Metodbeskrivning för framtagning
av ITSS 2: IT-säkerhetsarkitektur

Framtagning av ITSS 2

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
1.1	2014-05-30	Mindre uppdateringar med avseende på begrepp och förtydliganden	DAOLO

Innehåll

1 Inledning

Detta dokument utgör en metodbeskrivning för att ta fram IT-säkerhetsarkitektur, fortsättningsvis benämnd som ITSS 2 (IT-säkerhetsspecifikation), som är en leverabel i ISD-processens fas Kravnedbrytning/arkitektur.

Metodbeskrivningen innehåller:

- Generell information om metodbeskrivningen samt en presentation av hur ITSS 2 passar in i ISD-processen (IT-Säkerhetsdeklaration).
- De förberedelser som behövs för arbetet.
- Ett arbetssätt för framtagning av ITSS 2.

1.1 ITSS 2

ISD-processen är framtagen för att möjliggöra kostnadseffektivt och enhetligt IT-säkerhetsarbete i projekt och systemledning inom FM och FMV. Processen tydliggör ansvar och roller mellan olika aktörer, säkerställer att IT-säkerhetsarbetet görs rätt från början samt ökar förtroendet för FMV:s leveranser till FM. Mer detaljer om ISD ges i *[1]*.

Framtagning av ITSS 2 är en del av detta arbete och utgör ett underlag för den slutgiltiga designen. *Bild 1:1* visar ITSS 2 i ISD-processen.

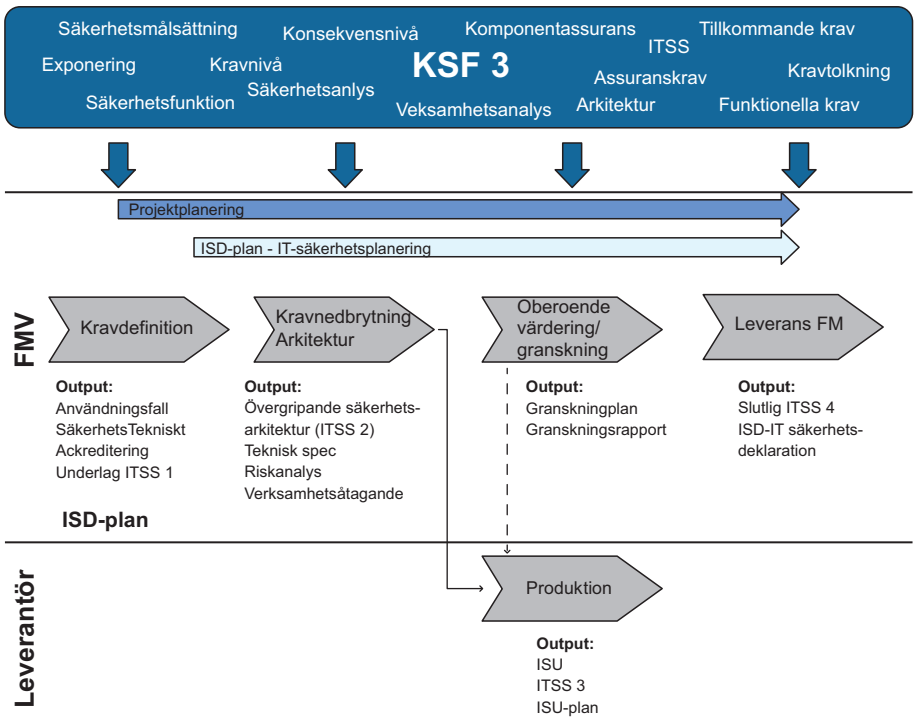

Bild 1:1 ITSS 2 i ISD-processen

1.2 Syfte med ITSS 2

Syftet med IT-säkerhetsarkitektur är att visa på hur IT-säkerhetsfunktionerna används, hur dessa interagerar med varandra och med systemet samt visa på gränsytor.

