ISD och SE

2016-06-30

Revisionshistorik

Version	Datum	Beskrivning	Ansvar
2.3	2016-06-30	Mindre uppdateringar med avseende på begrepp och förtydliganden baserat på erfarenhetsåterkoppling. Version 2.2 är bokformatet.	DAOLO
2.1	2014-05-26	Mindre uppdateringar med avseende på begrepp och förtydliganden	DAOLO
2.0	2013-10-25	Uppdatering efter remissynpunkter	DAOLO
1.3	2013-05-29		DAOLO
1.2	2013-05-22	Uppdatering efter granskning	DAOLO
1.1	2013-05-21	Uppdatering av AKLed vägledning för utveckling av säkra system till FMV Vägledning	DAOLO

Innehåll

1 Inledning

Denna vägledning är utformad för att tillgodose FMV behov av att på ett strukturerat sätt kvalitetssäkra leveranser av säkra och godkända IT-system till Försvarsmakten. Vägledningen är harmoniserad med Försvarsmaktens processer såsom KSF och IT-processen. Den är generaliserad för att kunna fungera som bas för IT-säkerhetsarbetet under en lång tid framöver. Vägledningen kan med fördel användas inom ramen för projektets arbete med IT-säkerhet samt vid oberoende granskning.

Vägledningen ska etablera och vidmakthålla förtroende för FMV utformning och implementering av funktioner som direkt eller indirekt bidrar till att FM kan operera materielen med känd och värderad risk. Förtroendet skapas framför allt genom

- strukturerad hantering av krav
- bevis för att kundens (verksamhetens) krav är implementerade
- spårbarhet från krav till implementering
- ökad effektivitet
- ökad kompetensuppbyggnad.

Förtroendet kan inte säkerställas om inte kravhanteringen i sig håller tillräckligt god kvalitet. Detta dokument presenterar ett antal omkringliggande frågeställningar i syfte att stärka kravhanteringsarbetet och kvaliteten i projekten.

1.1 Syfte

Det huvudsakliga syftet med vägledningen är att beskriva hur ovanstående förtroendeambition ska realiseras. Detta sker genom att framtagning och granskning av underlag genomförs enhetligt i alla faser. Till sist erhåller FM en enhetligt utformad leverans i form av ITSS 4 (IT-Säkerhetsspecifikation) och ISD (IT-säkerhetsdeklaration).

Syftet är sedan olika för olika målgrupper:

Målgrupp	Syfte
Projekten	Projekten ska få förståelse för vilket säkerhetsarbete som ska bedrivas och vilka underlag/artefakter som ska tas fram i olika faser för att kunna påvisa att man har kontroll på produktens säkerhetsaspekter.
FM	Försvarsmakten ska erhålla IT-system i rätt tid, till rätt kostnad och till rätt kvalitet avseende IT-säkerhet.
MUST	MUST ska inför yttrande få underlag av god kvalitet så att IT-systemet kan bedömas och godkännas utan omfattande egen resursinsats.
Leverantör till FMV	Leverantörer till FMV ska genom en IT-säkerhetsarkitektur få förståelse för de IT-säkerhetskrav som produkten omfattas av samt vilket ansvar för IT-säkerheten som FMV förväntar sig att leverantören tar.

1.2 Berörda system och produkter

IT-system som anskaffas och vidmakthålls av FMV och som ska ackrediteras hos FM ska följa ISD-processen.

Instruktionen gäller även de system som hanterar information som ej omfattas av sekretess.

2 Basfakta

2.1 Referenser

Ref.	Dokumentnamn	Dok. id.
[1]	Metodbeskrivning inklusive mall för framtagning av ISD-plan	13FMV5921-7:3
[2]	Metodbeskrivning ITSS 2	13FMV5921-9:3
[3]	Mall ITSS 2 (IT-säkerhetsarkitektur)	13FMV5921-17:3
[4]	Mall ITSS 4	13FMV5921-20:3
[5]	Mall ITSS 1	13FMV5921-16:3
[6]	Instruktion Verifiering system av system	13FMV5921-8:1
[7]	MIL std 1521	
[8]	Metodbeskrivningen för genomförande av oberoende granskning i ISD-processens faser Produktion och Leverans FM	13FMV5921-11:3
[9]	Checklista för värdering av indata från FM inför fas 1 Kravdefinition.	
[10]	Checklista för egenkontroll ISD-plan	
[11]	Checklista för egenkontroll ITSS 1	
[12]	Checklista för egenkontroll ITSS 2	
[13]	Checklista för egenkontroll ITSS/4	
[14]	Checklista för egenkontroll ISU/ISD	

2.2 Begrepp och förkortningar

Begrepp	Definition/förklaring
BOA	Beslut om användning
CDR	Critical Design Review
FCA	Functional Configuration Audit
ISD-plan	Plan för uppdragets genomförande avseende informationssäkerhet
ISPP	Information Security Program Plan

Begrepp	Definition/förklaring
KSF	MUST Krav på säkerhetsfunktioner
MÖL	Materielöverlämning
PPR	Project Plan Review
PDR	Preliminary Design Review
SFID	Säkerhetsfunktionsmål identitet (identitet på tekniska säkerhetsmål)
SDR	System Design Review
SI	Systemingenjör
SOW/VÅS	Statement of Work/verksamhetsåtagandespecifikation
SRR	System Requirement Review
SÖL	Systemöverlämning
TAU	Försvarsmaktens klassning av ackrediteringsobjekt. BOA tas för det system som använder objektet.
TRR	Test Readiness Review
TTEM	Taktisk – Teknisk – Ekonomisk målsättning
TS	Teknisk specifikation
VHL	Verksamhetsledningssystem

