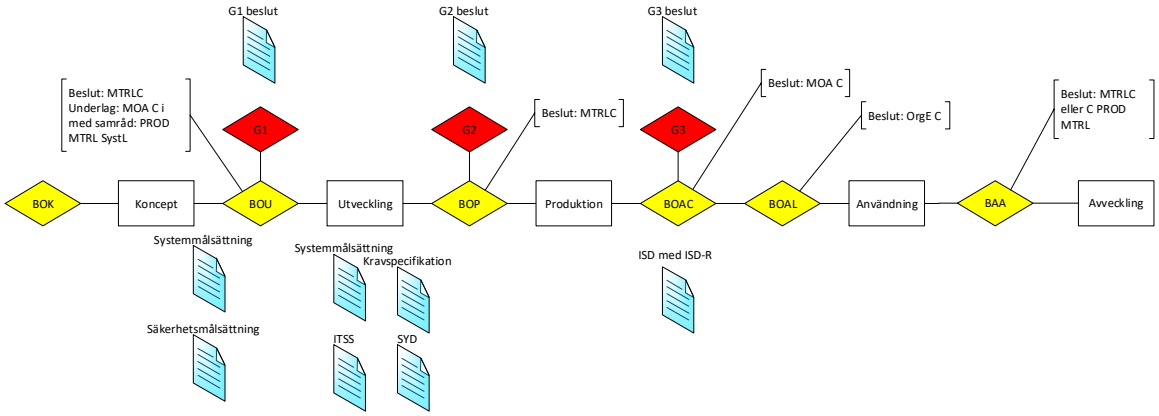


Figur 11 Informationssäkerhetskrav i förhållande till kravområden i SE

3.4.3 Samverkan ISD och FM BM TS

ISD-processen korrelerar med FM BM TS (FM beslutsmodell Tekniska System) såtillvida att FM ger indata till ISD-processen (främst Säkerhetsmålsättning inklusive ITSS)och i ISD-processen tas det fram ackrediteringsunderlag (ISD och ISD-R) inför FM beslut BOAC.

Följande figur illustrerar hur FM BM TS och FM IT-Process samverkar med ISD-processen.



ISD-processen förutsätter korrekt och aktuell indata i form av kravunderlag, såsom Systemmålsättning,, Säkerhetsmålsättning och ITSS. Resultatet från FMV ISD-process är leverans av ISD och ISD-R (med bilagor) till FM inför BOAC.

4 Roller

ISD-Processen tydliggör vilka roller som har ansvar för informationssäkerhetsarbetet i varje skede i produktprocessen. I och med tydliggörandet av roller, indikeras också vilken kompetens som krävs för att genomföra de aktiviteter som är knutna till respektive roll.

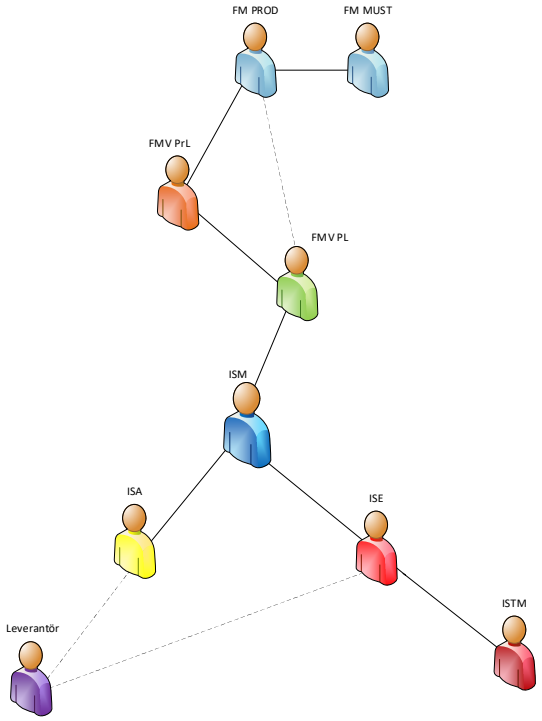
4.1 Roller i ISD-Processen

I genomförandeprojektet definieras följande projektinterna roller:

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

Rollerna, som inte nödvändigtvis behöver upprätthållas av olika personer, beskrivs i följande kapitel. Styrande vi rolltillsättning bör vara ackrediteringsobjektets komplexitet i förhållande till krav på kompetensnivå för respektive roll.

Följande figur illustrerar förhållande mellan rollerna inom ISD-processen.



Figur 12 Relation mellan rollerna i ISD-processen

Rollerna i ISD-processen, dvs ISM, ISA, ISE och ISTM, är informella roller inom genomförandeprojektet. Fördelningen av roller och ansvar görs i ISD-Planen. Det krävs normalt ingen formaliserad arbetsgång i arbetet som respektive roll genomför. Däremot ska de artefakter som respektive roll ansvarar för hanteras enligt FMV ordinarie regelverk.

4.1.1 ISM – Information Security Manager

ISM är ansvarig (delegerat ansvar från PL) för helhetsarbetet avseende informations- och IT-säkerhetsarbete samt ackrediteringen i genomförandeprojektet. Rollen bör vara medlem i projektledningen.

ISM arbetar huvudsakligen i faserna: *Definiera* och *Realisera*

I fasen *Definiera* har ISM följande uppgifter:

- Planer, koordinera och leda ISD-arbetet
- Klarlägg förutsättningar för att starta informationssäkerhetsarbetet i *Definiera*
- Producera ISD-Plan och koordinera denna med PL
- Komplettera, vid behov, identifierade kravkällor
- Leda riskarbetet
- Genomför, vid behov, kompletterande analyser
- Producera ISD-D, med bilagor
- Ta fram beslutsunderlag inför FMV VHL S3-beslut

I fasen *Realisera* har ISM följande uppgifter:

- Genomför, vid behov, kompletterande analyser
- Producera ISD-R, med bilagor, i samverkan med ISE
- Producera ISD (utkast)

4.1.2 ISA – Information Security Architect

ISA är ansvarig för krav- och designarbetet avseende IT-säkerhet och framtagning av ITSA.

ISA arbetar huvudsakligen i fasen *Definiera*, men kan även verka i *Realisera*.

I fasen *Definiera* har ISA följande uppgifter:

- Kravnedbrytning och –tolkning
- Genomför, vid behov, kompletterande analyser
- Planer, koordinera och leda arkitekturarbetet
- Skapa IT-säkerhetsarkitektur, med kravallokering
- Identifiera säkerhetskrav på omgivningen
- Samverka med Leverantör, PL och SE
- Ta fram informationssäkerhetskrav till TS och VÅS

I fasen *Realisera* bör ISA samverka med Leverantör avseende implementation av säkerhetsfunktioner.

4.1.3 ISE – Information Security Evaluator

ISE är ansvarig för aktiviteter kring granskning av kravuppfyllnad i *Realisera*. ISE har tillkommit i ISD-Processen för att genomföra evalueringsaktiviteterna i *Realisera*.

ISE arbetar huvudsakligen i fasen: *Realisera*

I fasen *Realisera* har ISE följande uppgifter:

- Granska underlag från Leverantör (-er)
- Verifiera rutiner/processer hos Leverantör (-er)
- Genomför, vid behov, besök hos leverantör
- Analysera kravuppfyllnad avseende funktionella säkerhetskrav
- Analysera kravuppfyllnad avseende icke-funktionella säkerhetskrav
- Initiera framtagning av ITSS-R
- Definiera krav för vidmakthållande
- Specificera, vid behov, krav på kompletterande säkerhetstester

Bilaga 2, ISE Granskningsinstruktion, bör användas som stöd för ISE granskningsaktiviteter.

4.1.4 ISTM – Information Security Test Manager

ISTM är ansvarig för planering, genomförande och dokumentation av kravställda säkerhetstester.

ISTM arbetar huvudsakligen i fasen: *Realisera*

I fasen *Realisera* har ISTM följande uppgifter:

- Koordinera testverksamhet
- Genomför säkerhetstester
- Analysera testresultat
- Ta fram testdokumentation
- Samverka, vid behov, med FMV T&E

4.2 FMV-roller med anknytning till ISD-Processen

4.2.1 FMV PrL – Produktledare

PrL är en formell roll på FMV som har lyfts upp speciellt i ISD-Processen 3.0 i och med aktiviteter i faserna *Identifiera* och *Vidmakthålla*. PrL har en viktig roll för att genomförandeprojektet ska få rätt förutsättningar för och inriktning av informationssäkerhetsarbetet.

PrL har inför TDir eller TC designansvaret för utpekat område med befogenheter enligt TDir eller TC beslut. I detta ingår att:

- utöva eget tekniskt designansvar inom tilldelat område samt stödja TDir, TC och/eller CI i dennes ansvarsutövning, bl.a. genom att fatta beslut i enlighet med Bilaga Besluts- och samrådsmatris
- stödja TDir, TC och/eller CI i beredningar och framtagning av underlag för beslut inom system och designledningen i enlighet med FMV VHL
- ansvara för utveckling, systemlivcykelplanering, kvalitetssäkring, konfigurationsledning samt

- status- och prestandauppföljning av de system som ingår i eget ansvarsområde
- ansvara för att ta fram förslag till åtgärder, samt för att initiera beslutad lösning, för att korrigera funktionella och säkerhetsmässiga oacceptabla tillstånd
- ansvara för att identifiera nödvändig Forskning och Utveckling, FoU

FMV PrL kan vid behov erhålla stöd från FMV ISD MetF, ISD KravF SystGL IT-Säk och/eller resurser med kompetens motsvarande ISD ISM.

