Metodstöd för ISD-processen –
Övergripande beskrivning

Kundnyttan med ISD-processens metodstöd

REVISIONSHISTORIK

Version	Datum	Beskrivning	Ansvar
2.3	2016-06-30	Mindre uppdateringar med avseende på be-grepp och förtydliganden baserat på erfarenhetsåterkopp-ling. Version 2.2 är bokformatet.	DAOLO
2.1	2014-05-30	Mindre uppdateringar med avseende på begrepp och förtydliganden	DAOLO
2.0	2013-10-25	Uppdaterad efter remissynpunkter från CIO och MUST	DAOLO
1.0	2013-06-18	Fastställd	DAOLO

Innehåll

1 INLEDNING

ISD-processen är en del av FM:s beslutsprocess. ISD-processen styr IT-säkerhetsarbetet vid utveckling av säkra och godkända system. Processen gäller även komponenter, som inte anses säkerhetskritiska (typ signalskydd). Inom ramen för CIO:s ISD-arbete tar FMV fram ett metodstöd som fokuserar på hur IT-säkerhetsarbetet ska bedrivas av FM, FMV och Leverantör.

1.1 SYFTE

Syftet med detta dokument är att ge en beskrivning av hur ISD-processen integrerar med FMV VHL, KSF 3 och FM IT-processen samt ge en övergripande beskrivning av det metodstöd som finns för ISD-processen. Beskrivningen består av erhållen kundnytta, metodstöd och i tillämpliga fall vad som krävs för genomförande.

1.2 AVGRÄNSNING

Detta dokument har inte ambitionen att beskriva ISD-processen i sin helhet utan enbart på ett sådant sätt att projekten kan se och skapa sig en uppfattning om vilka faser som finns i processen, vem som har vilket ansvar samt vilka artefakter som förväntas från varje fas. Projektsäkerhet är inte en del av ISD-processen.

1.3 MÅLGRUPP

Målgruppen för detta dokument är FM, MUST, FMV projektledare/chefer samt leverantörer.

1.4 Definition Informationssäkerhet

Området informationssäkerhet innefattar såväl det område som traditionellt benämns datasäkerhet som övriga begrepp som har anknytning till hur information kunna hanteras på ett säkert sätt i skilda slag av verksamheter. Informationssäkerhet beskrivs på flera olika sätt, beroende på ändamål. Enligt *[5]* är en vanlig uppdelning enligt *bild 1:1* nedan där man har utgått ifrån skyddsåtgärdernas miljö, teknisk respektive administrativ.

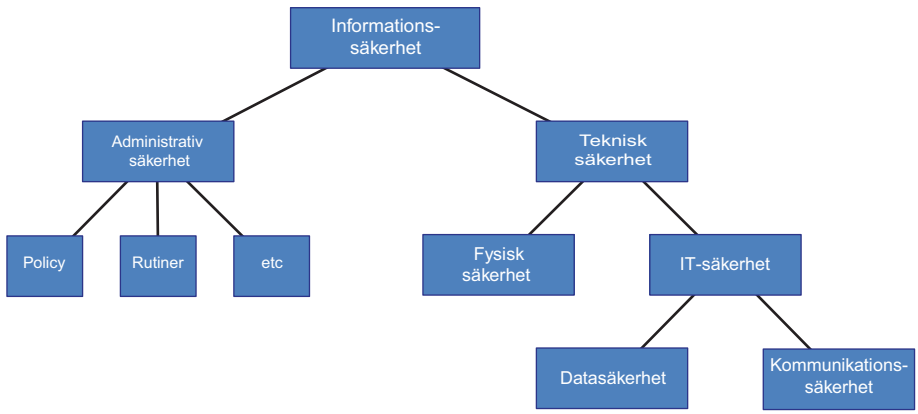

Bild 1:1 Definition Informationssäkerhet

1.5 Basfakta

1.5.1 Begrepp och förkortningar

Begrepp/förkortning	Förklaring
AG	Arbetsgrupp
Datasäkerhet	Säkerhet beträffande skydd av datorsystem och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling
FM	Försvarsmakten
FMV	Försvarets Materielverk
FSA	Funktionsansvarig

