<SYSTEM> <VERSION>
ISD-PLAN

Innehåll

Mallinformation 18FMV6730-3:1

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Mall för ISD-Plan	DAOLO

Mallinstruktion

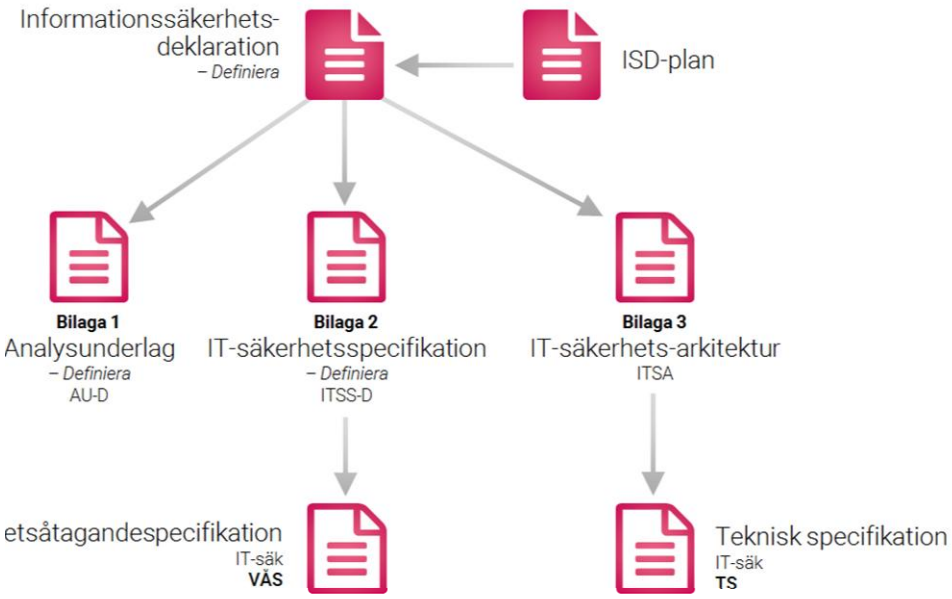
Denna mall ska användas för att ta fram dokumentet ISD-Plan.

Det skarpa dokumentet börjar med kapitel 1 Basfakta.

- Instruktionen om vad som ska stå under varje rubrik i det skarpa dokumentet anges i punktform. Den texten ska raderas innan dokumentet färdigställs.
- Text utan gulmarkering kan användas direkt i det färdigställda dokumentet.
- Ersätt Systemnamn med systemets namn.
- Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.

Omfattning av ISD-Plan

Informationssäkerhetsdeklaration *Definiera* (ISD-D) består av ett huvuddokument och tre bilagor. Huvuddokumentet utgör realiserbarhetsbedömning av IT-systemet, och ska enbart innehålla de faktorer som ligger till grund för bedömningen.



Figur 1 Dokumentstruktur Informationssäkerhetsdeklaration Definiera

ISD-plan, del av genomförandeprojektets projektplan, styr informationssäkerhetsarbetet och är en viktig styrning till dokumentet Informationssäkerhetsdeklaration *Definiera* ISD-D. Upphandlingsunderlagen (TS och VÅS) och ISD-plan är separata dokument och ingår inte i ISD 3.0.

ISD-planen klargör vilka aktiviteter som ska genomföras, i vilken omfattning ISD-processen ska användas och vilka roller som behövs. ISD-processen behöver inte alltid användas i sin helhet men det ska beskrivas vilka delar som avses användas och varför.

ISM ansvarar för framtagning av ISD-planen.

1 Basfakta

1.1 Giltighet och syfte

I detta avsnitt beskrivs syftet med aktuell ISD-plan. Exempel på syfte anges nedan.

Syftet med denna ISD-plan är att skapa en planering för det informationssäkerhetsarbete som krävs dels för att FMV ska kunna avge en IT-säkerhetsdeklaration till FM och dels för att förse underlag till FM för auktorisation och ackreditering.