4.2.2 FMV PL – Projektledare

PL ansvarar för genomförandeprojektet. Stöd till PL avseende informations- och IT-säkerhet erhålls av Information Security Manager (ISM), Information Security Architect (ISA), Information Security Evaluator (ISE) och Information Security Test Manager (ISTM).

4.2.3 FMV SystGL IT-Säk – Systemgranskningsledare

SystGL utses inom områden som kräver oberoende systemgranskning (OSG). SystGL som, fristående från produktionen, leder oberoende systemgranskare SystG. SystGL eller SystG granskar uppdrag de själva inte är aktivt involverade i. SystGL och SystG har inget ansvar mot det uppdrag han eller hon granskar och kan därmed inte fatta några beslut om hur uppdraget ska hanteras eller styras.
SystGL eller SystG har bland annat följande uppgifter:

- Svara inför TDir/TC för att den oberoende systemgranskningen säkerställer att de granskade objekten uppfyller gällande kvalitetskrav, alternativt att eventuella brister klarläggs.
- Föreslår TDir/TC tillämpningsanvisningar (motsv.) för gällande regelverk
- Föreslår TDir/TC att godkänna SystG efter att ha värderat deras kompetens
- Delta i utveckling av processer inom sitt verksamhetsområde samt utbilda personal.

SystGL har arbetsuppgifter i samtliga faser; *Identifiera*, *Definiera*, *Realisera*, *Vidmakthålla* och *Avveckla*.

Inom ramen för ISD-processen 3.0 är SystGL primära uppgifter granskning och samråd.

4.2.4 FMV SystG IT-Säk – Systemgranskare IT-Säk

SystG genomför OSG på mandat av SystGL. SystG granskar uppdrag de själva inte är aktivt involverade i. SystGL och SystG har inget ansvar mot det uppdrag han eller hon granskar och kan därmed inte fatta några beslut om hur uppdraget ska hanteras eller styras.

4.3 Övriga roller

4.3.1 FM MUST

FM MUST har en rådgivande och granskande roll i ISD-Process 3.0. Om det är bedöms nödvändigt, t ex på grund av ackrediteringsobjektets komplexitet eller kontext bör det om möjligt skapas en samverkansgrupp mellan genomförandeprojektet (främst PL, ISM och ISA) och FM MUST.

4.3.2 FM PROD

FM PROD är dels kravställare i fasen *Identifiera* och dels mottagare av ISD och ISD-R (med bilagor) i fasen *Realisera*.

FM PROD utgör också länk mellan genomförandeprojektet (FMV PL) och FM MUST i de fall bedömningar av t ex tekniska lösningar eller arkitektur behöver göras.

4.3.3 Leverantör

Leverantör av systemet skall utse en PoC, point-of-contact, för informationssäkerhetsrelaterade frågor.

Beroende på omfattningen av genomförandeprojektet bör Leverantör också utse följande roller:

- Arkitekt
- Testledare

I de fall FMV är integratör gäller motsvarande krav, tex avseende assurans och tester.

4.4 Sammanfattning roller

Följande tabell visar ansvarsfördelningen mellan roller och artefakter.

Roll/Aktivitet	Producera	Granska	Samråd	Godkänna
PrL	ISD-Strategi ISD-I AU-I ITSS-I ISD-A AU-A			ISD-Strategi ISD-I AU-I ITSS-I ISD-Plan ISD
SystGL			ISD-Strategi ISD-I AU-I ITSS-I ISD-Plan ISD-D AU-D ITSS-D ITSA ISD-R AU-R ITSS-R VMH-R	
PL	ISD	ISD-Plan ISD-D AU-D ITSS-D ITSA ITSS-R ISD-R AU-R ITSS-R VMH-R		ISD-D AU-D ITSS-D ITSA ISD-R AU-R ITSS-R VMH-R

Roll/Aktivitet	Producera	Granska	Samråd	Godkänna
ISM	ISD-Plan ISD-D AU-D ISD-R AU-R ISD (utkast)			
ISA	ITSS-D ITSA Krav till TS Krav till VÅS			
ISE	ITSS-R Testplan (utkast) VMH-R	Systemdok. Assuransdok. Testrapport		
ISTM	Testplan Testspecifikation Testrapport			
FM MUST			ITSA ITSS-R ISD ISD-V	
FM PROD	ISD-V			
FMV TC				ISD

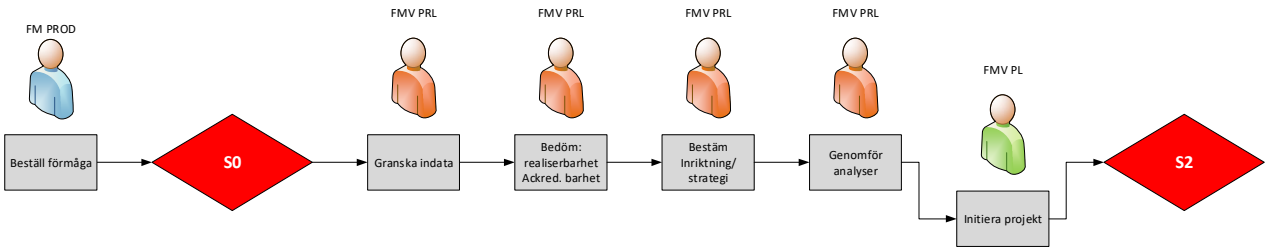
Tabell 3 – Sammanfattning roller

5 Fördjupad processbeskrivning

ISD-Processen är aktivitetsbaserat vilket innebär att för varje skede i produktprocessen beskrivs de aktiviteter som bör göras i informationssäkerhetsarbetet samt vilka roller som bör genomföra aktiviteterna. Rollerna är angivna som en indikation på var ansvaret för aktiviteterna bör finnas samt vilken kompetens som behövs för att genomföra aktiviteterna.

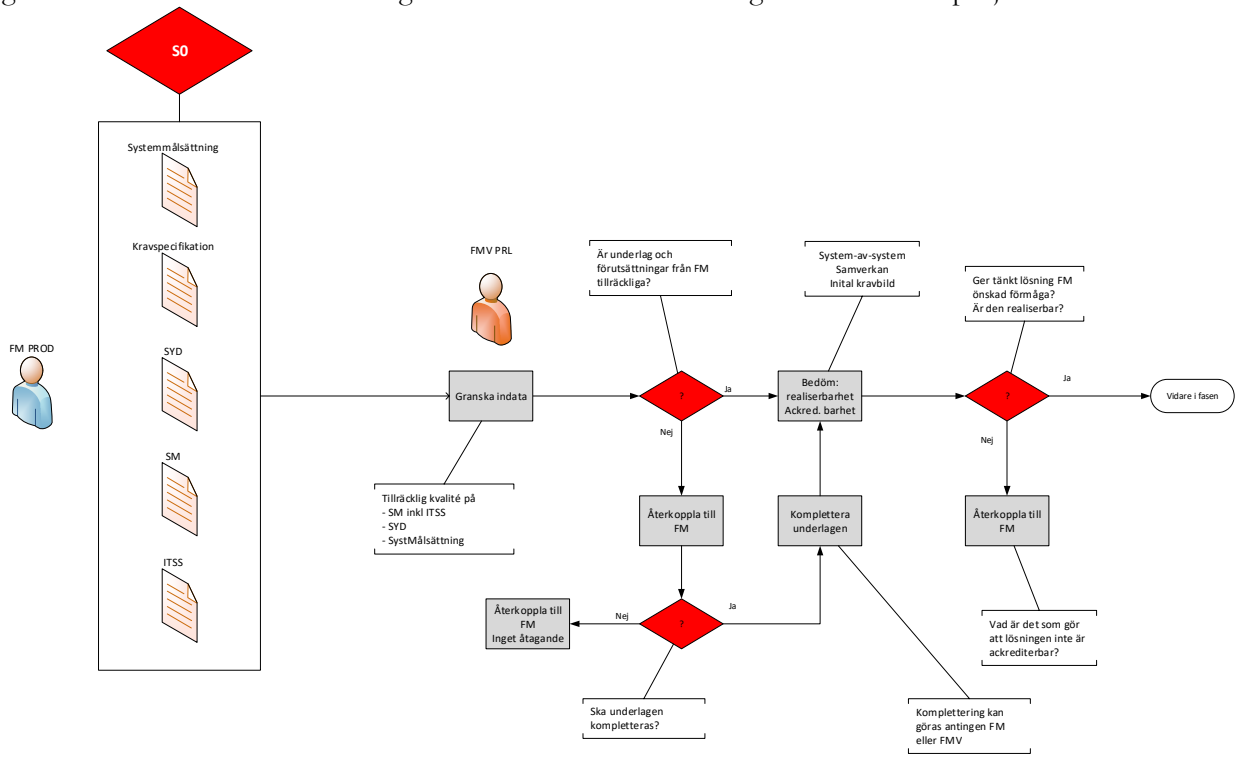
5.1 Identifiera

I *Identifiera* genomför PrL aktiviteter, se Figur 13 Huvudaktiviteter i Identifiera inför FMV VHL S2-beslut, som ska resultera i att förutsättning och inriktning kan ges till genomförandeprojektet. Genom den första realiserbarhetsbedömningen säkerställs att inga genomförandeprojekt startar utan att rätt förutsättningar finns. Samverkan i gränsytorna mellan FM och FMV PrL samt mellan PrL och PL är viktiga för det fortsatta arbetet för att säkerställa att samtliga parter har förstått varandras behov.
I *Identifiera* görs även en första bedömning av vilka delar av ISD-Processen som behöver användas och det dokumenteras i tekniskt projektdirektiv.



