Metodbeskrivning för framtagning av
ISD/ISU-plan

ISD/ISU-plan

Tryck:

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	2014-05-30	Mindre uppdateringar med avseende på begrepp och förtydliganden	DAOLO
2.0	2013-10-29	Uppdaterad med ny bild avseende processen. Hänvisning till bedömd omfattning i sidor borttaget. I avsnittet tillämpning av ISD är det förtydligat att ISD-planen styr omfattning på arbetet.	DAOLO
1.0	2013-05-14	Uppdaterad med intern samverkan VoV	DAOLO

Innehåll

1 METODSTÖD ISD-PLAN

1.1 SYFTE MED ISD-PLAN

ISD-planen är en del av projektplaneringen vars syfte är att skapa en planering, prioritering och budgetering för det IT-säkerhetsarbete 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.

1.2 NYTTAN

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.

1.3 TILLÄMPNING

Dokumentet *FMV Vägledning för ISD och SE, 13FMV5921-1:3* beskriver hur ISD-planen ska tillämpas. ISD-planen styr omfattningen på IT-säkerhetsarbetet och vilka moment i ISD-processen som är tillämpliga.

1.4 FÖRUTSÄTTNINGAR OCH UTMANINGAR

För projektets styrning ska ISD-planen klargöra resurser, förutsättningar, utmaningar, artefakter med mera så att FMV kan göra en IT-säkerhetsdeklaration. Med IT-säkerhetsdeklaration avses att:

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

ISD-planen resulterar i ett antal leverabler som används för att kunna ange en IT-säkerhetsdeklaration för aktuellt system, och vad som krävs för IT-säkerhetsarbetet. Efter viss justering med mer detaljer skulle denna kunna användas även för ISU-plan (industrins plan för IT-säkerhetsarbete som resulterar i ett IT-säkerhetsutlåtande).

Nedan visas ISD-processen, som ligger till grund för ISD-planen, inklusive ansvarsförhållanden avseende leverabler. *Bild 1:1* visar också de leverabler som blir resultatet i varje fas. Finns inte relevant indata inför respektive fas ska detta resultera i aktiviteter i ISD-planen.

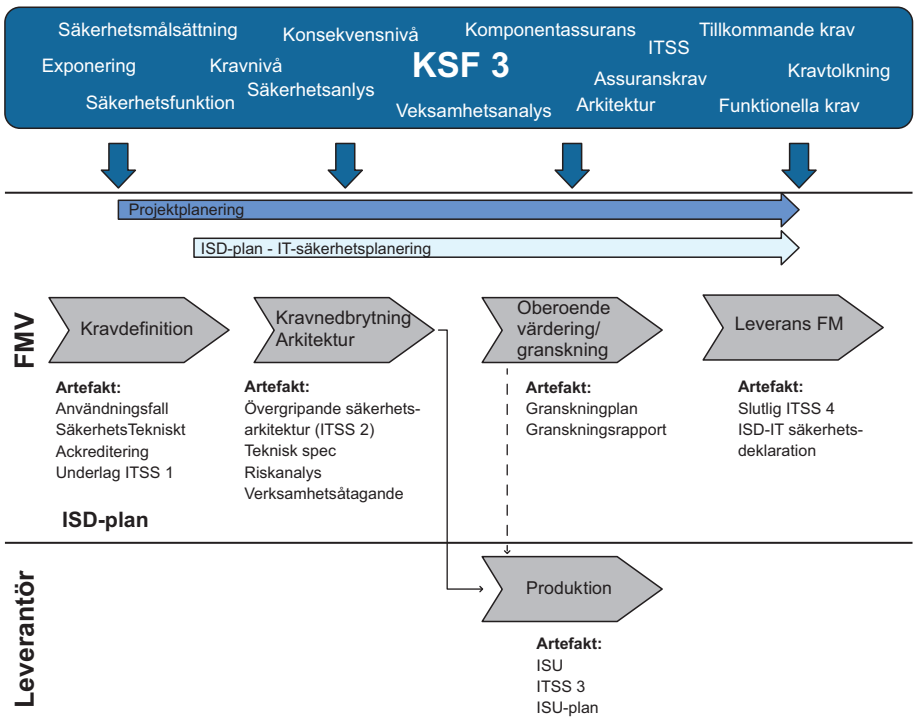


Bild 1:1 ISD-processen med ansvarsfördelning

Inriktning från systemledningen avseende IT-säkerhetsarbetet omfattar planen från systemledningen innan projektstart. Systemledningen beskriver hur olika system hänger ihop så att utveckling, verifiering mm levereras som en helhet. En tanke är att den även ska kunna användas så att MUST kan planera in granskningstider för sina resurser över projektens livscykel.