Med IT-säkerhetsdeklaration avses:

- FMV tar designansvar för IT-säkerhetslösningen
- FMV uppfyller FM krav på informationssäkerheten och tolererbar risk
- Ackrediteringsdokumentation är utformad enligt den norm som gäller

Denna ISD-plan omfattar följande:

- Förutsättningar och avgränsningar
- Roller och ansvar
- Leveranser och tidplan
- Leverabler i varje leverans
- Aktiviteter för att ta fram varje leverabel
- Krav på säkerhetsarbete som krävs för att skapa ett säkert system

ISD-Planen styr genomförandeprojektets informationssäkerhetsarbete i faserna *Definiera* och *Realisera* enligt FMV VHL.

ISD-planen är att betrakta som ett förändligt objekt, så på grund av förändrade förutsättningar i genomförandeprojektet, kan denna ISD-plan behöva uppdateras.

1.2 Revisionshistorik

Datum	Utgåva Version	Beskrivning	Ansvarig

Tabell 1 - Revisionshistorik

1.3 Terminologi och begrepp

Följande tabell innehåller specifika begrepp som gäller för detta dokument. En generell lista återfinns i ref [1].

Term (förkortning)	Definition	Källa	Kommentarer/ Anmärkningar
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	

Tabell 2 - Terminologi och begrepp i detta dokument

1.4 Bilageförteckning

Detta dokument har inga bilagor.

1.5 Referenser

Dokumenttitel	Dokumentbeteckning, datum	Utgåva nr
[1] ISD 3.0 Begrepp och förkortningar	18FMV6730-8:1.1	1
[2] ISD-Processen 3.0	18FMV6730-8:1	1
[3] <Dokumentnamn>	<dokumentid., åååå-mm-dd>	<nr>

Tabell 3 - Referenser

2 Förutsättningar och principer för informationssäkerhetsarbetet

I detta avsnitt beskrivs de förutsättningar, principer och avgränsningar som gäller och påverkar det aktuella informationssäkerhetsarbetet. Nedan fokuseras förutsättningarna framförallt på områdena beroenden till andra system och samverkanspartners samt de kravunderlag från FM och FMV som krävs som input till IT-säkerhetsarbetet.

2.1 Principer

Detta avsnitt beskriver om det finns specifika principer/förhållningssätt till informationssäkerhetsarbetet. Ett exempel på principer kan vara att ISD-planen rör ett system av system där detaljerade ISD-planer tas fram för varje delsystem, där det aktuella systemet är ett övergripande system. Här kan också anges vad som måste krävas i form av underlag, beslut och leverabler m m för att gå vidare i informationssäkerhetsarbetet samt hur olika överlämningar av resultat ska ske.

Finns inte nödvändiga underlag ska det finnas en plan för hur dessa underlag ska tas fram.

Nr	Princip	Beskrivning	Referens

Tabell 4 - Principer

2.2 Avgränsningar

Detta avsnitt beskriver eventuella avgränsningar t ex om ISD-planen inte ska omfatta någon del av ett system.

Stöd till detta kapitel kan hämtas från ISD-Strategin.

2.3 Beroenden till andra system

Detta avsnitt ska beskriva hur beroenden ser ut till andra system. Flera aspekter är viktiga faktorer som kan påverka IT-säkerhetsarbetet såsom:

- Redan godkända komponenter/system/delsystem är en del av lösningen vilket påverkar de aktiviteter som behöver genomföras i IT-säkerhetsarbetet bland annat i form av analys av återbrukbarhet av dokumentation m m.
- Krav på godkännande från/till annat projekt/system. Det är viktigt att klargöra vem som har ansvar för godkännandet av ett system och framtagning av dokumentation i det fall system ska användas som utvecklas i annat projekt.

2.4 Beroenden till andra samverkanspartners

Detta avsnitt ska beskriva hur beroenden ser ut till andra samverkanspartners. Aspekter att ta hänsyn till är:

- Vilka krav på IT-säkerhet ställer samverkanspartners?
- Vilka krav på IT-säkerhet ställer FMV på samverkanspartners?