3 VÄGLEDNING

3.1 ÖVERSIKT

Syftet med processen för utveckling av säkra system är att säkerställa att göra rätt saker från början och därmed säkerställa kvaliteten. Det innebär bland annat att redan i kravdefinitionsfasen se till att:

- Systemet utvecklas på rätt grunder med underlag från FM. vilket håller tillräckligt god kvalitet.
- Det finns en ISD-plan för hur IT-säkerhetsarbetet ska bedrivas under systemets livscykel.
- Ta fram ITSS, för att i varje fas vidareutveckla det fram till det slutgiltiga ITSS. Varje ITSS 1-4 är anpassad till utvecklingscykeln.

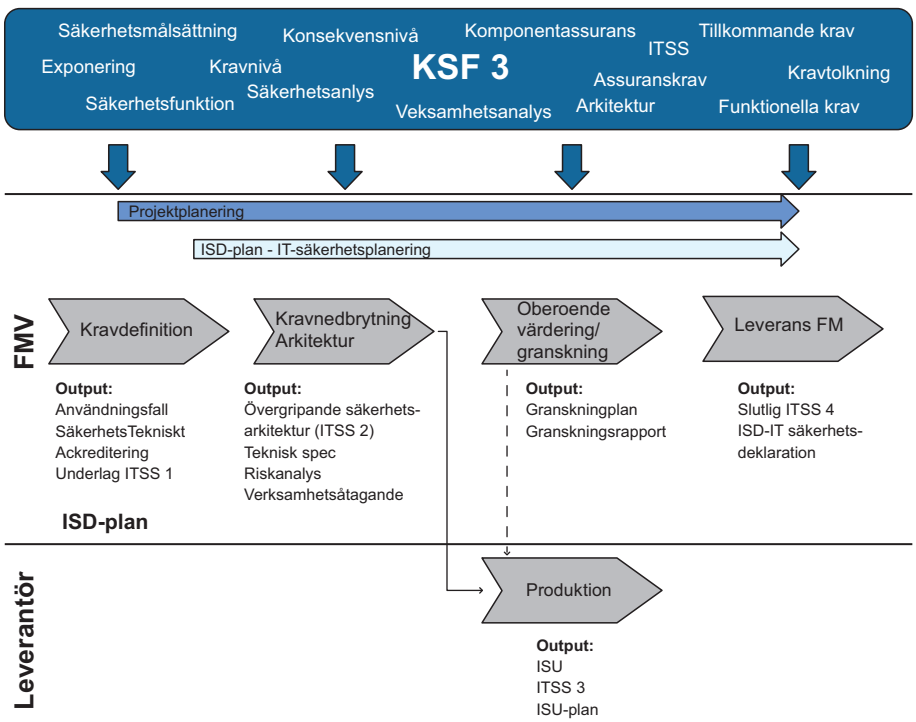


Bild 3:1 Processen för utveckling av säkra system

Ovan visas processen för säker utveckling av system samt vilket resultat varje fas ska ge. Avsnitten som följer beskriver respektive fas i processen, omfattning av dess leverabler, granskningskriterier, kriterier för avslag samt stöd.

3.2 Tillämpning av ISD-processen

Alla IT-system som anskaffas och vidmakthålls av FMV och som ska ackrediteras hos FM ska följa ISD-processen.

Informationssäkerhet omfattar såväl rutiner, fysiskt skydd som teknik. Vad som ska uppfyllas genom teknik och vad som ska uppfyllas med fysiskt skydd och rutiner måste avgöras senast innan upphandling. Därefter ökar kostnader avsevärt. FMV tar ansvar för tekniken och FM tar ansvar för att säkerställa kravuppfyllnad för IT-systemets omgivning.

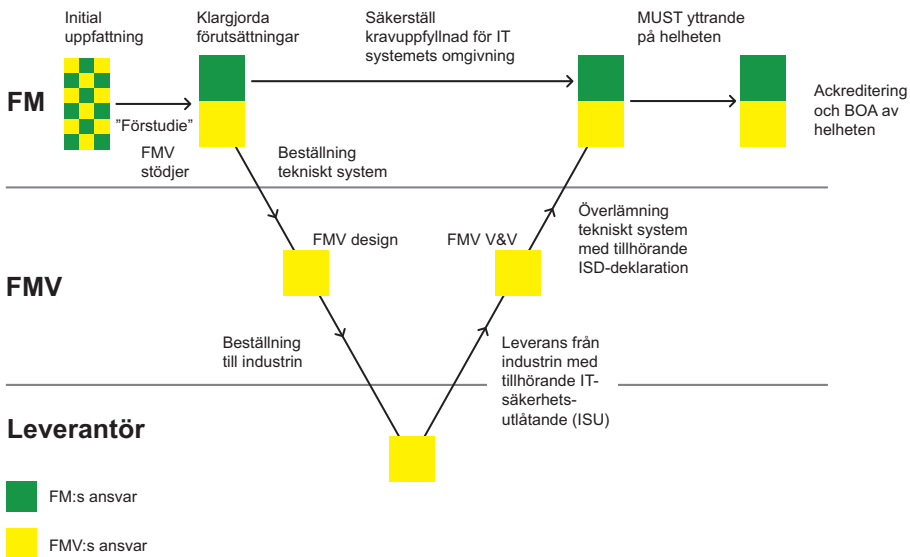


Bild 3:2 Ansvar och roller

I vidmakthållande sker ändringar i systemet och bedöms avseende påverkan på ackrediteringsarbetet enligt följande klasser:

1. Kravuppfyllnaden i befintlig ITSS 4, ISD påverkas inte.
   Resultatet: Ska inte ackrediteras, det gamla godkännandet gäller.
2. Kravuppfyllnaden i befintlig ITSS 4 och ISD påverkas. Förändringen är dock inte sådan att den påverkar ITSS 2 det vill säga IT-säkerhetsarkitekturen är robust och stabil med anledning av ändringen.
   Resultatet: De kravområdena som påverkas ska ses över. Det kan också innebära att man behöver bedöma enskilda krav.
3. Kravuppfyllnaden i såväl ITSS 4, ISD som i ITSS 2 påverkas.
   Resultat: Detta är en större ändring och projektet behöver starta ISD processen med ITSS 2 arbetet.
4. Resulterar bedömningen i att detta är ett nytt uppdrag ska man ge-nomföra hela ISD-processen.

ISD-planen styr omfattningen av ackrediteringsarbetet samt vilka moment i ISD-processen som ska gås igenom.

3.3 Fas – Kravdefinition

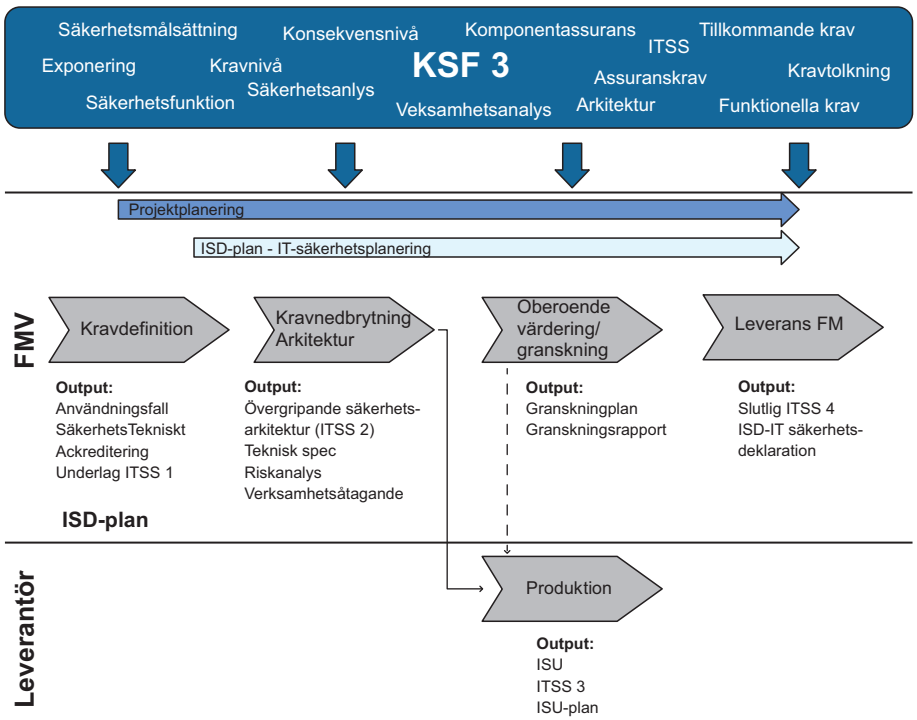


Bild 3:3 ISD -processen fokus kravdefinition

Syftet med *kravdefinition* är att tolka FM krav och ta fram en plan för IT-säkerhetsarbetet (ISD-plan) samt IT-säkerhetsspecifikation (ITSS 1) som tillsammans leder till IT-säkerhetsdeklaration (ISD). Krav på omgivning ska framgå av ITSS 1. Vilka aktiviteter som krävs för att tydliggöra krav på omgivningen ska framgå i ISD-planen. Resultatet från denna fas avgör vilket ansvar FMV kan ta, ur ett ackrediteringsperspektiv, för att utveckla systemet samt vilka tillkommande aktiviteter som kan krävas.

Indata till fasen kravdefinition kan vara Säkerhetsmålsättning samt TTEM. Finns inte dessa indata ska FMV verka för att ta fram användningsfall. Arbetet med att ta fram användningsfall inkluderar även att genomföra riskanalys där verksamhetens sårbarheter framkommer via konsekvensbedömning.

Leverablerna från fasen Kravdefinition är

- ITSS 1
- ISD-plan.

3.3.1 Roller

Fasen Kravdefinition innehåller tre steg:

1. Värdering av FM input, till stöd för att värdera indatat från FM finns checklista, se *[9]*.
2. Genomföra kravfångst samt identifiera vilka aktiviteter som krävs för IT-säkerhetsarbetet. Resultatet dokumenteras i ITSS 1 och ISD-plan.
3. Granskning av fasens artefakter.
4. Fastställs av chefsingenjör.