1.3 Nyttan

ITSS 2 är en del av kravnedbrytningen och är en viktig del i upphandlingen till leverantör. ITSS 2:

- Ökar leverantörens förståelse för kravbilden, vilket ökar projektets förmåga att leverera i tid till rätt kostnad. ITSS 2 kan med fördel vara en utgångspunkt för leverantörens designarbete.
- Är en förutsättning för att minska exponeringen och underlag för alternativa säkerhetslösningar.
- Ökar möjligheten till tidig dialog mellan FMV och leverantörerna kring leverantörernas olika designförslag kring IT-säkerhet.
- Underlättar FMV:s verifiering inför leverans till FM genom bland annat kravallokeringen.

1.4 Dokumentation

Syftet med metodstödet för ITSS 2 är att ge projekten ett redskap för att kunna genomföra ett IT-säkerhetsarkitekturarbete på ett effektivt sätt och med rätt resurser och på det sättet skapa ökade förutsättningar för att upphandla system med rätt kravbild.

Metodstödet för IT-Säkerhetsarkitekturarbetet omfattar:

- Denna metodbeskrivning
- Mall för ITSS 2.
- Mall för leverantörens nedbrytning av ITSS 2.

1.5 Basfakta

1.5.1 Begrepp och förkortningar

Begrepp/förkortning	Förklaring
GFE	Government Furnished Equipment – IT-säkerhetskomponenter tillhandahållna av FMV
ISD	Informationssäkerhetsdeklaration

Begrepp/förkortning	Förklaring
IT-säkerhet	Säkerhet beträffande IT-system, med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid data behandling samt dator- och telekommunikation.
IT-säkerhetsarkitektur	Övergripande teknisk beskrivning av i ett system ingående säkerhetstjänster, inklusive samverkan och gränssnitt, mellan olika komponenter
IT-säkerhetsfunktion	Specifik teknisk egenskap hos en systemkomponent som svarar för en viss del av säkerheten
IT-säkerhetskomponent	En IT-komponent som implementerar IT-säkerhetsfunktionalitet som del av ett IT-system
ITSS	IT-säkerhetsspecifikation
Krav på säkerhetsfunktioner	De krav i KSF som ska implementeras av IT-systemet dess operativa miljö eller båda i samverkan för att uppfylla säkerhetsmålen
SE	System Engineering

1.5.2 Referenser

Ref.	Dokumentnamn	Dok. id.
[1]	FMV Vägledning för ISD och SE	13FMV5921-3:4
[2]	Mall ITSS 2	13FMV5921-17:3
[3]	Metodbeskrivning Användningsfall	13FMV5921-8:3

2 Översikt av arbetet

2.1 Förutsättningar och principer

ITSS 2 är en del av systemets arkitekturbeskrivning och tillsammans beskriver de den övergripande strukturen på systemet. Då ITSS 2 är en del av kravställningen inför designlösningen måste ITSS 2 harmonisera med övrigt systemarbete för att såväl designbeslut samt beslut avseende IT-säkerhetsfunktioner ska få minsta möjliga påverkan på användbarhet och IT-säkerhet.

För att en relevant ITSS 2 ska kunna tas fram måste kravtolkning från både KSF och verksamhetens behov ur ett säkerhetsperspektiv vara fastställda. Det är också viktigt att ITSS 1 innehåller antaganden/beskrivningar avseende exponering av systemet.

IT-säkerhetskraven från den tekniska specifikationen ska allokeras till rätt IT-säkerhetsområde i ITSS 2.

2.2 Arbetsflöde

För att få en översikt av arbetet med framtagning av ITSS 2 visar *bild 2:1* ett arbetsflöde med ett antal arbetsmoment.

Varje moment presenteras här kortfattat för att i avsnitten 3 och 4 ge en mer detaljerad beskrivning. Rutorna i *bild 2:1* har ritats i olika storlekar för att relativt visualisera den uppskattade arbetsmängden i varje moment.