2.5 Kravunderlag från Försvarsmakten

De underlag som IT-säkerhetsarbetet ska baseras på från Försvarsmakten ska anges i detta avsnitt. Underlagen kan vara av olika styrande karaktär vilket också kan anges här. Vanliga underlag är:

- Systemmålsättning
- Säkerhetsmålsättning
- FM ITSS
- MUST KSF
- Beslut från FM
- Externa krav och beroenden såsom internationella krav och andra organisationers system
- Styrning av val av system/komponenter

Nr	Dokument	Dokumentnummer	Styrande

Tabell 5 – Kravunderlag från Försvarsmakten

2.6 Kravunderlag från FMV

De underlag som IT-säkerhetsarbetet ska baseras på från Försvarets materielverk ska anges i detta avsnitt. Exempel:

- ISD-Strategi
- vägledning för utveckling av säkra system
- instruktioner
- designregler
- mallar
- olika inriktningar
- styrning av val av system/komponenter

Nr	Dokument	Dokumentnummer	Styrande

Tabell 6 – Kravunderlag från FMV

3 Ackrediteringsobjekt

Detta avsnitt ska beskriva vilka systemdelar som ingår i ackrediteringsobjektet. Avsnittet ska också innehålla en bild över systemen och dess delsystem (om det är aktuellt med uppdelning/segmentering).

Beskrivningen ska vara på en övergripande nivå för att skapa en förståelse av aktuellt system och vilka delar som ingår i ackrediteringsobjektet. Den faktiska systembeskrivningen och verksamhetsbeskrivningen tas fram i andra aktiviteter och inte i ISD-planen.

3.1 Exponering

Detta avsnitt ska innehålla en övergripande bild över de tekniska externa beroenden som finns till ackrediteringsobjektet och som påverkar IT-säkerheten för systemet och dess exponering. Detta kan vara samverkan med andra system, krav på specifika protokoll och transmissionsmedia m m.

En mer detaljerad specifikation av externa gränssnitt sker i andra aktiviteter men denna beskrivning kan underlätta specificeringen av nödvändiga aktiviteter för IT-säkerhetsarbetet.

4 Utmaningar

Detta avsnitt ska beskriva vilka utmaningar som projektet identifierat att de kan ställas inför under projektets början. Kapitlet uppdateras även med de utmaningar som projektet kan stöta på under utvecklingens gång.

Utmaningar kan vara dimensionerade exponeringsfaktorer, ofullständig indata från FM, hantering av assuranskrav eller oklara ackrediteringsbeslut.

Ange en/flera planerade åtgärder för att hantera utmaningarna.

Nr	Utmaning	Åtgärd

Tabell 7 – Utmaningar

Observera att dimensionerande utmaning kan komma att utgöra en projektrisk, vilket ska analyseras i AU-D och redovisas i ISD-D.

5 Säkerhetsarbete

5.1 Roller och uppgift

Ett informationssäkerhetsarbete kräver ett antal roller med olika profiler för att täcka upp projektets behov. Samtliga nedanstående roller är Point of Contact (PoC) inom respektive område mot FM PROD, FM MUST och FMV SysGL IT-Säk.

En beskrivning av rollerna och deras aktiviteter i respektive fas i produktprocessen finns i beskrivning ISD-Processen 3.0 (referens [2]).

Normalt skall rollerna ISM, ISA, ISE och ISTM bemannas, men de kan också kombineras eller slås ihop beroende på ISD-arbetes omfattning.

5.1.1 ISM - Information Security Manager

Inom ISD för aktuellt projekt är följande individ utsedd till ISM. I de fall det finns flera individer som delar på ISM ansvar ska huvudansvarig PoC utses. Ange PoC med kryss i denna kolumn.

Roll	Namn	Organisation	PoC
ISM			

Tabell 8 – ISM

Om det förändras vilka individer som agerar ISM, ska denna ISD-Plan uppdateras.