Steg 1-2 genomförs av projektet.

Steg 3 genomförs av Systemgranskningsledare (SystGL) IT-säkerhet.

Granskning av leverablerna som genomförs ska genomföras av certifierad resurs (kravställs av SystGL)för att säkerställa att den genomförs med rätt kunskapsnivå. Kompetenskvalificering för granskare ska finnas. Berörd systemgranskningsledare har som ansvar att följa upp kompetensen hos granskare och även tillhandahålla utbildning. Se även *[8]*.

3.3.2 Överlämningspunkt FM till FMV

Fasen kravdefinition ska resultera i en överenskommelse mellan FM och FMV med avseende på användningsfall som kompletterar Förvarsmaktens säkerhetsmålsättning från ett säkerhetsperspektiv. Denna information kan tas fram genom extra workshops och utredningar som kräver deltagare från FM. Alla sådana aktiviteter ska redovisas i IT-säkerhetsplanen.

3.3.3 Omfattning ITSS 1

STAU 1 är ett dokument som beskriver resultatet från analys av verksamhetens behov från ett säkerhetsperspektiv och TTEM.

Syftet med STAU 1 är kravtolkning av FM krav och att ge förutsättningar för vilka aktiviteter som ska finnas med i ISD-planen.

STAU 1 ska innehålla:

- en beskrivning av säkerhetsfunktionaliteten i systemet utifrån den kravfångst och – tolkning som genomförts i fasen Kravdefinition.
- spårbarhet mot FM-krav och interna FMV-krav
- krav på exponering och assurans.

3.3.4 Omfattning ISD-plan

ISD-planen är ett dokument motsvarande projektplan med utifrån perspektivet IT-säkerhetsarbete. Precis som projektplanen kommer den att uppdateras under systemet utvecklingscykel. ISD-planen omfattar aktiviteter för att FMV ska kunna leverera underlag till FM inför FM beslut om central ackreditering och beslut om användning.

ISD-planen ska innehålla:

- Förutsättningar och utmaningar för IT-säkerhetsarbetet. Exempel på utmaningar kan vara krav på högassurans, hög exponering av information med mera.
- Beskrivning av ackrediteringsobjektet
- Beskrivning av IT-säkerhetsarbetet (roller, samverkan, finansiering och ändringshantering)
- Aktiviteter som krävs för att möta identifierade utmaningar som finns för att kunna leverera godkänt system. Främst fokus på att minska exponering och därmed kravmängd.
- Artefakter (leveranser och aktiviteter)
- Kontrollpunkter för MUST.

3.3.5 Granskningskriterier

För att gå vidare till fasen Kravnedbrytning/arkitektur så ska framtagna dokument tydligt följa *[1]* och *[5]*. Vid avvikelser ska detta dokumenteras. Till stöd för granskningen (egenkontroll) kan checklista *[10]* och *[11]*användas.

Granskningen dokumenteras i ett granskningsprotokoll där deltagare bekräftar att innehållet är korrekt och accepterat.

3.3.6 Kriterier för avslag

Avslag, det vill säga att SystGL inte godkänner dokumenten efter granskning, sker då projektet inte i ISD-planen visar på viljan att lösa identifierade brister i ITSS 1 framförallt avseende identifierade utmaningar i form av exponering samt FM input av verksamhetens behov från ett säkerhetsperspektiv och TTEM.

3.3.7 Stöd

Mallar, instruktioner och vägledningar finns i FMV VHL. FMV har lagt upp det stöd som finns på isd.fmv.se.

Exempel på stöd:

- Metodbeskrivning inklusive mall för framtagning av ISD-plan *[1]*.
- Mall för ITSS 1 *[5]*.
- Facilitering på FMV vid framtagning av användningsfall från ett säkerhetsperspektiv.
- Checklistor för egenkontroll *[10]* och *[11]*.
- Checklista för att värdera indata i TTEM och säkerhetsmålsättning från ett säkerhetsperspektiv från FM, *[9]*.