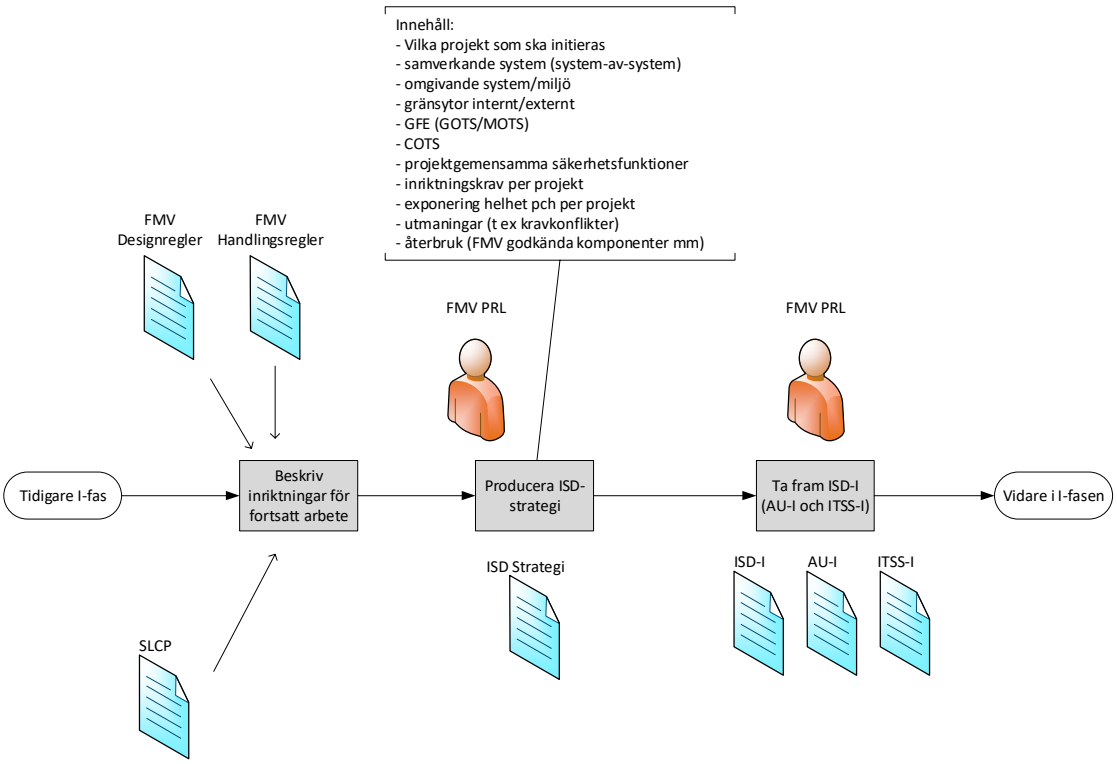
Figur 13 Huvudaktiviteter i Identifiera inför FMV VHL S2-beslut

Aktiviteten analys av indata från FM kan resultera i att informationen/underlagen från FM inte innehåller den information som krävs för att kunna ta fram ett realiserbart IT-system. Figur 14 Identifiera - Iterativt arbete mellan FM och FMV visar iterativt arbete mellan FM och FMV för att uppnå gemensam förståelse för verksamhetens behov. När komplettering av FM är genomförd gör FMV PrL en första bedömning av realiserbarhet och vid ett godkännande tas projektet vidare.



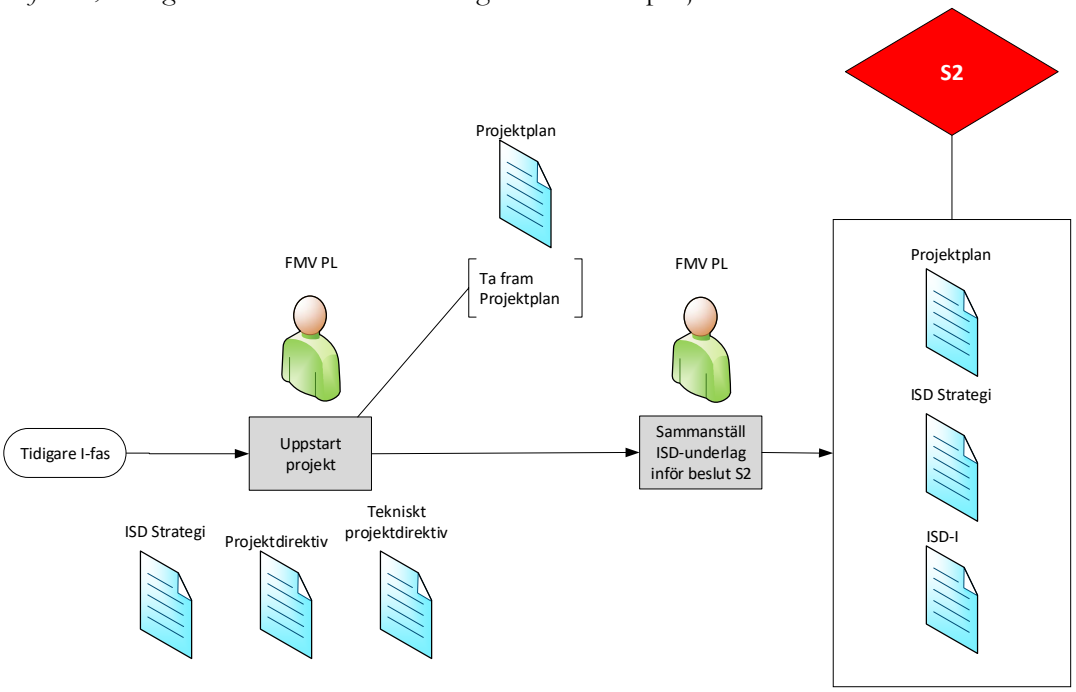
Figur 14 Identifiera - Iterativt arbete mellan FM och FMV

Innan genomförandeprojektet initieras, genomförs aktiviteter för att ta fram strategi i form av möjliga återbruk av komponenter, system av system, relationer till andra projekt, bruk av specifika FMV Design- och handlingsregler mm. ISD-strategi och analyserna ger underlag till deklaration av realiserbarhet från *Identifiera,* se Figur 15 Identifiera - Aktiviteter för framtagning av ISD-strategi och ISD-I.



Figur 15 Identifiera - Aktiviteter för framtagning av ISD-strategi och ISD-I

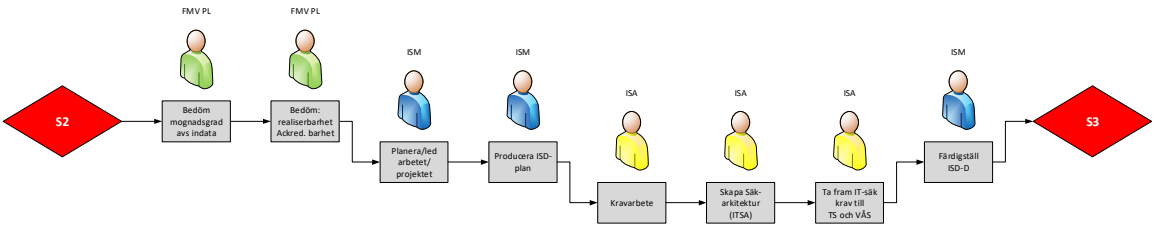
Med PrL ISD-strategi och deklaration av realiserbarhet har PL bra förutsättningar för att starta genomförandeprojekt. PrL sammanställer underlag inför S2-beslut och PL startar arbetet i *Definiera,* se *Figur 16* Identifiera - Initiera genomförandeprojekt.



Figur 16 Identifiera - Initiera genomförandeprojekt

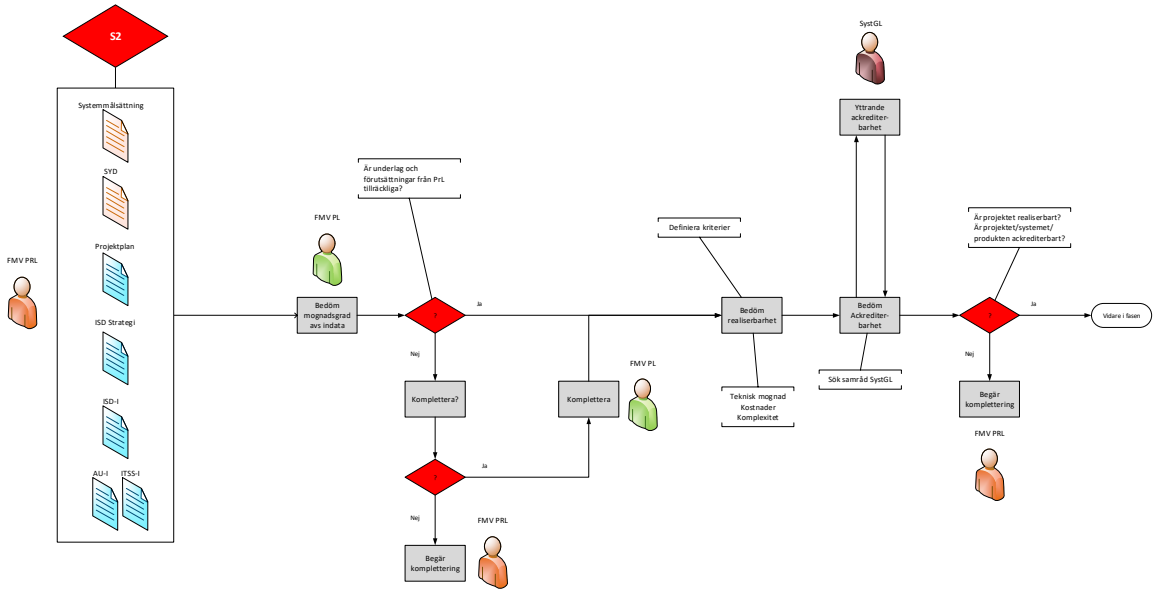
5.2 Definiera

Definiera är första skedet i genomförandeprojektet där planering av IT-säkerhetsarbetet, aktiviteter för kravarbete inklusive IT-säkerhetsarkitektur samt framtagning av upphandlingsunderlag är huvudaktiviteterna, se Figur 17 Definiera – Huvudaktiviteter i Definiera inför FMV VHL S3-beslut. Aktiviteterna resulterar i att PL deklarerar realiserbarhet inför FMV VHL S3-beslut för upphandling. I detta skede kan PL ta stöd av rollerna ISM och ISA med specifik kompetens inom informationssäkerhetsområdet, se avsnitt 4Roller.