Begrepp/förkortning	Förklaring
Fysiskt skydd	Skydd som ingår i IT-systemets omgivning och som skyddar mot obehörig direkt fysisk tillgång till systemets resurser
GFE	Govermental Furnished Equipment
Informationssäkerhet	Säkerhets för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet
ISD	IT-säkerhetsdeklaration
ISPP	Information Security Process Plan – ingår i en leverantörs verksamhetsåtagande och beskriver hur säkerhetsarbetet ska genomföras för att skapa ett säkert system. Ex ändringshantering, Arbetsgrupper för säkerhet m m
ISU	IT-säkerhetsutlåtande
IT-säkerhet	Säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation
ITSS	IT-säkerhetsspecifikation
Kommunikationssäkerhet	Säkerhet i samband med överföring av data
MSA	MaterielSystemAnsvarig
SE	System Engineering – utveckling av komplexa system med hänsyn tagen till systemets hela livscykel
SM	SäkerhetsMålsättning
TTEM	Taktiskt Tekniskt Ekonomiskt Målsättning
VHL	VerksamhetsLedningsystem
VoV	Verifiering och Validering
VÅ	VerksamhetsÅtagande

1.5.2 Referenser

Nr	Referens	Dokumentnummer
[1]	Försvarsmaktens IT-styrmodell	Bilaga till HKV 09700:64970
[2]	KSF 3	FM2014-5302:1
[3]	Instruktion för Verifiering system av system	13FMV5921-8:1
[4]	FMV Vägledning för ISD och SE	13FMV5412-3:4
[5]	SIS Handbok 550	Utgåva 3
[6]	Metodbeskrivning för framtagning av ISD/ISU-plan (inkluderar mall)	13FMV5921-7:4
[7]	Metodbeskrivning för framtagning av användningsfall (inkluderar mallar)	13FMV5921-8:2
[8]	Metodbeskrivning för framtagning av ITSS 2: IT-säkerhetsarkitektur (inkluderar mall)	13FMV5921-9:3
[9]	Metodbeskrivning för genomförande Oberoende granskning (inkluderar mallar)	13FMV5921-11:4
[10]	Mall för ITSS 1	13FMV5921-16:3
[11]	Mall för ITSS 4/3	13FMV5921-20:3

2 ISD-PROCESSEN

ISD kvalitetssäkrar leveranser till FM och är därmed en förutsättning för att FMV ska kunna ta sitt designansvar. Detta görs genom att integrera ISD med FMV VHL och därmed SE-arbete. Ambitionen är även att integrera ISD med MUST KSF 3 och FM IT-styrningsprocess, se *bild 2:4* och *bild 2:5*.

2.1 ISD-PROCESSEN

ISD-processen kan dels beskrivas i ett SE-perspektiv (System Engineering), se *bild 2:1*. Mer detaljerade beskrivningar kring detta finns i Vägledningarna ISD och SE *[4]*.

Syftet med ISD-processen i ett SE-perspektiv är att säkerställa att göra rätt saker från början och därmed säkerställa kvaliteten på leveransen till FM.