3.4 Fas – Kravnedbrytning /Arkitektur

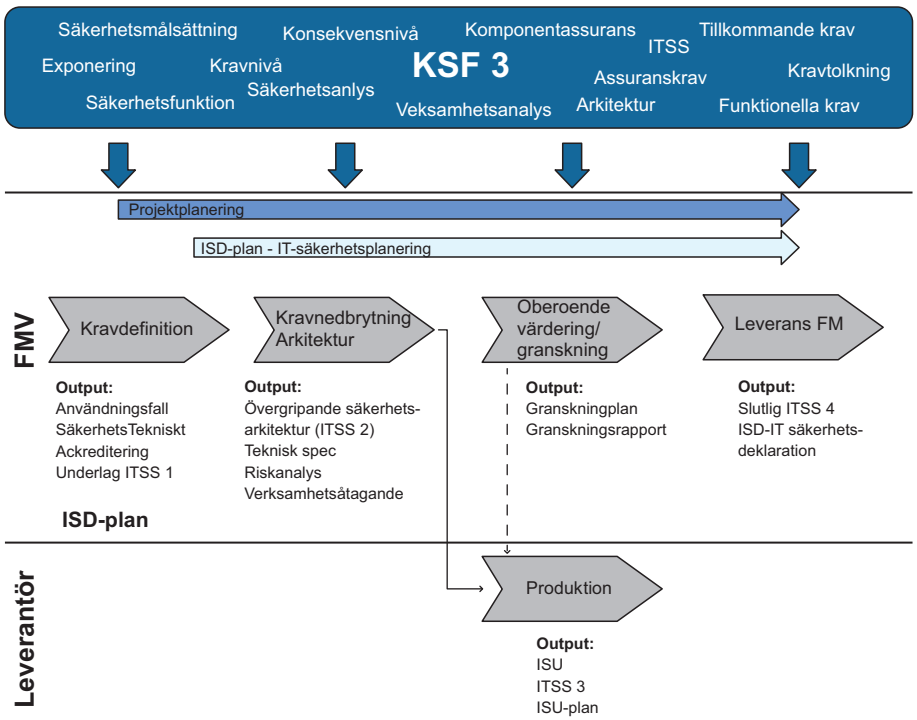


Bild 3:4 ISD -processen fokus kravnedbrytning/arkitektur

Fasen Kravnedbrytning/arkitektur är en iterativ fas med syfte att optimera exponeringsnivån baserad bl.a. på risk- och sårbarhetsanalys så att rätt upphandlingsunderlag finns.

Utifrån en första version av IT-säkerhetsarkitektur prövas om exponeringen kan minskas. Beroende på resultatet från prövningen kan effekt erhållas på verksamheten och/eller IT-säkerhetsarkitekturen. T.ex. kan säkerhetsanalysen behöva omprövas, vissa säkerhetskrav kan behöva överföras till verksamheten, separera informationen i flera olika domäner etc.

Underlaget ska ge leverantören tillräcklig styrning och inriktning både för utveckling/anskaffning av produkt och för dess ackrediteringsarbete.

IT-säkerhetsarkitekturen är nyckeln till att systemet ska bli godkänt med rimliga resurser.

Leverablerna från fasen Kravnedbrytning/arkitektur är

- ITSS 2
- Teknisk specifikation
- Verksamhetsåtagande.

3.4.1 Omfattning STAU 2

Aktiviteter från ISD-planen i fas Kravdefinition genomförs i denna fas och resultatet arbetas in och kompletteras i ITSS 2.

ITSS 2 omfattas av en IT-säkerhetsarkitektur bland annat inkluderande beskrivning av säkerhetsmekanismer och relevanta designmönster som ska vara till leverantörens hjälp i utvecklingen. Se även *[3]*.

3.4.2 Teknisk specifikation för säkerhetslösningen

Den tekniska specifikationen för säkerhetslösningen är en del av den totala tekniska specifikation som tas fram för systemet.

Säkerhetskraven utgörs dels av tekniska krav som är en nedbrytning av verksamhetens behov ur ett säkerhetsperspektiv och av MUST KSF. ITSS 2 utgår ifrån ITSS 1 och omfattar en IT-säkerhetsarkitektur baserad på identifierade säkerhetskrav se *3.4.1*. IT-säkerhetskraven från dessa arbeten inarbetas därefter i den tekniska specifikationen som ska uppfyllas av leverantören.

3.4.3 Omfattning verksamhetsåtagande

Verksamhetsåtagande (VÅS) beskriver kraven på det åtagande som leverantören ska vara ansvarig för i processen.

VÅS innehåller krav på (eventuellt i bilagor):

- Innehåll i milstolpar PPR, SRR, SDR, CDR, TRR och FCA.
- ISPP (krav på leverantörens IT-säkerhetsarbete vad gäller utformning av produkt) innehåller organisation, ändringshantering, avsteg m m.
- Nedbrytning av FMV IT-säkerhetsarkitektur
- Testverksamhet - kompetenskvalificering för testare ska finnas
  - Funktions- och systemtester
  - Penetrationstester (planering, genomförande och resultat med separata oberoende godkännanden)
  - Kryptoverifiering (planering, genomförande och resultat med separata oberoende godkännanden).
- Oberoende granskning, ej relaterat till utveckling av projektet eller närliggande projekt.
- leverantörens ITSS-dokument (enligt ITSS 4).
- leveranser och krav på oberoende värdering vid definierade milstolpar och betalningsutfall

3.4.4 Spårbarhet

Det ska finnas en spårbarhet mellan ITSS 2 och krav från TTEM samt verksamhetens behov från ett säkerhetsperspektiv. I de fall ITSS 1 kan ersätta TTEM och verksamhetens behov från ett säkerhetsperspektiv sker spårbarheten från ITSS 1.

3.4.5 Roller

Granskning av leverabler genomförs av Systemgranskningsledare (SystGL) IT-säkerhet.

Granskning ska genomföras av certifierad resurs för att säkerställa att den genomförs med rätt kunskapsnivå.

3.4.6 Överlämningspunkt FMV till leverantör

Fasen Kravnedbrytning/arkitektur ska resultera i en överenskommelse mellan FMV och leverantör med avseende på artefakterna Teknisk specifikation, VÅS och ITSS 2.