Figur 17 Definiera – Huvudaktiviteter i Definiera inför FMV VHL S3-beslut

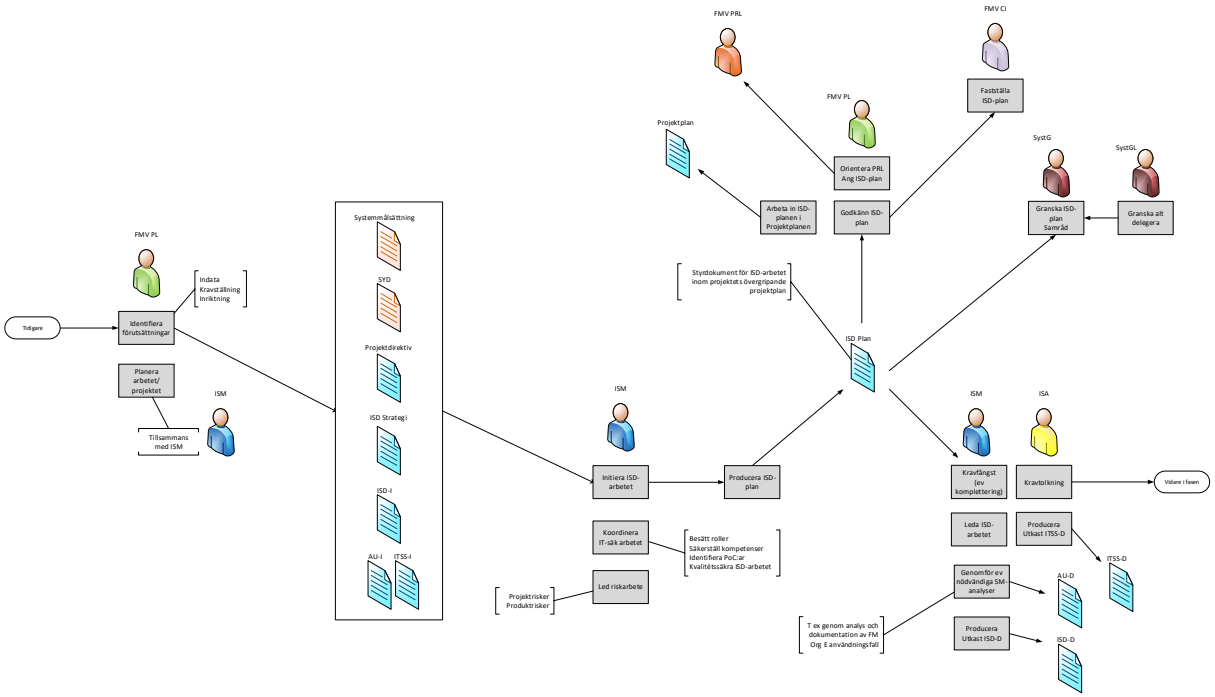
Förutsättningarna för att kunna göra bedömningar av realiserbarhet och ge förutsättningar till upphandling och realisering är att ett förberedande arbete har genomförts i *Identifiera*. Det är viktigt att PL gör en bedömning av mognadsgraden av indatat från PrL och begär komplettering i de fall det bedöms att informationen inte är tillräcklig, se Figur 18 Definiera - Iterativt arbete mellan FMV PrL och PL.



Figur 18 Definiera - Iterativt arbete mellan FMV PrL och PL

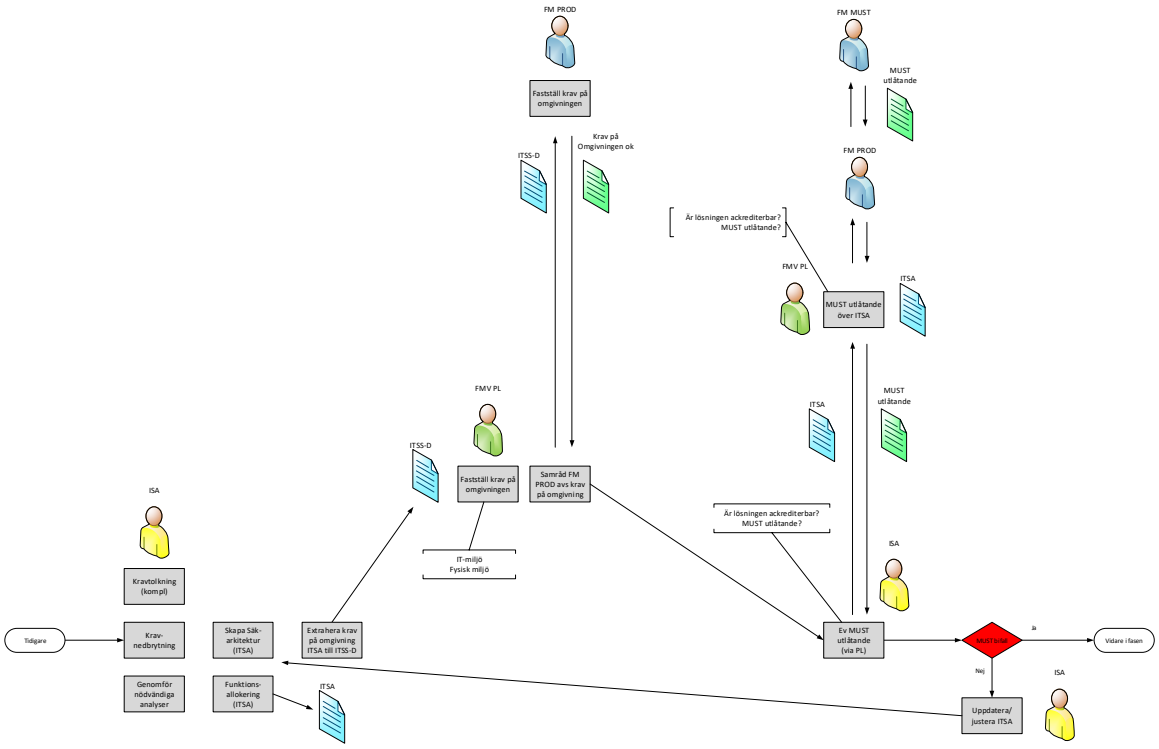
PL planerar arbetet/projektet och tar tillsammans med ISM fram en ISD-plan.
ISD-planen granskas av SystGL och samråd sker med PrL.

Aktiviteter som kravfångst och eventuellt ett kompletterande av analyser från *Identifiera* sker av ISM. Detta använder ISA till att genomföra kravtolkning och framtagning av ITSA.
ISM tar sen tillsammans med ISA fram deklaration för realiserbarhetsbedömning samt upphandlingsunderlag i form av VÅS och TS.



Figur 19 Definiera - Aktiviteter för första iteration kravarbete

Aktiviteter som kravtolkning (komplettering), kravnedbrytning och framtagning av ITSA kräver kompetens enligt ISA. IT-säkerhetskraven från kravnedbrytningen fördelas på IT-säkerhetsarkitekturen. Detta arbete sker iterativt och kan ske i dialog med PrL och FM för att tillsammans komma fram till beslut som kan minska exponering och därmed minska kravnivån. Indatat dvs. underlaget från *Identifiera* kan då komma att behöva förändras.