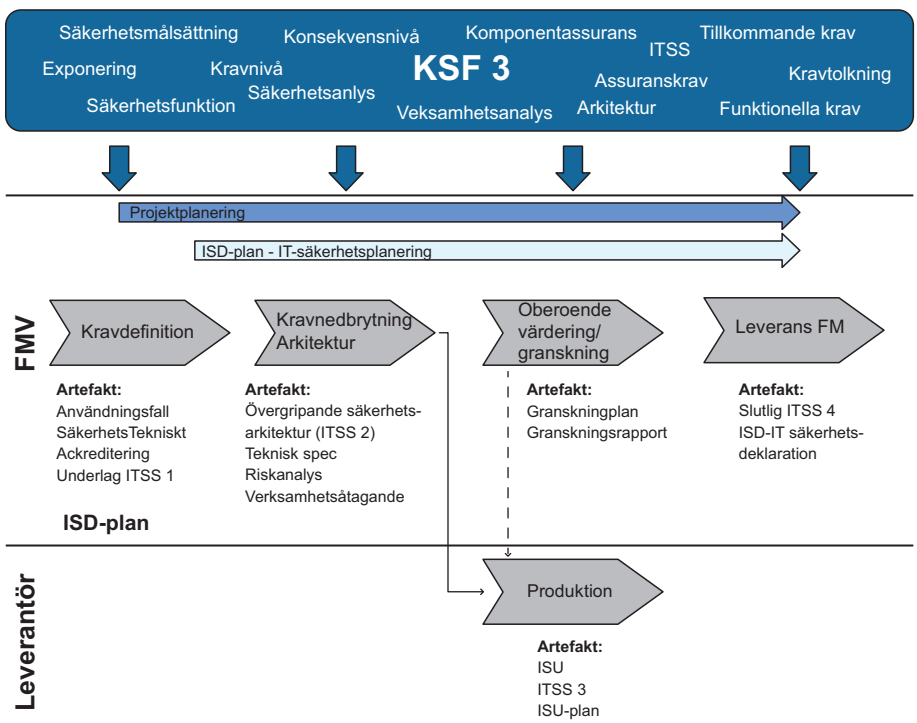

Bild 2:1 ISD-processen

Kvaliteten på leverablerna från varje fas i ISD-processen kan kontrolleras med hjälp av egenkontroll som ska illustreras i *bild 2:2* Leverablerna från varje fas i SE- System Engineering genomgår en egenkontroll via checklistor. Resultatet från egenkontroll kan resultera i en rapport innehållande slutsatser och beslutsunderlag till projektledningen för fortsatt hantering i projektet.

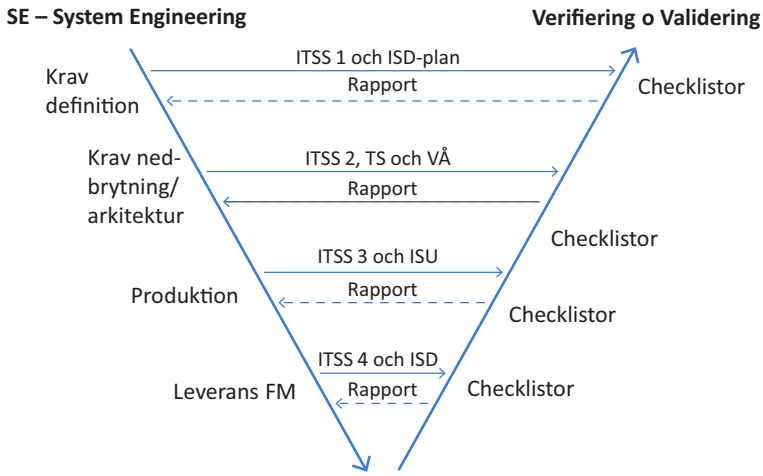

Bild 2:2 ISD-processen egenkontroll

2.2 ISD:S RELATION TILL FMV VHL, KSF 3 OCH FM IT-STYRNINGSPROCESS

Det metodstöd som nu finns framme för ISD är integrerad med FMV verksamhetsledningssystem (VHL), MUST KSF 3 och FM IT-processen, vilket beskrivs i detta avsnitt.

2.2.1 FMV VHL

ISD-processen är integrerad med FMV VHL. Vid projektstart stöds PL av planeringsstöd för domänerna Systemsäkerhet, Systemarbete, Verifiering och validering samt Överlämning. ISD har tillfört planering av IT-säkerhetsarbete vilket innebär att när processen mynnar ut i planerat systemarbete är IT-säkerhetsarbetet inkluderat. Detsamma gäller för planering av VoV, när det arbetet mynnar ut i planerad VoV är IT-säkerhetsarbetet inkluderat.