3.4.7 Granskningskriterier

Underlaget är utformat så att FMV i detta läge kan avgöra om projektet har förutsättningar för att bli godkänt efter leverantörens designarbete. En förutsättning för detta är att VÅS och IT-säkerhetsarkitektur är utformad på ett sådant sätt att:

- Det finns en spårbarhet avseende kravallokering mellan verksamhetens behov, teknisk specifikation och säkerhetsarkitektur.
- Exponeringsanalys är tillfyllest.
- VÅS innehåller krav på aktivt IT-säkerhetsarbete av leverantören.
- Riskhantering med plan/tidplan för åtgärder och ansvarig person.

Säkerhetslösning bör även vara utformad på ett kostnadseffektivt sätt.

Granskningen dokumenteras i en granskningsrapport.

Ett stöd för egenkontroll av ITSS 2 finns i form av checklista *[12]*.

3.4.8 Kriterier för avslag

Avslag sker då:

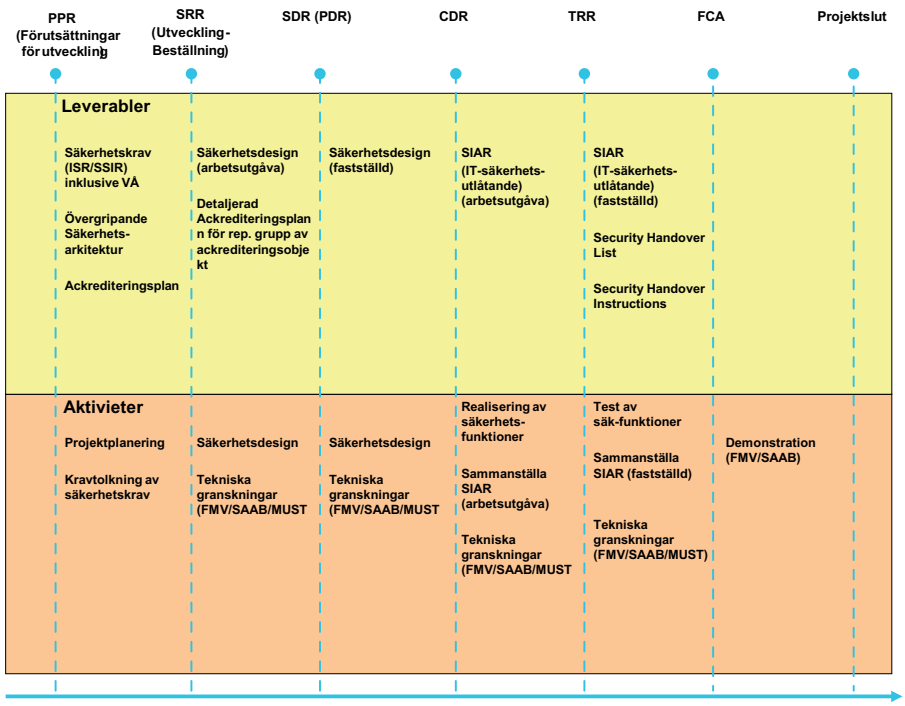
- Projektet har inte förutsättningar att bli godkänt enligt ovan
- Riskbedömning/ar är inte gjord.

3.4.9 Stöd

Metodbeskrivningar, mallar, instruktioner och vägledningar är integrerade i FMV VHL. FMV har lagt upp det stöd som finns samt goda exempel på isd.fmv.se.

Exempel på stöd:

- Metodbeskrivning ITSS 2(IT-säkerhetsarkitektur) *[2]*
- Mall ITSS 2 (IT-säkerhetsarkitektur) *[3]*
- Checklista för egenkontroll ITSS 2 *[12]*.
- Exempel på hur Gripen-projektet har kravställt milstolpe leverablerna *[7]*.



3.5 Fas – Produktion

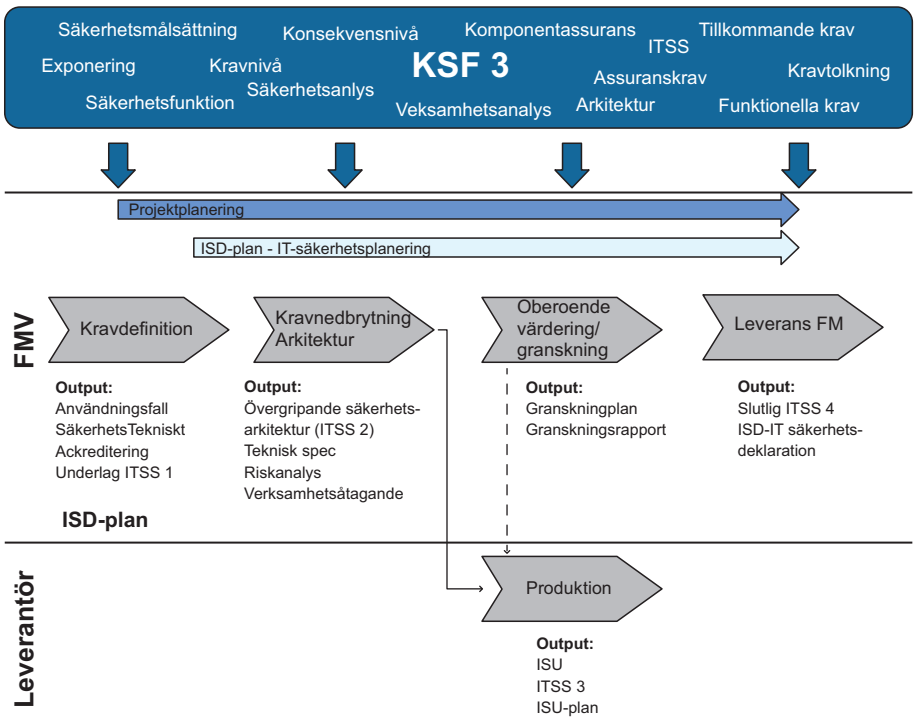


Bild 3:5 ISD-processen fokus fas Produktion

Syftet med fas Produktion är att parallellt med produktion av system/komponent ta fram ackrediteringsunderlag så att FMV:s arbete med ackrediteringsunderlag minimeras. Resultatet tydliggör leverantörens ansvar för IT-säkerhetslösningen.