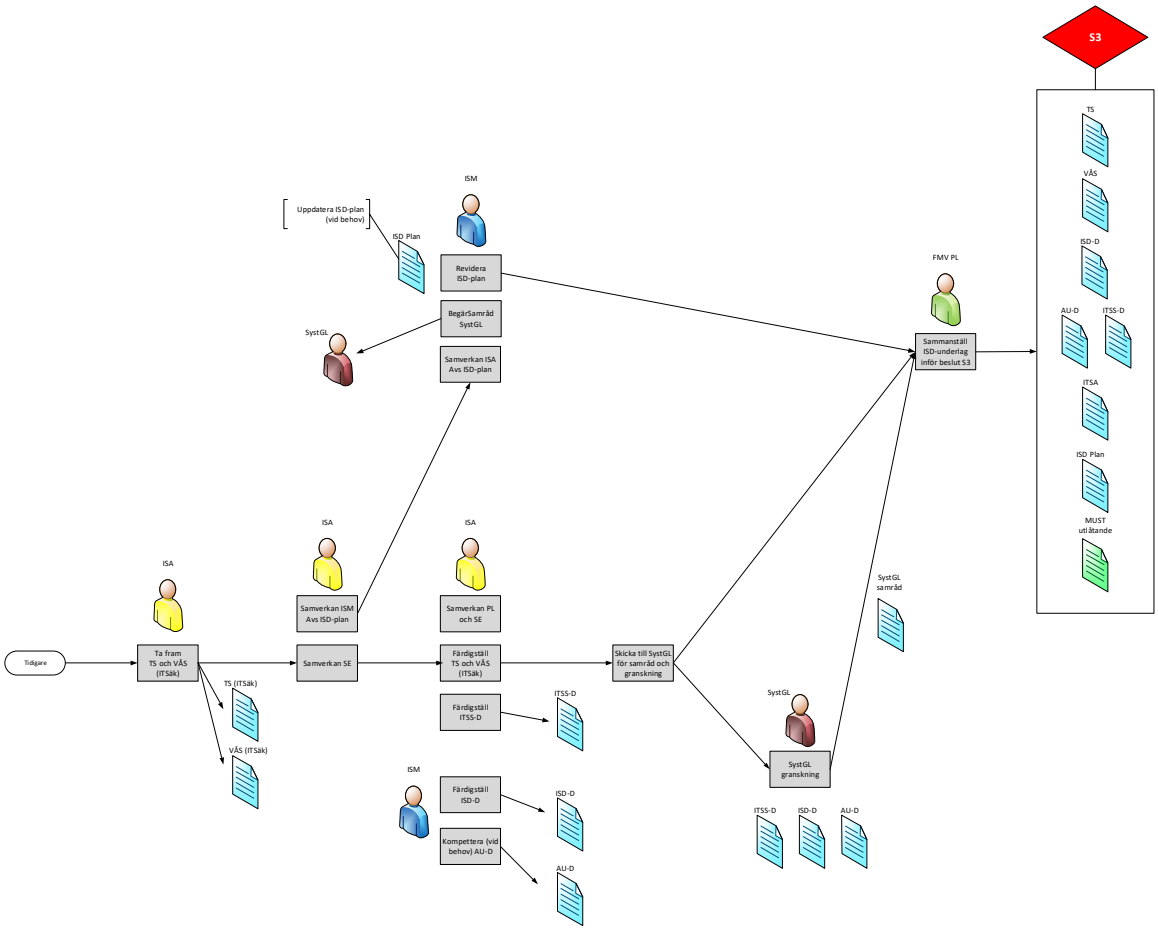


Figur 20 Definiera - Andra iteration kravarbete och samråd MUST

Aktiviteter fortsätter för att genomföra realiserbarhetsbedömning samt ta fram upphandlingsunderlag, Tekniska Specifikation (TS) och VerksamhetsÅtagandeSpecifikation (VÅS).

Arbetet med TS och VÅS sker i samverkan med SE för att säkerställa realiserbarhet med övriga systemområden. I slutskedet av arbetet initieras oberoende granskning av SystGL samt samråd med FM MUST.

Därefter sammanställs deklaration av realiserbarhet och upphandlingsunderlag inför FMV VHL S3-beslut.

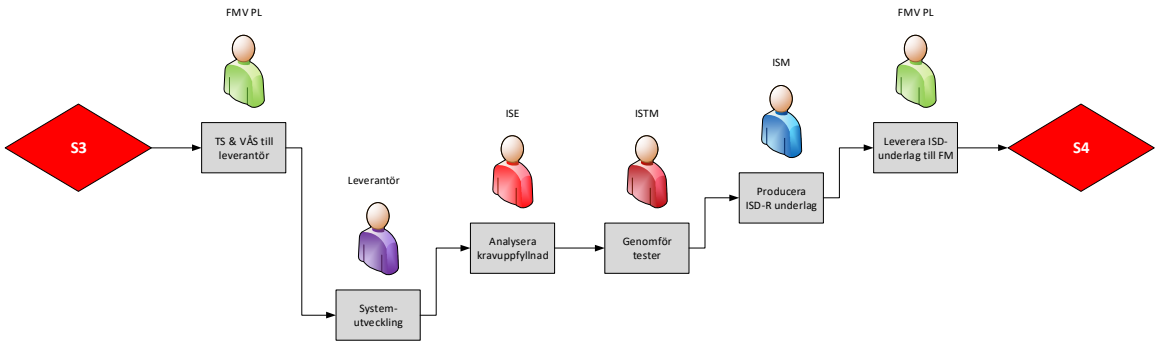


Figur 21 Definiera - Aktiviteter för samverkan med SE och SystGL i framtagning av underlag inför FMV VHL S3 beslut

5.3 Realisera

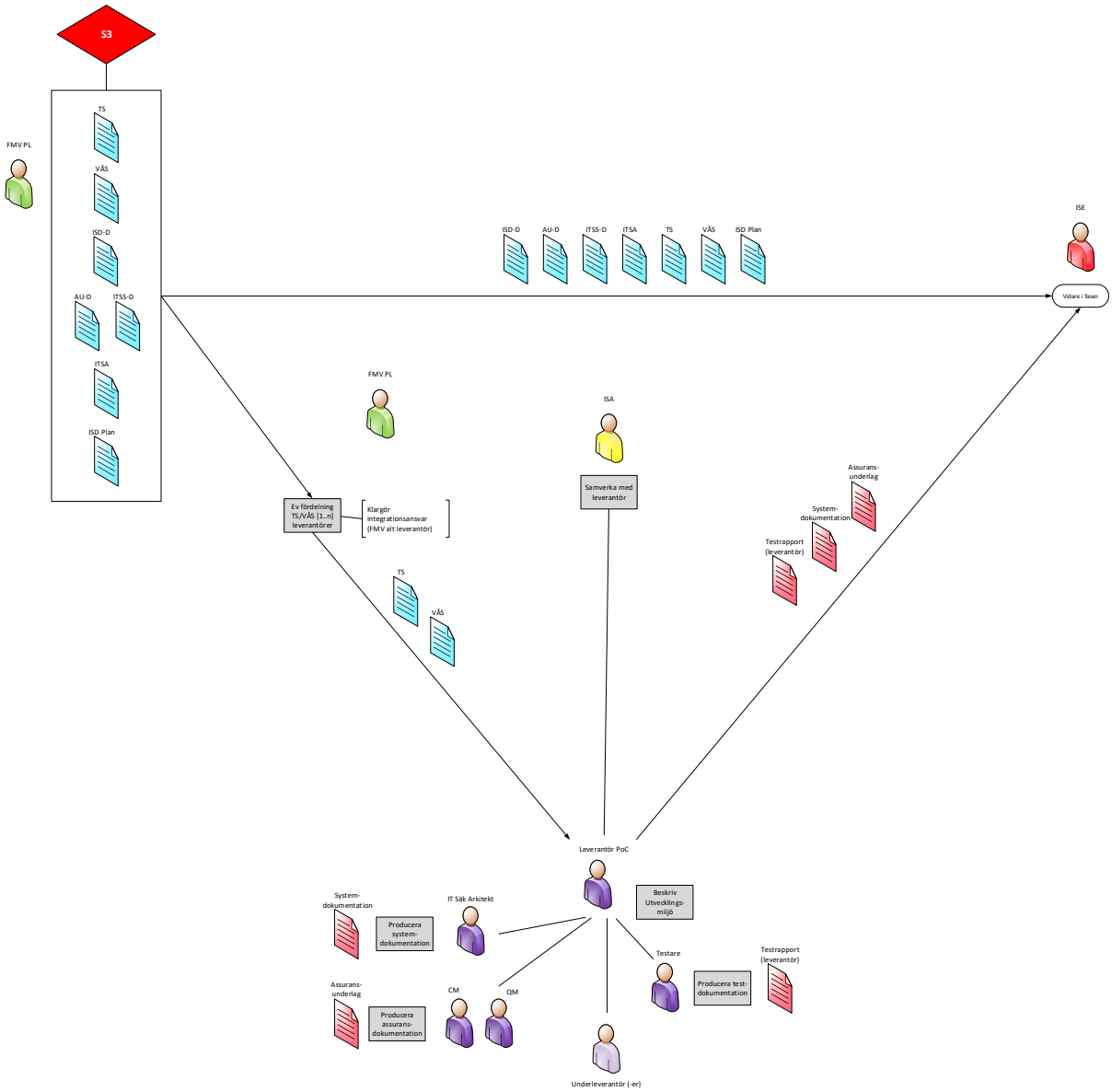
I *Realisera* sker aktiviteter för utveckling av det aktuella systemet, kravuppfyllnad samt leverans till FM. Flera leverantörer kan utveckla system som ska ingå i det totala systemet till FM. Efter utveckling av systemet analyseras kravuppfyllnaden av Information Security Evaluator (ISE) baserat på underlag från leverantören. Tester genomförs av Information Security Test Manager (ISTM) och avvikelser och kvarvarande risker identifieras. PL genomför tillsammans med ISM aktiviteter för framtagning av underlag till deklaration av ackrediterbarhet, ISD-R. Efter detta sker leverans till FM, se Figur 22 Realisera - Huvudaktiviteter inför FMV VHL S4-beslut.

FMV PL är ansvarig för aktiviteterna i *Realisera* med stöd från rollerna; ISM (Information Security Manager), ISE (Information Security Evaluator), ISTM (Information Security Test Manager) där ISE genomför huvuddelen av arbetet.