5.1.2 ISA - Information Security Architect

Inom ISD för aktuellt projekt är följande individ utsedd till ISA. I de fall det finns flera individer som delar på ISA ansvar ska huvudansvarig PoC utses. Ange PoC med kryss i denna kolumn.

Roll	Namn	Organisation	PoC
ISA			

Tabell 9 – ISA

Om det förändras vilka individer som agerar ISA, ska denna ISD-Plan uppdateras.

5.1.3 ISE - Information Security Evaluator

Inom ISD för aktuellt projekt är följande individ utsedd till ISE. I de fall det finns flera individer som delar på ISE ansvar ska huvudansvarig PoC utses. Ange PoC med kryss i denna kolumn.

Roll	Namn	Organisation	PoC
ISE			

Tabell 10 – ISE

Om det förändras vilka individer som agerar ISE, ska denna ISD-Plan uppdateras.

5.1.4 ISTM - Information Security Test Manager

Inom ISD för aktuellt projekt är följande individ utsedd till ISTM. I de fall det finns flera individer som delar på ISTM ansvar ska huvudansvarig PoC utses. Ange PoC med kryss i denna kolumn.

Roll	Namn	Organisation	PoC
ISTM			

Tabell 11 – ISTM

Om det förändras vilka individer som agerar ISTM, ska denna ISD-Plan uppdateras.

5.2 Behov av intern samverkan

Ett IT-säkerhetsarbete kräver nära samarbete med andra delar i ett projekt för att IT-säkerhetsfunktionerna på ett integrerat sätt ska implementeras i systemet. Olika sätt att designa systemet kan påverka hur IT-säkerhetsfunktionerna ska implementeras.

Detta avsnitt beskriver de roller som är aktuella att samarbeta med samt vilka arbetsuppgifter rollerna har.

Exempel på samverkan:

- Projektledare (PL) – för att minimera risker för produkten i ett tidigt skede. Samverkan sker med ISM.
- SE, System Engeneering – systemutformning - för att kunna avgöra om och hur designval påverkar säkerhetsfunktionaliteten i produkten. Samverkan sker med ISA.
- Produktion (internprojekt)
- Förvaltning – för att kunna från början ta hänsyn till hur systemet är tänkt att förvaltas/vidmakthålla. Samverkan sker med ISM.
- Systemsäkerhet –där systemet har höga krav på systemsäkerhet. Samverkan sker med ISA.
- Verifiering och Validering – planering och samverkan för verifiering och validering av IT-säkerhetsarbetet. Samverkan sker med ISM.

5.3 Behov av extern samverkan

Detta avsnitt beskriver samverkan med de externa samverkanspartners utanför projektet men som har eller kommer att ha en påverkan på IT-säkerhetsarbetet.

Exempel på externa samarbetspartners är:

- Industri – samverkan sker i enlighet med av FMV kravställd VÅS
- FM MUST – Det ska beskrivas när och under vilka former samverkan med MUST ska ske. Syftet är att tidigt planera in granskning av artefakter under hela utvecklingsprocessen.
- Internationella samarbetspartners i enlighet med upprättade avtal
- Samverkan ska ske med andra delar på FMV som utvecklar system
- Andra projekt inom egen domän i de fall samverkan ska ske med system/produkter utvecklade inom annan domän

5.4 Rutiner för ändringshantering, uppföljning och leverans

5.4.1 Ändringshanteringsprocess

Detta avsnitt ska beskriva processen för ändringshantering, uppföljning och leverans. Styrande är att varje ändring i designen ska redovisas i en ändringshanteringsgrupp.

För varje ändrings ska en bedömning göras huruvida ändringen är säkerhetspåverkande och i så fall i vilken grad, eller ej.

Ändringshanteringsprocessen ska också beskriva vem som är ansvarig, vem bedömer, fattar beslut och dokumenterar ändringar samt hur ändringar påverkar IT-säkerheten i systemet. Dessutom ska det beskrivas hur bedömningen integreras i övrig ändringshantering i projektet för att rätt beslut ska kunna fattas och dokumenteras.