Indata till fasen Produktion är de leverabler och den planering som gjordes i föregående fas.

Leverablerna från fasen produktion är:

- leverantörens slutdokumentation
- ITSS 3
- ISU-plan
- ISU.

3.5.1 Omfattning leverantörens slutdokumentation

- Enligt krav från VÅS samt leverantörens ISU-plan, ISU och ITSS 3.
- Leveranser vid definierade milstolpar PPR, SRR, SDR, CDR, TRR och FCA med betalningsutfall, *[7]*.
- Testverksamheten: Funktionella- och penetrationstester, kryptoverifiering.
- Nedbrytning/detaljering av säkerhetsarkitekturen för vidare design- och utvecklingsarbete.

3.5.2 Omfattning ITSS 3

Se ITSS 4 exklusive GFE och annat som FMV själva adderar efter överenskommelse.

3.5.3 Roller

Oberoende granskning av leverantörens IT-säkerhetsarbete ska genomföras. Syftet är att säkerställa kravuppfyllnad mot FMV:s krav. Detta kan genomföras i två steg, dels genom att leverantören själv anlitar en oberoende part för granskning, dels genom att projektet anlitar oberoende granskare som stöttar i de olika faserna mot leverantören. Oberoende granskning ska genomföras av en resurs med rätt kompetens och som inte är knuten till leverantören eller till FMV:s projekt.

Oberoende granskning kan genomföras som del av de leverantörsgranskningar som har definierats i VÅS.

Leveransen ska granskas och godkännas av juridisk person hos leverantören vid sidan av projektet.

3.5.4 Överlämningspunkt Leverantör till FMV

Fasen produktion ska resultera i en överenskommelse mellan Leverantör och FMV med avseende på leverablerna ITSS 3 och ISU. Detta ligger till grund för FMV:s leverans till FM.

3.5.5 Granskningskriterier

För att gå vidare till fasen leverans så ska framtagna dokument tydligt beskriva följande:

- ISU-plan som visar att alla förutsättningar beslutas i SDR och att den färdiga designen beslutas i CDR.
- ITSS 3 har den omfattning och innehåll som kravställts i VÅ.
- Kravuppfyllnad mot ställda krav.
- Ansvarig person oberoende från projektet ska underteckna ISU.
- Resultat av oberoende granskning.

Till stöd för granskningen finns checklistor för egenkontroll för ISU *[13]* och ITSS 3/4 *[14]*.

3.5.6 Kriterier för avslag

Kriterier för avslag är olika beroende på om det är PPR, SRR, SDR, CDR, TRR eller FCA.

- Vid PPR sker avslag då FMV bedömer att tidplan är orealistisk.
- Vid SRR sker avslag då FMV bedömer att leverantören inte har förstått IT-säkerhetskraven.
- Vid SDR sker avslag då FMV bedömer att designansatsen inte är hållbar.
- Vid CDR sker avslag då FMV bedömer att IT-säkerhetslösningen inte kan ackrediteras.
- Vid TRR sker avslag då FMV bedömer att kravställda tester inte är tillräckliga.
- Vid FCA sker avslag då ISU saknas.

3.5.7 Stöd

Mall för ITSS 4 *[4]*.

Checklistor för egenkontroll ITSS 3 *[13]* och ISU *[14]*.

Metodbeskrivningar, mallar, instruktioner och vägledningar finns integrerat i FMV VHL. FMV har lagt upp det stöd som finns på isd.fmv.se.