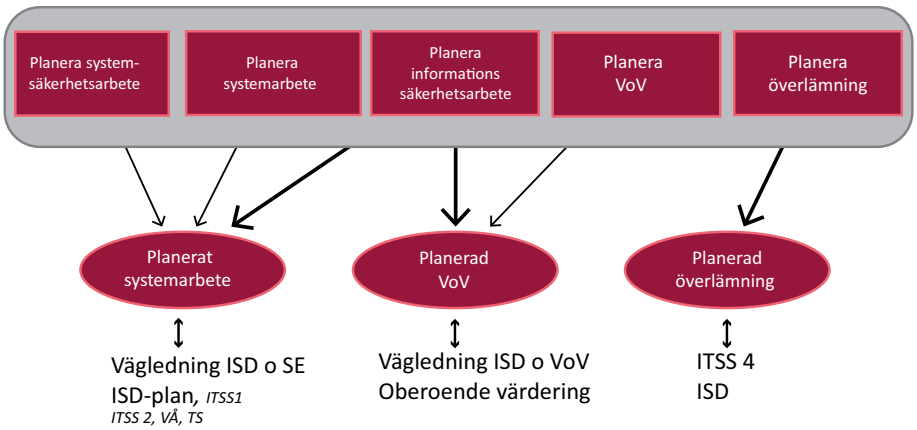

Bild 2:3 ISD, en del av FMV VHL

2.2.2 KSF 3

Bild 2:4 visar kravnedbrytningsflödet från Säkerhetsmålsättning till krav på IT-säkerhetsfunktioner i KSF 3 *[2]*. Den kravnivå ett system tilldelas avgörs utifrån en konsekvensbedömning av information ur ett sekretessperspektiv och den exponeringsnivå som ett system utsätts för. Utan ingångsvärden från Säkerhetsmålsättningen kan inte denna kravnivå bestämmas och värdering av KSF-krav utifrån ett verksamhetsperspektiv kan inte göras. Den totala kravbilden på IT-systemet och dess omgivning består då detta är gjort av funktionella IT-säkerhetskrav och assuranskrav från KSF, tillkommande säkerhetskrav från verksamhets-, och säkerhetsanalyserna samt övriga säkerhetskrav såsom tillträdesbegränsning, utbildning etc. I ISD-processen beskrivs kravnerbrytning i ITSS 1, 2, 3 och 4.

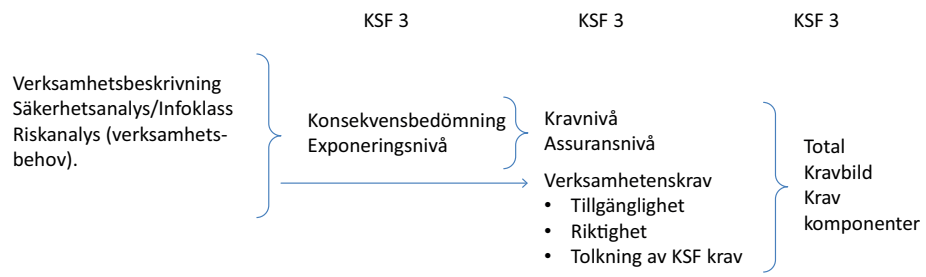

Bild 2:4 Kravnedbrytning KSF 3

2.2.3 ITSS

FM initierar dokumentation enligt IT-säkerhetsspecifikationen (ITSS) och det blir indata till FMV:s IT-säkerhetsarbete. Därifrån tar FMV över ansvaret och utvecklar ITSS över systemutvecklingens livscykel enligt *bild 2:1*, inklusive kravhanteringsprocessen med kravfångst, kravnedbrytning och överlämning. FMV överlämnar vid utvecklingens slut ett ITSS till FM, som använder det i sina beslut. Alla resultat från *avsnitt 2.2.1* dokumenteras i ITSS enligt KSF 3.

2.2.4 FM IT-process

Syftet med Försvarsmaktens IT-process är att öka effektiviteten och kvaliteten inom sakområdet och att skapa förutsättningar för ökad verksamhetsnytta genom samordning och utveckling av Försvarsmaktens IS/IT-verksamhet se *[1]*. *Bild 2:5* visar den tänkta kopplingen mellan ISD-processen och FM IT-styrmodell, samt den tänkta nya modellen för produktprocessen.