Figur 22 Realisera - Huvudaktiviteter inför FMV VHL S4-beslut

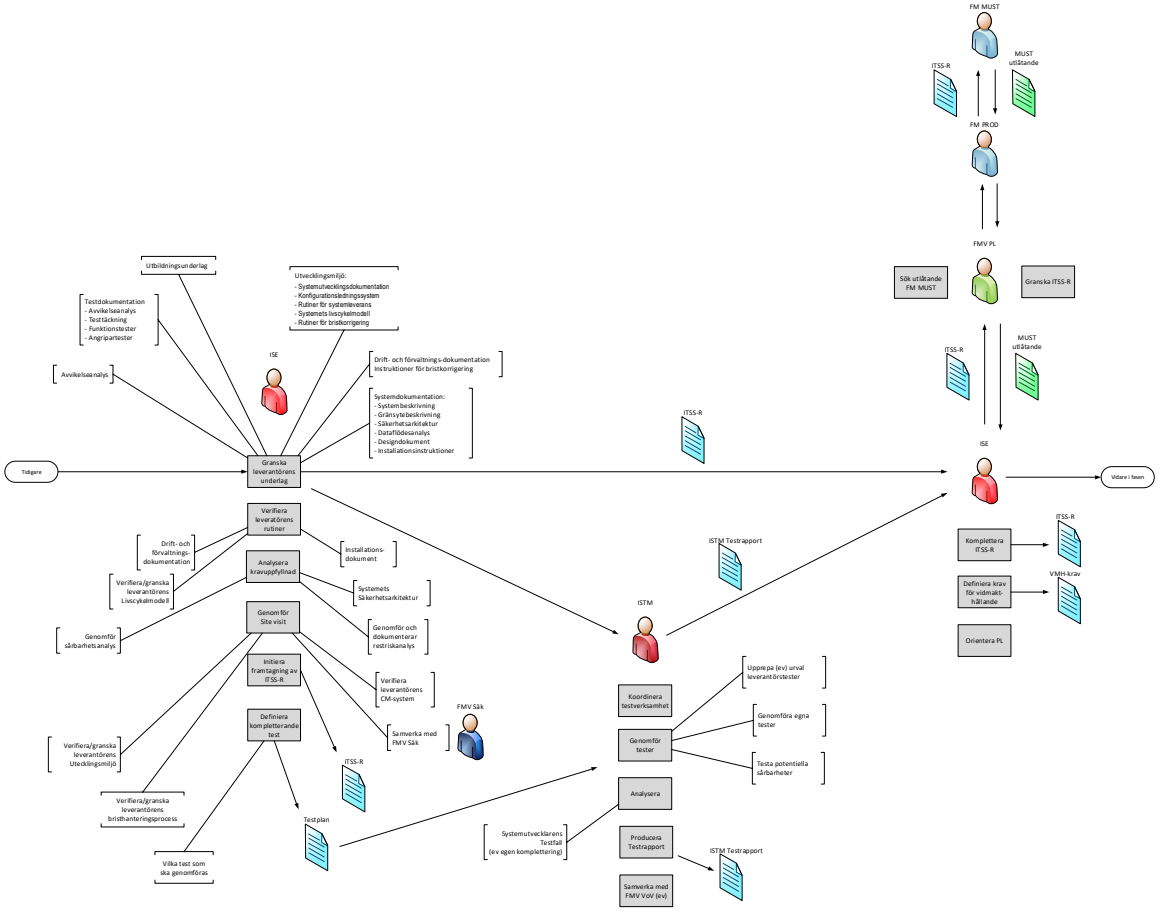
Efter upphandling startar leverantören arbetet kring utvecklingen av det aktuella systemet, se Figur 23 Realisera - Leverantörens IT-säkerhetsarbete och leverans. Vid utveckling av flera system från flera leverantörer sker integrering av det totala systemet av FMV, alternativt av en upphandlad integratör. Det är av stor vikt att det finns en utpekad kontaktperson hos leverantören som specifikt hanterar IT-säkerhetsområdet och som samverkar med ISA för att det skall bli ett ackrediterbart system. Leveransen från leverantören sker till FMV där ISE tar hand om det för att använda det i granskningen av kravuppfyllnad.



Figur 23 Realisera - Leverantörens IT-säkerhetsarbete och leverans

Huvuduppgiften för ISE är att granska leverantörens underlag såsom utvecklingsmiljöer, rutiner och dokumentation m.m. och använda det i bedömning av kravuppfyllnad, ITSS-R. När det gäller krav på utvecklingsmiljö har Leverantören avtal med FMV där FMV Säk har ett ansvar. Granskning av dessa miljöer görs generellt inte av genomförandeprojektet utan av FMV Säk. Genomförandeprojektet skall lyfta behov till FMV Säk.

I arbetet med kravuppfyllnad kan det bedömas behov av att genomföra praktiska säkerhetstester av speciellt kritiska säkerhetsfunktioner. Dessa tester genomförs och/eller koordineras av ISTM. En riskanalys ska även göras med avseende på kravuppfyllnaden och dess resultat för att beskriva eventuella kvarvarande brister och dess konsekvenser, se Figur 24 Realisera - ISE granskningsarbete inför realiserbarhetsbedömning.

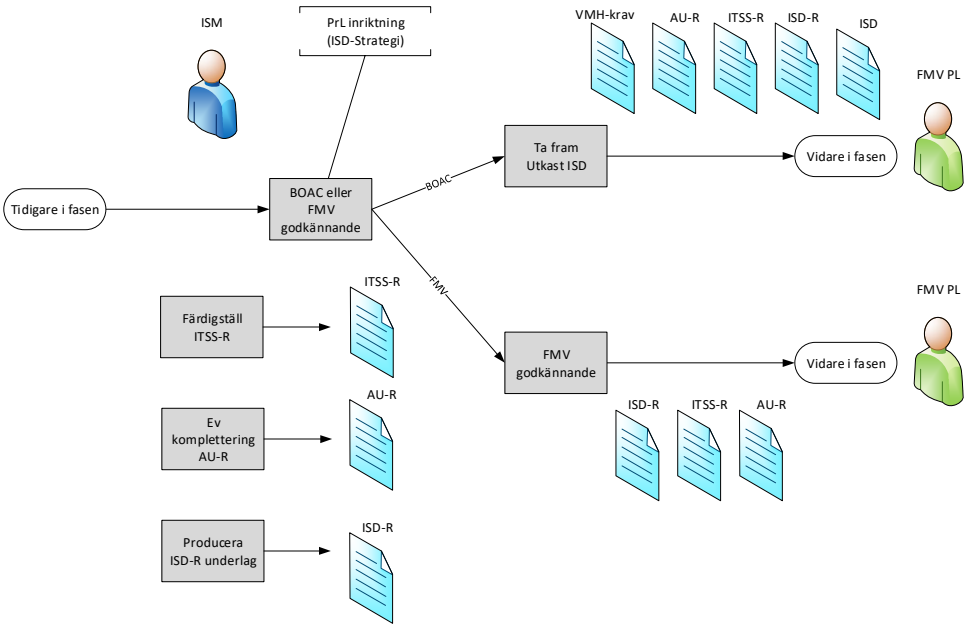


Figur 24 Realisera - ISE granskningsarbete inför realiserbarhetsbedömning samt samråd med FM MUST

SystGL genomför en oberoende granskning och det resultat ligger till grund för fastställande av ITSS-R och informationssäkerhetsdeklarationen (ISD). Den oberoende granskningen kan genomföras dels som dokumentgranskning men även som praktiska säkerhetstester av speciellt kritiska säkerhetsfunktioner. FM MUST kan lämna ett utlåtande baserat på det material som tidigare granskat av SystGL, se Figur 24 Realisera - ISE granskningsarbete inför realiserbarhetsbedömning samt samråd med FM MUST. Delprocessen för hur detta utlåtande ska gå till ska hanteras i införandet av ISD-Processen.