3.6 Fas – FM Leverans

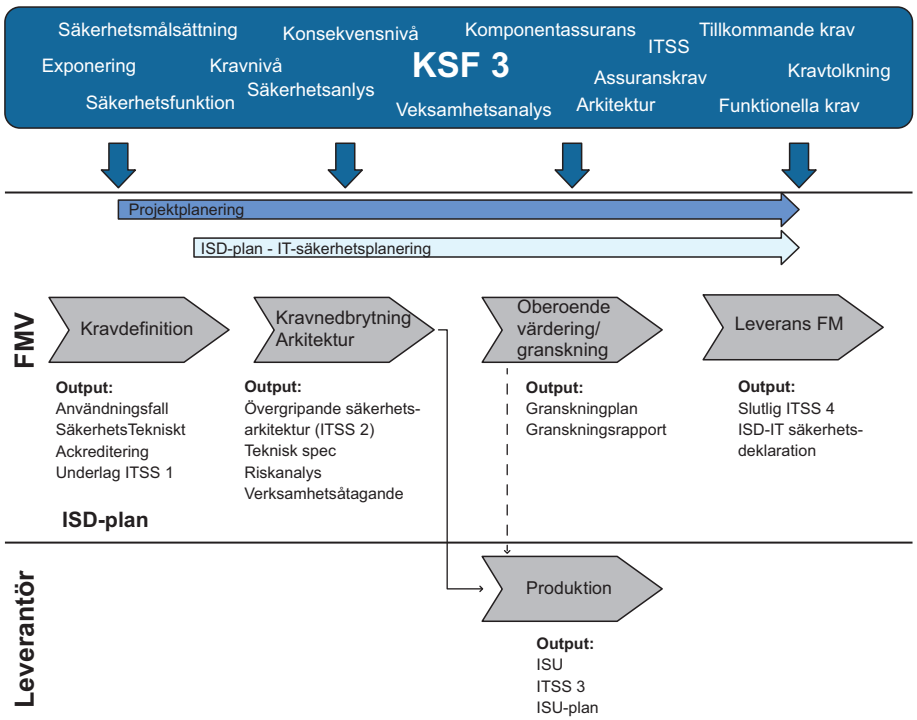


Bild 3:6 ISD-processen fokus Leverans

Syftet med fas Leverans FM är att leverera ett enhetligt kvalitativt underlag för ackreditering. Resultatet tydliggör FMV:s ansvar för IT-säkerhetslösningen.

I fasen FM Leverans levereras en fullt utvecklad ITSS 4 och ISD för godkännande till FM efter TC beslut.

Genom att underlaget följer enhetlig struktur och spårbarhet vet FM hur denna bedömning har genomförts, på vilka grunder samt vad som återstår för dem att bedöma. Underlaget som överlämnas i form av ITSS 4 ska underlätta för FM:s fortsatta handläggning.

3.6.1 Omfattning ITSS 4

ITSS 4 är huvuddokumentet och sammanfattning för hela ackrediteringsarbetet. Huvuddokumentet ska vara ett väl sammanställt, läsbart underlag som beskriver de mest, utifrån IT-säkerhet, relevanta aspekterna kring systemet, dess säkerhetsfunktionalitet och kravuppfyllnad för IT-säkerhet på ett spårbart sätt. Ett antal mer detaljerade dokument medföljer sedan som bilagor och hänvisning till dessa för mer information sker vid behov. Se även *[4]*.

3.6.2 Roller

Granskning av leverabler genomförs av Systemgranskningsledare (SystGL) IT-säkerhet.

Granskningen dokumenteras i ett granskningsprotokoll.

3.6.3 Granskningskriterier

Huvuddokumentet för ITSS 4 ska hjälpa MUST i sitt arbete i underlag för godkännande och ska därför vara läsbart i den bemärkelsen att det finns spårbarhet, en röd tråd i dokumentet och att MUST ser hur säkerhetslösningen ser ut. Det ska också gå att läsa ut avvikelser, brister och alternativa åtgärder.

Granskningskriteriernas utgångpunkt är att ITSS 4 ska hålla sådan kvalitet och nivå att ett godkännande kan lämnas baserat på dess innehåll.

Till stöd för granskningen finns checklistor för egenkontroll ITSS 4, *[13]* och ISD *[14]*.

3.6.4 Överlämningspunkt FMV till FM

I fasen FM Leverans fattar Teknisk Chef beslut om överlämning av produkten till FM genom att underteckna ISD. Viktig grund för detta är dels den oberoende granskning som genomförts av systemgranskningsledaren dels utifrån ISU. MUST har ett starkt intresse av att det blir en oberoende granskning. ITSS 4 med bilagor, granskningsrapport utgör grunden för ISD. Se även *[8]*.

3.6.5 Kriterier för avslag

Avslag erhålls om:

- Dokumentet inte visar på att ett genomtänkt IT-säkerhetsarbete har bedrivits. Det saknas hållbar motivation till olika viktiga ställningstaganden och spårbarhet har inte upprätthållits genomgående.
- Systemgranskningsledare har bedömt att projektet inte har förutsättningar för att bli godkänt.

3.6.6 Stöd

Metodbeskrivningar, mallar, instruktioner och vägledningar finns integrerat i FMV VHL. FMV har lagt upp det stöd som finns på isd.fmv.se.

Mall ITSS 4 *[4]*.

Checklistor för egenkontroll ITSS 4 *[13]* och ISD *[14]*.

Bilaga 1 Mallar

Följande mallar i word-format finns till ISD IT-säkerhet.

- Metodbeskrivning ISD/ISU-plan
  - *Mall ISD/ISU-plan*
  - *Mall ISD*
  - *Mall ITSS 4 och 3*
- Metodbeskrivning Användningsfall
  - *Mall Verksamhetsbeskrivning*
  - *Mall Säkerhetsanalys*
  - *Mall för ITSS 1*
- Metodbeskrivning ITSS 2
  - *Mall för STAU 2*
- Metodbeskrivning oberoende värdering
  - *Mall Granskningsplan*
  - *Mall Granskningsrapport*
- Checklista för egenkontroll

Upprättad ISD-plan fastställs av chefsingenjör.

Rekommenderas att upprättad ITSS 1 fastställs parallellt med ISD-plan.

Rekommenderas att upprättad ITSS 2 och verksamhetsåtagande (VÅS) fastställs av chefsingenjör.

Upprättade ISD och ITSS 4 fastställs av teknisk chef.