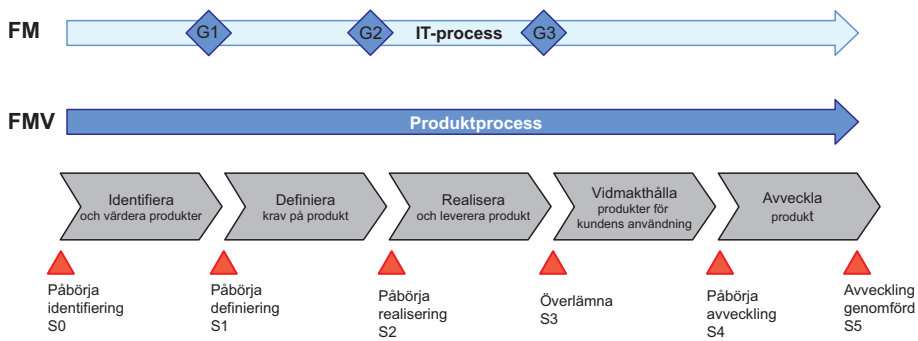

Bild 2:5 FM IT-styrmodell i samverkan med ISD-processen

Försvarsmaktens uppgift är att beskriva vilken förmåga system eller komponenter ska ha. Detta beskrivs i TTEM. FM tar även fram en plan för avstämningspunkter med MUST. Övriga dokument tas fram av FMV förutsatt att tillräckliga FM-resurser är tillgängliga. ISD-planen är ett viktigt dokument som visar på hur IT-säkerhetsarbetet är tänkt att bedrivas från FMV under hela systemet livscykel.

3 OMFATTNING ISD 2.3

Metodstödet för IT-säkerhetsarbetet för ISD-processen omfattar områden enligt *bild 3:1*. För varje område har metodbeskrivningar tagits fram samt i tillämpliga fall vägledningar, checklistor och mallar. Metodstödet har tagit hänsyn till KSF 3 samt FM IT-processen vilka utgör påverkansfaktorer på ISD-processen.

FM ansvarar för KSF 3 (MUST) och IT-processen (CIO). Vid införande av KSF 3 ska ITSS 1,2,3 och 4 ersättas med ITSS (motsvarande dokument i KSF 3). Innehållsmässigt innehåller dokumenten samma information.

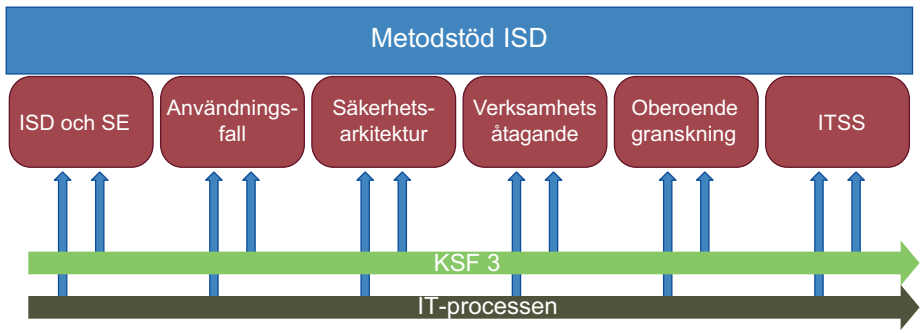

Bild 3:1 Omfattning metodstöd ISD

- Metodstöd ISD (detta dokument) beskriver ISD-processens metodstöd i sin helhet.
- Metodstöd Management omfattar metoder för stöd till projektledare och chefer. Metoderna här är ett stöd i projektgenomförandet och redovisar viktiga förberedande åtgärder innan start av projekt. Metodstödet omfattas av ISD och SE som beskriver ISD-processen ur ett SE-perspektiv. Utbildning, kompetens och erfarenhet är viktigt för att kunna arbeta med IT-säkerhetsfrågor i projekt. Därför fokuserar ISD på utbildning, dels avseende ISD- processen specifikt men även för IT-säkerhet i allmänhet. Utbildningen kan med fördel integreras i FM utbildningar för IT-säkerhet.

- Metodstöd omfattar metoder för framtagning av dimensionerande användningsfall, säkerhetsanalys och en analys av verksamhetens sårbarheter. Arbetet ska resultera i en beskrivning av FM:s verksamhetskrav såsom systemets användningsområde, miljö och omgivning, informationssäkerhetsklass samt användare.
- Metodstöd Oberoende granskning omfattar metod för genomförande av granskning av system/komponent av en instans/part som inte har haft någon inblandning i utvecklingen av granskningsobjektet.
- Metodstöd IT-Säkerhetsarkitektur omfattar metodstöd för nedbrytning av säkerhetskrav från FM till en övergripande beskrivning av systemets IT-säkerhetsfunktioner och dess integration i systemet. Nivå på nerbrytning av krav styrs efter ambition i upphandling av system. Trenden är att FMV upphandlar på högre systemnivå vilket innebär att det är leverantören som gör nerbrytningen av krav i detalj.
- Metodstöd Verksamhetsåtagande omfattar metoder för stöd i kravställning på leverantörens IT-säkerhetsarbete som mynnar ut i ett ISU (IT-SäkerhetsUtlåtande) och ett ITSS 3 (IT-SäkerhetsSpecifikation). Nästa version av ISD ska omfatta metodstöd för ett generiskt verksamhetsåtagande.
- ITSS – Allt eftersom de olika faserna utvecklas i ISD-processen kan systemets IT-säkerhetsfunktioner och kravuppfyllnad beskrivas på olika nivåer. Detta görs i ITSS 1,2,3 och 4. För de system som utnyttjar KSF 3 görs denna beskrivning i ITSS. I *[3]* beskrivs hur ITSS 4 tas fram ur ett system av system perspektiv samt hur verifiering system av system kan genomföras.