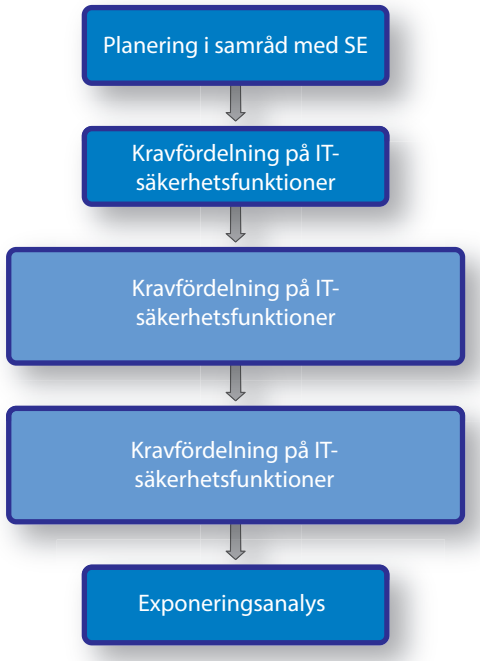

Bild 2:1 Översikt och flöde över arbetsmoment för framtagning av ITSS 2

2.2.1 Planering i samråd med SE (System Engineering)

I planeringsmomentet ska det säkerställas att all indata finns till projektet, främst i form av kravtolkning av FM krav från ITSS 1, men även andra förutsättningar som är av betydelse för arbetet.

Tidigare arbeten, ”best practises” samt goda exempel inhämtas där det är möjligt. Övergripande riktlinjer och designprinciper som ska gälla för IT-säkerhetsarkitektur arbetet bör fastställas, se *avsnitt 4.1* Planering av arbetet ska harmonisera med SE-funktionen för att integreras i övrigt designarbete, se *avsnitt 3.1*.

2.2.2 Kravfördelning på IT-säkerhetsfunktioner

I detta moment ska FMV:s tolkning av FM-krav brytas ner till IT-säkerhetskrav på systemet. Detta moment ställer krav på att det är känt hur systemet ska användas Därefter sker en kravallokering på olika IT-säkerhetsområden i ITSS 2, se även *avsnitt 4.2*. Kravallokeringen ska ske i nära samarbete med SE-funktionen.

2.2.3 Allokering av IT-säkerhetsfunktioner på systemet

De identifierade IT-säkerhetsfunktionerna allokeras på systemet ex på applikation, infrastruktur samt nät, se *avsnitt 4.3*.

2.2.4 Beskrivning av hur IT-säkerhetsfunktionerna används i systemet

I detta moment beskrivs hur IT-säkerhetsfunktionerna samverkar med varandra, med systemet samt visa på gränsytor som är dimensionerande för IT-säkerheten, se *avsnitt 4.4*. I detta moment sker själva designen IT-säkerhet integrerat med systemet.

Säkerhetsfunktionerna används också för att minska exponeringen av information. IT-säkerhetsarkitekturen används för att iterativt ta fram en övergripande design. Detta innebär att kravnivån kan minska. Här har första versionen av ITSS tagits fram som sedan prövas, se *avsnitt 0.0.1*.

2.2.5 Exponeringsanalys

I detta moment görs en exponeringsanalys av den tänkta IT-säkerhetsarkitekturen tillsammans med parter från SE-funktionen, IT-säkerhetsexperter samt, önskvärt, MUST. Denna exponeringsanalys syftar till att identifiera hur man kan minska exponeringen och vad detta får för konsekvenser i förändringar av designen och verksamhetsperspektiv. Projektetet återvänder till verksamheten för att identifiera och pröva alternativa lösningar där de identifierade konsekvenserna måste förankras i projektet och beställare. Vid behov genomförs aktiviteterna ovan igen i syfte att pröva exponeringen.

3 Förberedelser

3.1 Planering av arbetet med ITSS 2

Då en stor del av indata till ITSS 2 kommer från tidigare arbete i projektet, främst ITSS 1 är det viktigt att fastställa att en sådan finns. Om så inte är fallet, eller om den saknar delar behöver ett arbete initieras för att inhämta FMV-tolkning av FM:s krav. I det fall nuvarande projektdeltagare inte har deltagit i arbetet med ITSS 1 måste även projektet säkerställa att förståelse finns för ITSS 1.

Följande information ska inhämtas från ITSS 1:

- En FMV-tolkning av FM:s krav med spårbarhet mot TTEM, KSF samt verksamhetens behov ur ett säkerhetsperspektiv i form av exponering, informationssäkerhetsklass m m.
- FMV interna krav (om sådana finns).
- En beskrivning av systemet bestående av:
  - systembild
  - exponering mot externa system och användare
  - avgränsningar.