5.4.2 Uppföljningsprocess

Uppföljningsprocessen ska bland annat beskriva vad som ska följas upp och vem som har ansvar för IT-säkerhetsarbetet i syfte att säkerställa kvalité.

5.4.3 Leveransprocess

Leveransprocessen ska beskriva under vilka former leverans ska genomföras av de artefakter som enligt denna ISD-Plan tas fram inom projektet.

Avsnittet ska också beskriva vem som godkänner dessa artefakter för leverans, t ex FMV CCB.

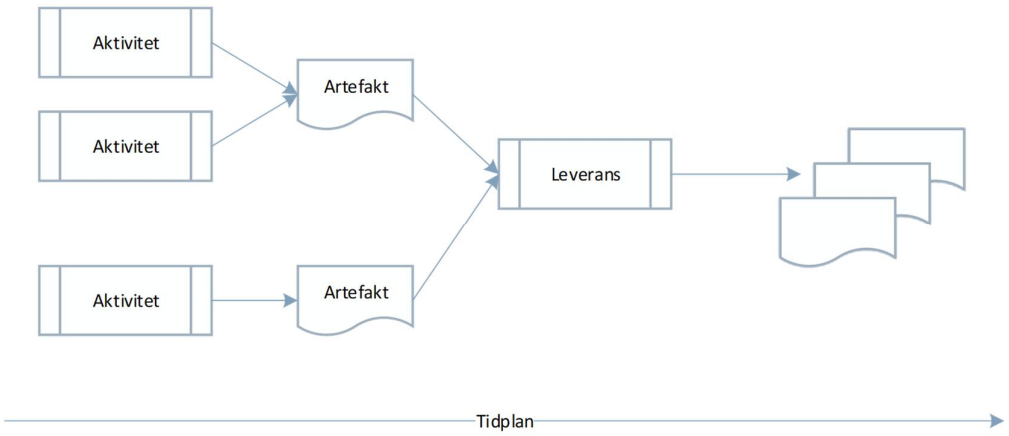
6 Artefakter

Detta avsnitt ska beskriva vilka leveranser som ska göras för IT-säkerhetsarbetet, vilka artefakter som är kopplade till vilka leveranser samt vilka aktiviteter som krävs för att ta fram identifierade artefakter samt när i tiden dessa aktiviteter och artefakter ska göras/finnas. En generell beskrivning av vilka aktiviteter som ska genomföras och vilka artefakter som ska tas fram finns i beskrivning ISD-Processen 3.0 (referens [2]). Denna generella beskrivning ska i detta kapitel anpassas för att stödja det aktuella genomförandeprojektet.

Leveranserna ska integreras med projektets leveranser, vilket innebär att tidplanen för informationssäkerhetsarbetet ska korrelera med projektets huvudtidplan. Ansvarig för detta är ISM.

Detta avsnitt ska beskriva de artefakter och aktiviteter som konkret formar informationssäkerheten i det aktuella ackrediteringsobjektet och dess dokumentation för att kunna genomföra ackreditering.

Följande figur illustrerar sambandet mellan aktivitet, artefakt och leverans. Detta ska också korrelera med ISD tidplan och projektets tidplan.



Figur 2 Aktiviteter, artefakter och leveranser

6.1 Leveranser

Genomförandeprojektet för <system> <version> avser att genomföra följande leveranser inom ramen för informationssäkerhetsarbetet.

Nr	Leverans	Innehåll

Tabell 12 – Leveranser

6.2 Artefakter

6.2.1 Kravidentifiering

Ange vilka artefakter som projektet avser att ta fram inom ramen för kravidentifiering. Typiska artefakter är ISD-I med AU-I och ITSS-I.

6.2.2 Kravnedbrytning/arkitektur

Ange vilka artefakter som projektet avser att ta fram inom ramen för kravarbete och framtagning av säkerhetsarkitektur. Typiska artefakter är ISD-D med AU-D, ITSS-D och ITSA.