4 METODER

4.1 INLEDNING

I nedanstående avsnitt beskrivs mer detaljerat ISD-processens metodstöd och framtagning av dess artefakter. Varje metod beskrivs med utgångspunkt från kundnytta, typ av metodstöd samt i tillämpliga fall även vilka förberedelse som krävs samt genomförande. I texten förekommer roller som beställare och leverantör, där till exempel FMV kan vara både beställare och leverantör beroende på var i ISD-processen man befinner sig.

4.2 MANAGEMENT

4.2.1 FMV Vägledning ISD och SE

4.2.1.1 Kundnytta

Det huvudsakliga syftet med vägledningen är att tillgodose FMV:s behov av att på ett strukturerat sätt kvalitetssäkra leveranser till Försvarsmakten.

4.2.1.2 Metodstöd

FMV Vägledning ISD och SE, se *[4]*.

4.2.2 ISD-plan

4.2.2.1 Kundnytta

Nyttan med ISD-planen är att få kontroll över IT-säkerhetsarbetet i tidigt skede så att bland annat rätt resurser och rätt indata kan sättas in i rätt skeden i processen. Tidiga avstämningar med FM bör genomföras, där IT-säkerhetsarbetets upplägg presenteras.

4.2.2.2 Metodstöd

Metodbeskrivning för framtagning av ISD/ISU-plan inkluderande mall för framtagning av ISD-plan, se *[6]*.

4.3 Verksamhetens behov från ett säkerhetsperspektiv

Denna metod omfattas Verksamhetsbeskrivning i form av dimensionerande användningsfall, säkerhetsanalys och genomförande av riskanalys. Riskanalysen i denna fas fokuserar på verksamhetens sårbarheter och konskevenser. Tilläggskraven omfattar främst avseende tillgänglighet och riktighet. Resultatet av arbetet beskriver verksamhetens perspektiv och är nödvändigt inför det fortsatta IT-säkerhetsarbetet.

En effektivisering av arbetet med att få fram användningsfall har gjorts i samband med framtagning av metodstödet:

- Författningsanalys är begränsad till att genomföras i de fall då andra lagar än de rörande nationella krav kring rikets säkerhet är aktuella. För rikets säkerhet hanteras författningskraven med KSF Krav på säkerhetsfunktioner. Tolkningen av KSF ska kopplas till verksamhetens behov och krav.
- Insamling av fakta kring verksamheten omfattande verksamhetsbeskrivning, säkerhetsanalys och risk- och sårbarhetsanalys genomförs på två workshops á 1 dag.
- Den risk-och sårbarhetsanalys som sker är kopplad till verksamhetsbeskrivningen i form av dimensionerande användningsfall, det vill säga en traditionell risk- och sårbarhetsanalys på verksamheten genomförs inte.
- De dimensionerande användningsfallen omfattar såväl sekretess, som tillgänglighet och riktighet och tillsammans med informationsflödet innebär detta en bra start på kommande designarbete.
- Metodstödsmaterialet innehåller mallar för de delar som ingår i arbetet med att ta fram verksamhetens behov. Ambitionen är att om dessa mallar följs, se *[7]*, möjliggöra att tillräcklig information kring verksamheten ur ett säkerhetsperspektiv ska finnas för att utvecklingsarbetet ska bli kostnadseffektivt och att rätt säkerhetskrav ställs på systemet.