Finns användningsfall framtagna i verksamhetsbeskrivningen från Säkerhetsmålsättningsarbetet *[3]* kan de användas i arbetet.

Innan arbetet påbörjas ska även specifika designprinciper och riktlinjer för arbetet fastställas.

Efter insamling av förutsättningar planeras arbetet med framtagning av ITSS 2 med avseende på resurser och tidplaner mm. I planeringen bestäms också på vilket sätt arbetet ska genomföras.

3.1.1 Hur ska arbetet genomföras?

Planeringen av arbetet med framtagning av ITSS 2 ska göras i samverkan med övrigt SE-arbete. Det är viktigt att erbjuda MUST delaktighet i arbetet och då planera in avstämningsmöten.

Delar av arbetet med ITSS 2 lämpar sig speciellt att genomföras i workshops. Detta gäller främst vid beskrivandet av IT-säkerhetsfunktioner, *avsnitt 4.3* samt risk- och sårbarhetsanalysen, *avsnitt 4.4* där den stora fördelen med workshops är att det är ett effektivt sätt att samla en bred kompetens.

3.1.2 Inblandade resurser

Vid genomförandet av workshops ska IT- säkerhets- och systemarkitekten samverka eftersom framtagningen av ITSS 2 ska harmonisera med övrigt systemarbete.

Fastställande av designprinciper och riktlinjer görs tillsammans med SE-funktionen.

4 Genomförande

4.1 Kravfördelning på IT-säkerhetsfunktioner

4.1.1 Syfte

Syftet är att fastställa vilka IT-säkerhetsfunktioner som ska lösa ut vilka IT-säkerhetskrav för att systemet ska erhålla rätt IT-säkerhetsnivå i sin helhet.

4.1.2 Arbetsmetodik

En nerbrytning av de krav som finns i ITSS 1 görs i detta moment. 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. IT-säkerhetsfunktionerna överensstämmer till stor del med de delområden som finns i KSF 3 för att underlätta granskning mot de kraven. IT-säkerhetskraven blir en delmängd av den Tekniska specifikationen.

IT-säkerhetskraven fördelas på IT- säkerhetsfunktioner vilka återfinns i Mallen för ITSS 2 *[2]*. Är inte IT-säkerhetsfunktionerna tillämpliga ska detta motiveras.

- intrångs- och separationsmekanismer
- logghantering och säkerhetsloggar
- autentisering och behörigheter
- signalskydd
- IDS-funktionalitet
- informationshantering och backup
- skydd mot RÖS
- integritetsskydd
- avbrott (tillgänglighetsattacker)
- säkerhetsadministration
- skydd mot skadlig kod
- övrigt.

4.1.3 Resultat

Arbetet resulterar i IT-säkerhetskrav fördelade på IT-säkerhetsfunktion/er och utgör stommen till IT-säkerhetsarkitekturen.

4.2 Allokering av IT-säkerhetsfunktioner på systemet

4.2.1 Syfte

Skapa IT-säkerhetsarkitekturen genom att allokera de IT-säkerhetsfunktioner som identifierades i förra momentet, *avsnitt 4.1* till systemet. Detta moment ska också påvisa vilka systemets säkerhetskritiska delar är samt identifiera möjliga hotaktörer till systemet.

4.2.2 Arbetsmetodik

Allokering av IT-säkerhetsfunktionerna till systemet kan bli tydligare och mer överblickbar via bilder och vyer. Beskrivningar, bilder och vyer ska på ett tydligt sätt visa allokering mellan tekniska specifikationen och ITSS 2 samt påvisa vilka delar av systemet som är säkerhetskritiska.

Då en av IT-säkerhetsarkitekturens viktigaste funktioner är att säkerställa harmoniseringen mellan olika systems IT-säkerhetsfunktioner är det i detta skede viktigt att kartlägga hur liknande krav och funktioner brukar lösas. Detta kan inhämtas genom ”best practises” och goda exempel.