Här ska också anges vilka artefakter som används för att dokumentera funktionella respektive icke-funktionella säkerhetskrav. Typiskt görs detta i TS respektive VÅS/SoW. Observera att de krav i TS och VÅS/SoW som härstammar ur ISD-arbetet ska arbetas in i projektets TS respektive VÅS/SoW.

6.2.3 Kravanalys

Ange vilka artefakter som projektet avser att ta fram inom ramen för analys av kravuppfyllnad och testverksamhet. Typiska artefakter är ISD-R med AU-R och ITSS-R.

6.2.4 Säkerhetstester

Ange vilka artefakter som projektet avser att ta fram inom ramen för säkerhetstester i syfte att verifiera och eventuellt komplettera analys av kravuppfyllnaden.

6.2.5 Leverans FM

Ange vilka artefakter som projektet avser att leverera till FM. Typiska artefakter är ISD, ISD-R med AU-R, ITSS-R och VMH-R.

6.2.6 Övriga underlag

Ange vilka övriga artefakter som tas fram inom ISD-arbetet. Exempel på detta är separata analysunderlag, utredning, osv.

6.3 Aktiviteter och tidplan

Generellt sett är följande aktiviteter obligatoriska i ISD-arbetet:

- Underbyggt underlag för realiserbarhetsbedömningar
- Spårbarhet i kravarbetet
- Dokumenterade designbeslut
- Spårbarhet i granskning av kravuppfyllnad
- Deklaration av säkerhetslösningen

-

6.3.1 Obligatoriska aktiviteter

Följande aktiviteter är obligatoriska i *Definiera*-fasen:

- Ackrediteringsobjektet ska definieras tillsammans med systemgräns, systemkontext och krav på omgivningen
- Tolkning av FM MUST KSF samt tillkommande krav ska göras
- Säkerhetsarkitektur (ITSA) ska vara integrerad i systemets systemarkitektur
- Projektet ska bedöma behovet av oberoende granskning t.ex. avseende penetrationstest
- ITSS-D ska tas fram för att dokumentera kravhanteringen

- ITSA ska tas fram för att dokumentera kravallokeringen
- ISD-D ska tas fram för att dokumentera realiserbarhetsbedömningen inför S3-beslut
- Krav till TS och VÅS avseende informationssäkerhet ska specificeras

Innan *Definiera* har genomförts ska projektet bedöma risken för att systemet inte blir ackrediterbart, vilket är förutsättning för *Realisera*.

Följande aktiviteter är obligatoriska i *Realisera*-fasen:

- ITSS-R ska tas fram för ISE granskning av kravuppfyllandet avseende systemet
- AU-R ska tas fram för ISE granskning av assuranskraven
- VMH-R ska tas fram för att dokumentera krav på användning inför BOAC
- ISD-R ska tas fram för att dokumentera realiserbarhetsbedömningen inför S4-beslut
- ISD ska tas fram för att deklarera uppfyllande av säkerhetsmålen

6.3.2 Planlagda aktiviteter

Ange identifierade aktiviteter samt vilken roll som är ansvarig för dessa, inklusive stödjande roller.

Aktivitet	Artefakt	Ansvarig	Stöd

Tabell 13 – Aktiviteter

Ansvarig och stöd i tabeller ovan ska vara någon av de definierade rollerna ISM, ISA, ISE eller ISTM.

6.3.3 Granskningar

Ange vilken roll som ska granska ISD-artefakterna i genomförandeprojektet. Typisk granskare är SystGL IT-Säk alternativt SystG IT-Säk.

6.3.4 Tidplan

Ange uppskattad tidplan för framtagning av leverabler.

Leverabel	Uppskattad tidplan

Tabell 14 – Tidplan

Observera att tidsplaneringen ovan måste korrelerar med projektets tidplan, och kan komma att uppdateras under projektets livscykel i faserna *Definiera* och *Realisera*.