4.3.1 Kundnytta

Framtagning av verksamhetens behov från ett säkerhetsperspektiv är FM:s ansvar. Syftet är att ta fram verksamhetens behov gällande informationssäkerhet på ett effektivt sätt så att FMs resurser används så effektivt som möjligt . Kraven ska på ett kostnadseffektivt och balanserat sätt möta miljö- och användarbehov samt ger möjlighet att tolka KSF-krav så att de stödjer verksamhetens behov. För verksamheten icke relevanta KSF-krav, kan då motiveras utifrån det egna behovet.

Resultatet tjänar även som underlag för kravställningar på tillgänglighet och riktighet, samt ger spårbarhet vid förändringar och granskningar under och efter projekt.

4.3.2 Metodstöd

Metodstöd för framtagning av användningsfall omfattar metodbeskrivning för förberedelser och genomförande samt mallar för Verksamhetsbeskrivning inklusive behov av skydd mot oönskade konsekvenser, Säkerhetsanalys, se *[7]*.

4.4 ITSS 2: IT-SÄKERHETSARKITEKTUR

ITSS 2: IT-säkerhetsarkitektur är leverabeln ITSS 2 från fas Kravnedbrytning/ arkitektur i ISD-processen, se *bild 2:1*.

Omfattningen på arbetet beror på komplexiteten på SE-arbetet bl.a. med avseende på beroenden, användningsområde (internationellt, nationellt), kvalitet på dokumentation och indata m m. Trenden är att FMV upphandlar på högre systemnivå vilket innebär att det är leverantören som gör nedbrytningen av krav i detalj.

I denna fas genomförs även en exponeringsanalys på den tänkta designen med intressenter från projektet såsom SE, IT-säkerhet men även från MUST i syfte att minska exponeringen.

Förutsättning för att leverantören (industrin) ska kunna ta fram en detaljerad IT-säkerhetsarkitektur är att FMV i sin kravbild har, en övergripande teknisk säkerhetsarkitektur.

4.4.1 Kundnytta

Med en IT-säkerhetsarkitektur ökar leveransprecisionen till beställaren genom att kravhantering och verifieringsarbetet underlättas för leverantören.

4.4.2 Metodstöd

Metodstödet för framtagning av Säkerhetsarkitektur består av metodbeskrivning för genomförande samt mall, vilka beskrivs i *[8]*.

4.5 VÅ – Verksamhetsåtagande

Verksamhetsåtagande är den andra leverabeln från fas Kravnedbrytning/arkitektur i ISD-processen, se *bild 2:1*.

4.5.1 Kundnytta

Syftet med ett verksamhetsåtagande (VÅ) är att möjliggöra ett effektivt IT-säkerhetsarbete hos leverantören. Utan krav på verksamhetsåtagande avsätts inga resurser för IT-säkerhetsarbetet vilket påverkar tid och pengar.

4.5.2 Metodstöd

Stöd kring verksamhetsåtagandet finns i form av följande vägledningar:

- *Information Security Process Plan* (ISPP), ingår i en leverantörs verksamhetsåtagande och beskriver hur säkerhetsarbetet ska genomföras för att skapa ett säkert system. Ex på områden som ska finnas inplanerade och specificerade i en ISPP är; ändringshantering, arbetsgrupper för säkerhet, tester m m.
- *IT-säkerhetsarkitektur* är en från leverantören detaljerad säkerhetsarkitektur nedbruten från FMV:s övergripande IT-säkerhetsarkitektur. Denna IT-säkerhetsarkitektur ligger till grund för leverantörens design- och implementationsarbete samt utgör en kravspårning till FMV:s krav.
- *IT-säkerhetsspecifikation*, se metodstöd ITSS. FMV ställer krav på innehåll i det ITSS som leverantören ska ta fram. Detta är sedan en del av det ackrediteringsunderlaget som FMV levererar till FM.
- *Säkerhetstekniska tester* – FMV kravställer vilka tester som ska genomföras, vilken information resultatet ska innehålla samt den kompetens som krävs för att genomföra testerna. De tester som är aktuella är:
  - funktionstester
  - penetrationstester
  - kryptoverifering
- *VÅ* – FMV kravställer hur leverantören ska beskriva det verksamhetsåtagande som de tar.