Identifiera:

- Möjliga hotaktörer till systemet, dess vilja och förmåga.
- Sårbarheter i systemet och vad som kan orsaka skada.
- Systemets säkerhetskritiska delar för att veta var säkerhetsfunktioner med hög assurans krävs.
- Tekniska IT-säkerhetsfunktioner som skyddar mot aktörerna samt fördela IT-säkerhetsfunktionerna på systemet och bestäm var de ska implementeras ex applikation, infrastruktur och kommunikation.
- Identifiera tillämpliga GFE (Government Furnished Equipment).

Arbetet med att identifiera de säkerhetskritiska komponenterna/gränsytorna ger även en indikation på om och på vilken delsystem/komponent en oberoende granskning ska genomföras. Detta blir sedan en kravställning på leverantören i upphandlingen.

Huvuddelen av arbetet med att beskriva IT-säkerhetsfunktionerna görs av IT-säkerhetsresurserna i projektet.

4.2.3 Resultat

En IT-säkerhetsarkitektur med IT-säkerhetsfunktioner identifierade, beskrivna samt integrerade i systemet. Säkerhetsfunktioner med hög assurans har identifierats samt tillämpliga GFE. Spårbarhet till teknisk specifikation och FMV-tolkning av FM-krav.

4.3 Beskrivning av hur IT-säkerhetsfunktionerna används i systemet

4.3.1 Syfte

Förstärka förståelsen för IT-säkerhetsarkitekturen genom att beskriva hur IT-säkerhetsfunktionerna är tänkta att användas, hur de interagerar med varandra och med systemet. Detta ger både en förståelse för övriga projektets arbete med systembeskrivningen samt för MUST vid en eventuell granskning.

4.3.2 Arbetsmetodik

Använda resultatet i föregående moment och ta fram beskrivningar för varje IT-säkerhetsfunktion.

4.3.3 Resultat

Beskrivning av hur IT-säkerhetsfunktionerna används, interagerar med varandra samt med systemet.

4.4 Risk- och sårbarhetsanalys med olika intressenter

4.4.1 Syfte

Kvalitetssäkra IT-säkerhetsarkitekturen tillsammans med intressenter till arbetet såsom ex SE-funktionen och önskvärt även MUST.

4.4.2 Arbetsmetodik

Detta arbete genomförs med fördel i workshop.

4.4.2.1 Förberedelser inför workshopen

De föregående momenten i processen ska vara utförda och de säkerhetskritiska områdena ska vara identifierade. Detta ska ingå som underlag inför workshopen och ska därmed skickas till samtliga deltagare.

Närvarande vid workshopen bör IT-säkerhetsexperter, personer med verksamhetserfarenhet samt systemarkitekt vara, dessa experter behöver inte vara en del av projektet utan kan vara sakkunniga under själva workshopen.

4.4.2.2 Genomförande av workshopen

Genomför en risk- och sårbarhetsanalys på det tänkta systemet med fokus på den tänkta tekniska krav/designen.

För att hålla ihop och leda workshopen behövs en moderator och en dedikerad resurs för dokumentation.

Tiden för genomförande varierar med komplexiteten men det är rimligt att anta att det minst tar en dag i anspråk.

Syftet med workshopen är att:

- Kvalitetssäkra säkerhetskritiska delar av systemet och därmed att kravställning kring assurans är rätt
- Kvalitetssäkra så att systemarbete och IT-säkerheten harmoniserar.
- Kvalitetssäkra att rätt IT-säkerhetsfunktioner allokeras till rätt del av systemet.
- Kvalitetssäkra att rätt konfigurerat GFE används.
- Identifiera frågeställningar.

Dokumentera löpande under hela workshopen.

4.4.2.3 Efterarbete

Det som har dokumenterats under workshopen renskrivs och genomgår eventuell efterbehandling för att lösa kvarvarande åtgärder.

Uppdatera upphandlingsunderlaget efter resultatet och skicka till samtliga deltagare på workshopen för synpunkter.

4.4.3 Resultat

Ett kravunderlag till upphandling omfattande en IT-säkerhetsarkitektur som harmoniserar med övrig systemarbete samt som uppfyller FM krav såväl från SM som KSF. Ifylld mall för ITSS 2 *[2]*.

Bilaga 1 Mallar

Följande mallar i word-format finns till Metodbeskrivning ITSS 2.

- *Mall för ITSS 2.*