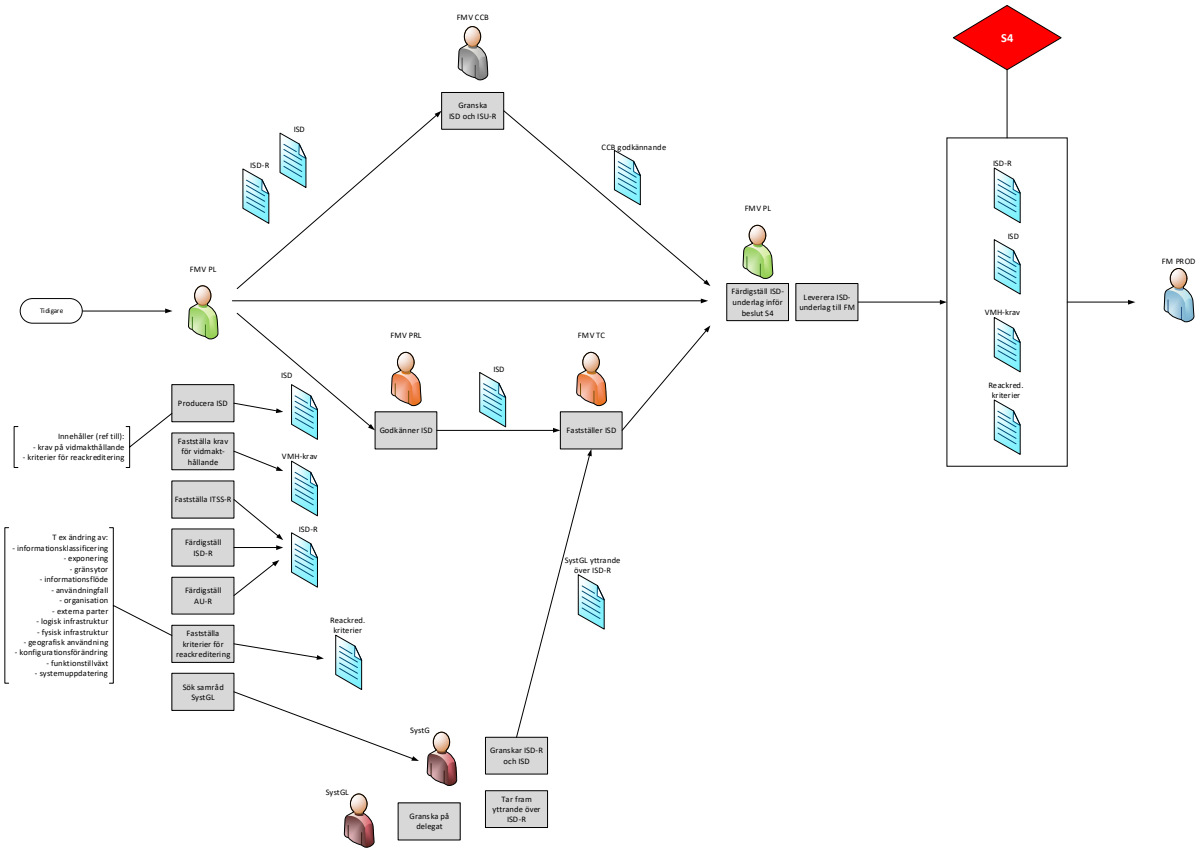
PrL har genom ISD-Strategin möjlighet att ta fram komponentgodkännande för relevanta systemkomponenter (i figuren nedan benämnt ”FMV godkännande”). Syftet med detta är att möjliggöra återbruk av granskade systemkomponenter för användning i system-av-system.

Det är fullt möjligt att system som är avsedda för överlämning till FM PROD också kan få ett komponentgodkännande av FMV. Det är dock viktigt att systemkontexten och –kraven är klarlagda och tydliga, så att komponenten går att återbruka i ett annat sammanhang.



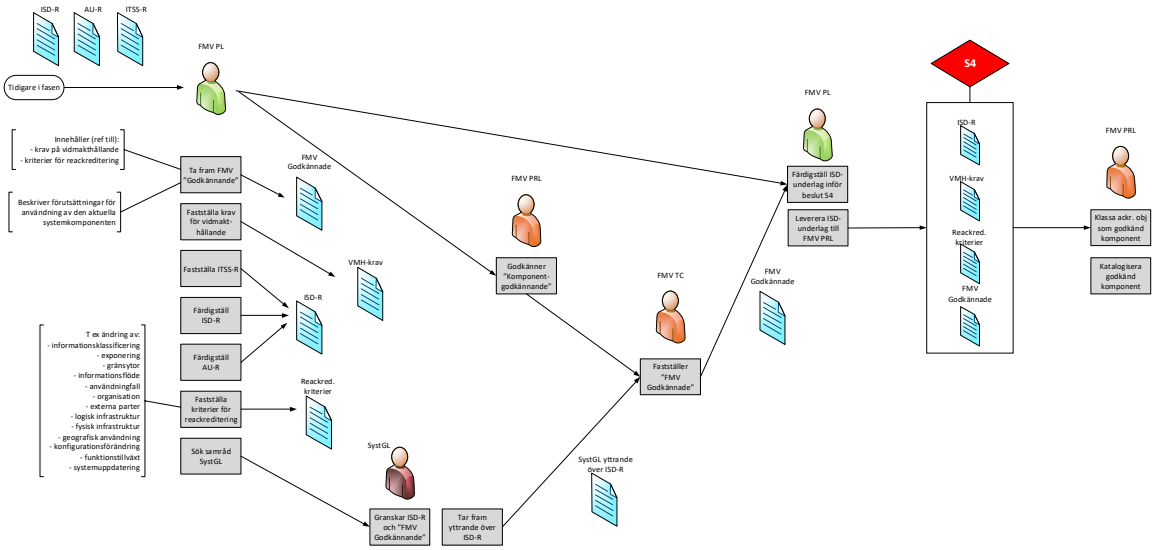
Figur 25 Realisera – BOAC eller FMV godkännande

Följande figur illustrerar PL slutaktiviteter då ett system ska överlämnas till FM för BOAC.



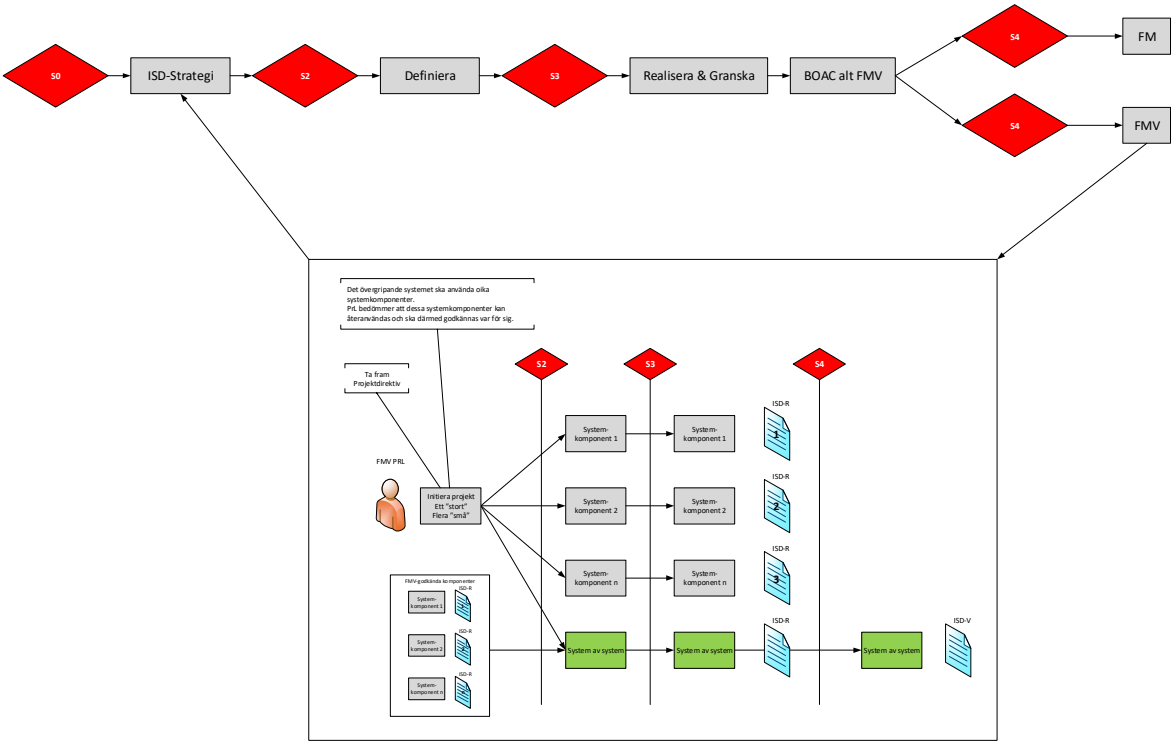
Figur 26 FMV Slutaktiviteter för överlämning till FM inför BOAC

Följande figur illustrerar PL slutaktiviteter då ett system ska överlämnas till FM för BOAC.



Figur 27 FMV Slutaktiviteter inför Komponentgodkännande

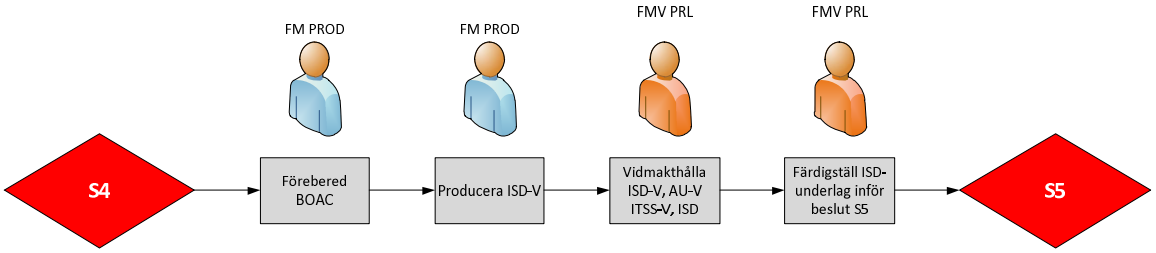
Principerna bakom godkännandeprocessen (återbruk) illustreras i följande figur.