4.5.3 Genomförande

Krav på verksamhetsåtagande tas fram i fasen Kravnedbrytning/arkitektur och är tillsammans med IT-säkerhetsarkitekturen den samlade kravbilden från FMV till leverantören.

FMV ska kravställa de områden som anges i *avsnitt 4.5.2* med utgångspunkt på hur FMV vill att leverantören ska svara upp mot dessa områden. Metodstödet ska tillhandahålla mallar för hur en sådan kravställning kan se ut.

4.6 OBEROENDE GRANSKNING

Med oberoende granskning avses granskning av objekt (system eller specifik produkt/lösning) av en instans/part som inte har haft någon inblandning i utvecklingen av granskningsobjektet. Oberoende granskning initieras av FMV eller MUST och genomförs på det resultat som kommer från leverantören (industri eller FMV). Granskningen kräver att leverantören har gjort en egen bedömning av kravuppfyllnaden och att spårbarhet från kravbilden finns dokumenterad.

Oberoende granskning genomförs i faserna Produktion och Leverans FM. Oberoende granskning kan genomföras på flera nivåer såsom systemperspektiv, övergripande lösningsperspektiv samt en riktad insats mot en specifik säkerhetsfunktion/lösning. Granskningen kan vara både teoretisk och praktisk.

4.6.1 Kundnytta

Ett för FM, FMV och leverantör gemensamt synsätt på att genomföra oberoende granskningar. Metoden visar vad som ska granskas vilket underlättar dokumentation och implementering av säkerhetsfunktioner i granskningsobjektet.

Metodstödet ska säkerställa att resultatet blir detsamma även om olika individer genomför arbetet. Den ska också ställa krav på kvalitet underlaget till granskningen ska ha.

4.6.2 Metodstöd

Metodstödet omfattar metodbeskrivning samt mallar för granskningsplan och granskningsrapport, se *[9]*.

4.7 Ackreditering – ITSS

ITSS 1,2,3 och 4 är leverabler från samtliga faser i ISD-processen, se *bild 2:1*. I ITSS-dokumenten sker kravhanteringen för hela livscykeln.

I de fall system av system ska ackrediteras finns ett stöd för tillvägagångssätt i dokumentet Instruktion Verifiering system av system *[3]*. Det är en beskrivning av hur redan godkända system/produkter och dokument kan återbrukas. Dokumentet beskriver också hur en verifiering system av system kan gå till i olika scenarier där komponenter (system/produkter), godkända såväl som icke godkända, ska sättas samman till ett system av system. När ett system ska utvecklas ska en bedömning göras huruvida andra systems leverabler till exempel Säkerhetsmålsättning/Användningsfall kan återbrukas. Dessutom bör det i planeringen från början tas hänsyn till huruvida systemet ska ingå i system av system.

4.7.1 Kundnytta

Utveckla IT-säkerhetsspecifikation (ITSS) för samtliga faser i ISD-processen. Det slutgiltiga underlaget utarbetas i fasen Leverans FM men arbetet med detta påbörjar redan i den initiala fasen.

Effektivisering av ackrediteringsarbetet i fall av system av system.

4.7.2 Metodstöd

Metodstöd för ITSS 1 omfattas av Vägledning för ISD och SE samt mall ITSS 1 *[10]*, metodstöd för ITSS 2 omfattas av metodbeskrivning och mall ITSS 2 se *avsnitt 4.4* och metodstöd för ITSS 3 och 4 omfattas av Vägledning ISD och SE samt mall för ITSS 3 och 4 *[11]*.

4.8 ISD/ISU

Med stöd från ITSS 4 ska FMV avge en IT - säkerhetsdeklaration ISD som ska skrivas under av Teknisk chef. I deklarationen ska det stå:

- FMV tar ansvar för IT-säkerhetslösningen i Materielsystemet/Produkten som levereras.
- Materielsystemet/produkten uppfyller ställda FM-krav.
- Materielsystemet/produkten har genomfört adekvata aktiviteter i syfte att klargöra att systemet inte har någon känd icke tolererbar risk/egenskap
- ITSS-dokumentet och ISD är utformad enligt de normer som gäller och som ska tas fram i metodarbetet
- Ackrediteringsarbetet följer ISD-plan.

Vid överlämning till FMV har leverantören samma ansvar som FMV enligt ovan. ISU ska tas fram och skrivas under av juridisk ansvarig.