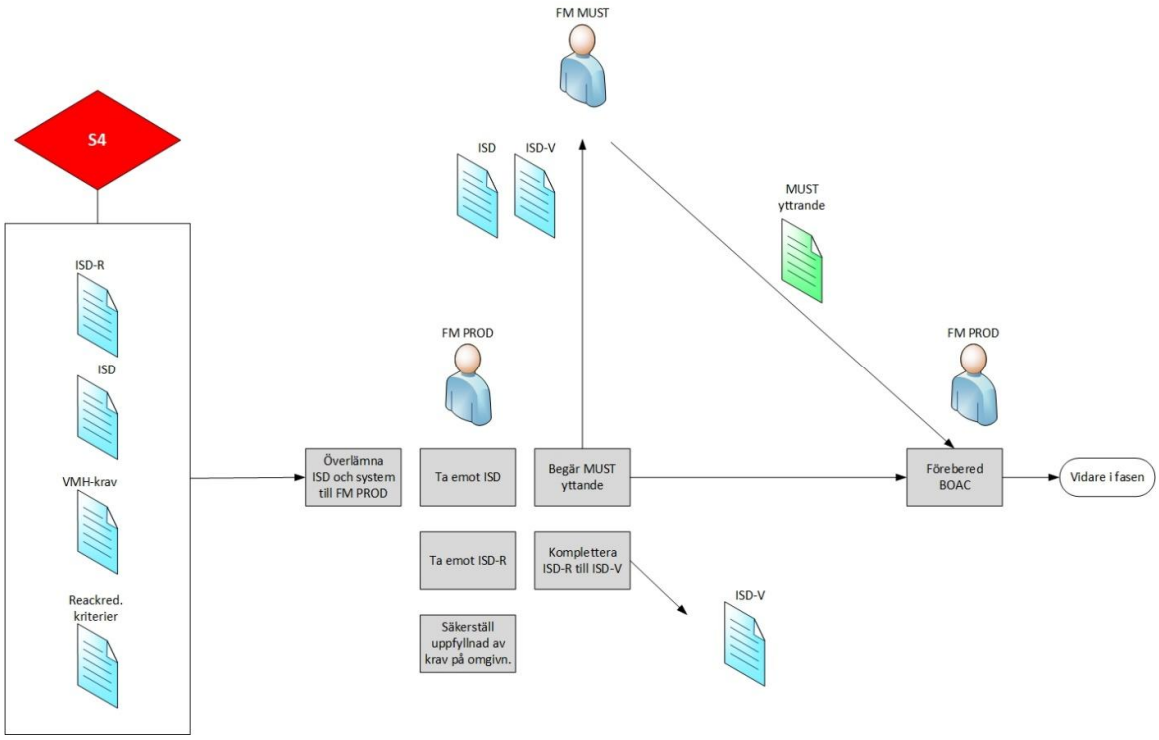
Figur 28 FMV Slutaktiviteter inför Komponentgodkännande

5.4 Vidmakthålla

Vidmakthåll startar när FMV har överlämnat systemet med tillhörande ackrediteringsunderlag ISD och ISD-R till FM, se Figur 29 Huvudaktiviteter i Vidmakthålla och Figur 30 FMV överlämning till FMFM ansvarar för att förbereda och ta fram ett BOA för systemet. Det finns ett behov av att förvalta ackrediteringsunderlaget för systemet, och det underlaget benämns ISD-V i ISD-Processen. Hur denna förvaltning exakt ska gå till och hur FMV kan få information om systemets förändringar och vidareutveckling behöver diskuteras och förankras hos FM PROD vid införandet av ISD-Processen.



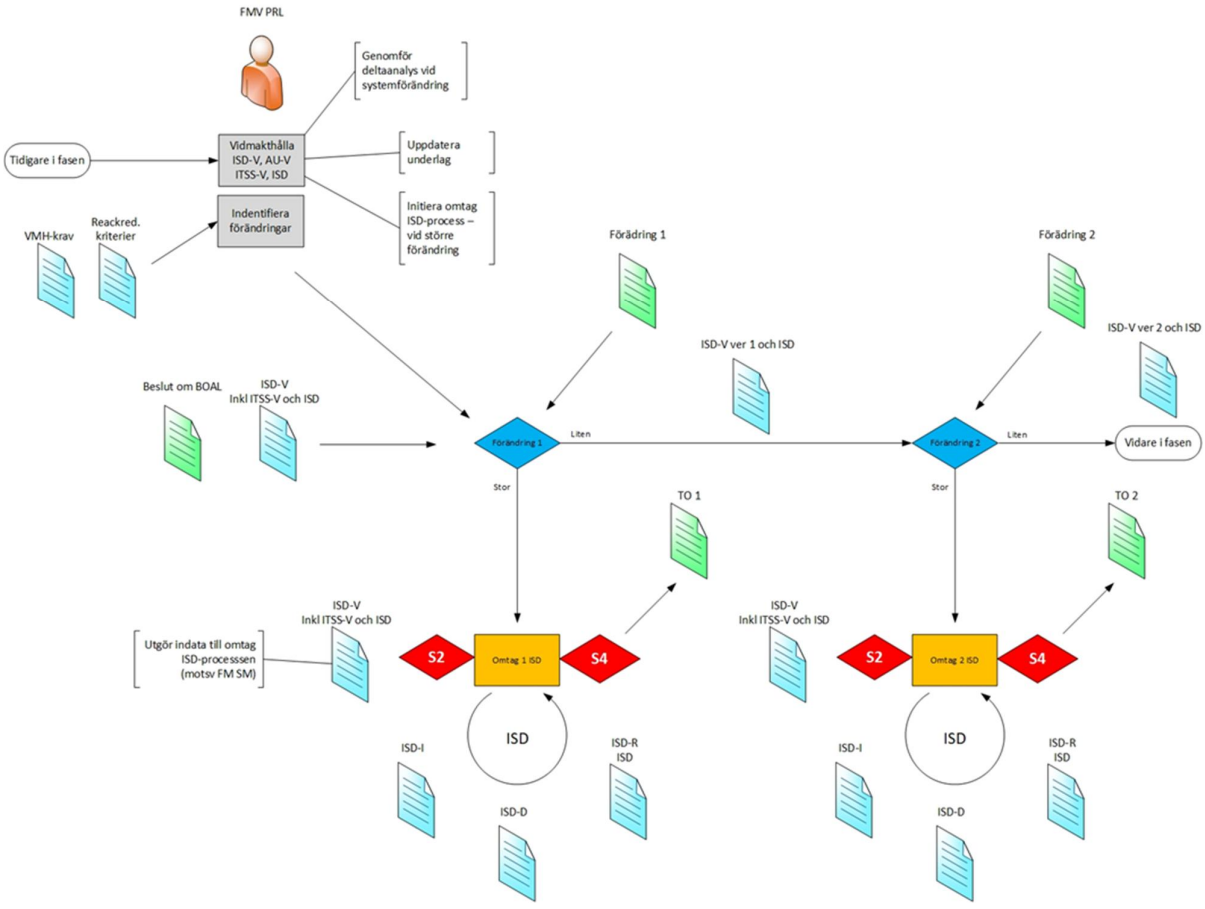
Figur 29 Huvudaktiviteter i Vidmakthålla



Figur 30 FMV överlämning till FM

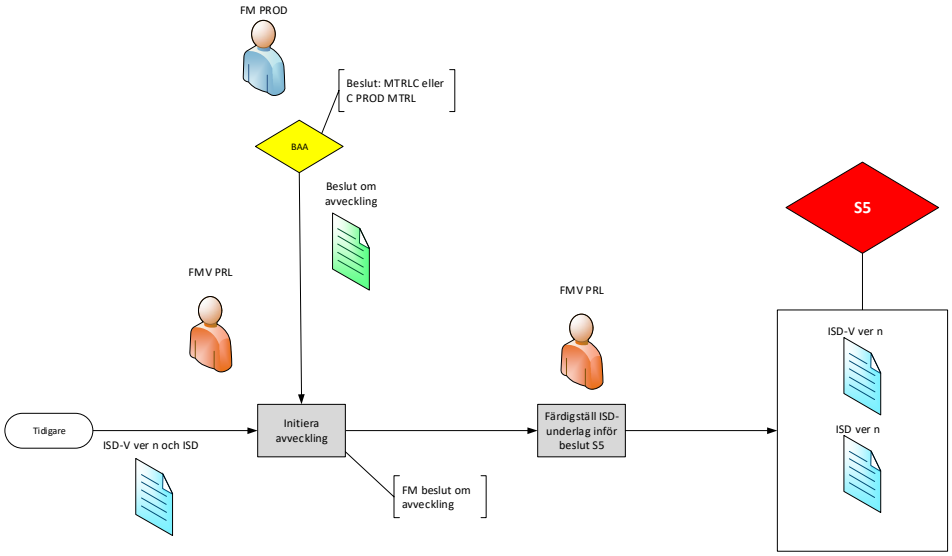
Systemet har behov av aktiv systemförvaltning för att kunna möta kontinuerliga förändringar. Ur ett informationssäkerhetsperspektiv görs deltaanalys med avseende på förändringen för att avgöra om och hur förändringen påverkar den ackreditering. Visar deltaanalysen att ändringen är omfattande och har stor påverkan på säkerhetslösningen genomförs omackreditering och IT-säkerhetsarbetet fortsätter med hela processen från *Identifiera* o.s.v.

Deltaanalysen kan också resultera i en tilläggsackreditering, där skillnaden mellan det som levererades i ISD-R och den tillkomna förändringen tas med i ackrediteringsarbetet. ISD-R och ITSS-R uppdateras och levereras till FM. FM uppdaterar i sin tur ISD-V och ITSS-V med nytt versionsnummer för det aktuella systemet. Liten förändring resulterar i en Teknik Order, ISD-V uppdateras med nytt versionsnummer.



Figur 31 Vidmakthålla - Processen vid omackreditering

Systemet vidmakthålls fram till FM beslut om avveckling (BAA) varvid PrL färdigställer ISD-R inför beslutspunkt S5 enligt FMV VHL.



Figur 32 Vidmakthålla - Processen vid beslut om avveckling