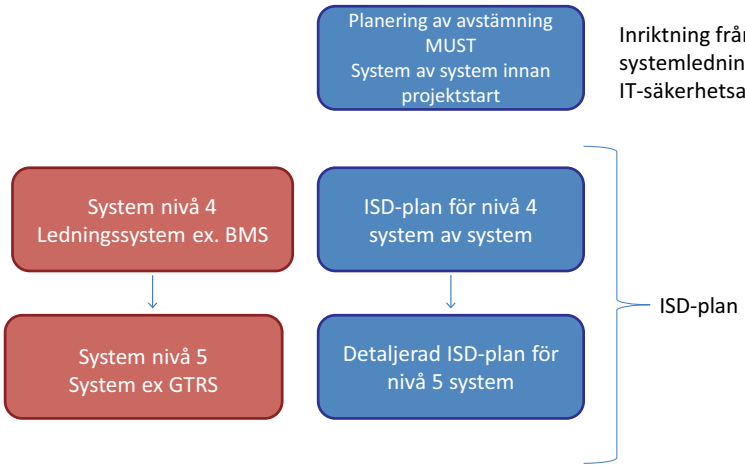


Bild 1:2 ISD-plan i nivåer

1.5 FÖRBEREDELSER

PL är ansvarig för att ta fram ISD-planen, med fördel tillsammans med rollen Information Security Manager som beskrivs i *avsnitt 2.4.1*. I takt med att projektet genomgår respektive fas, se *avsnitt 1.3*, konsulteras ansvariga resurser för respektive leverabel i de olika faserna samt övriga externa samverkansparter i projektet såsom ansvarig för kravarbete, design och test. Säkerställ i tidigt skede, via planen, samverkan med MUST och bestäm i tiden när granskningar kan genomföras.

1.6 GENOMFÖRANDE

Input till ISD-plan kan inhämtas dels från inriktningen från systemledningen avseende IT-säkerhetsarbete och dels från TTEM och verksamhetens behov från ett säkerhetsperspektiv. ISD-plan kan med fördel göras i olika nivåer beroende på vilken systemnivå som är i fokus. Är det system av system görs en planering på övergripande nivå medan mer detaljplanering görs i detaljerad ISD-plan.

Hur arbetet startar beror på i vilken fas projektet befinner sig.

IT-säkerhetsarbetet finns med från start och följande aktiviteter är relevanta:

Finns tillräckligt med information från Försvarsmakten för att kunna genomföra ett IT-säkerhetsarbete i projektet? Till stöd används checklista för att värdera indatat från FM. Exempel på ingångsvärden är Säkerhetsmålsättning inklusive verksamhetsbeskrivning. Finns inte tillräcklig information, är det prioriterat att kartlägga vad som saknas och att planera aktiviteter för att få fram information.

Ta fram en första version av ISD-plan, omfattning enligt *1.5*. Projektet behöver genomföra ett arbete i ITSS1 för att veta vad som ska utföras i ISD-planen. Initialt är ISD-planen en övergripande beskrivning med detaljer kring aktiviteter som påverkar tidiga leveranser. ISD-planen utvecklas kontinuerligt med mer detaljer och olika fokus i takt med systemets utveckling i förhållande till dess livscykel. ISD-planen integreras i projektplanen och versionshantering görs i samråd med SystGL. Dessutom kan ISD-planen behöva ses över i samband med ISD-deklarationen.

Ta beslut att genomföra IT-säkerhetsarbetet enligt ISD-plan.

Projektet har pågått en tid och det finns ett antal leverabler.

ISD-planen ska tas fram redan i kravdefinitionsfasen men det är aldrig försent att göra en plan. I det fall projektet har pågått görs en bedömning vad som måste tas fram för att kvalitetssäkra leveransen till FMV.

Efter nulägesanalysen så planeras och initieras aktiviteter för att säkra de leverabler som behövs för leveransen till Försvarsmakten.

1.7 OMFATTNING

För att säkerställa IT-säkerhetsarbetet som krävs för att utveckla säkra system ska ISD-planen minimum omfattar följande områden:

- Förutsättningar och avgränsningar.
- Utmaningar i IT-säkerhetsarbetet till exempel i form av exponering.
- Roller och ansvar.
- Leveranser och tidplan.
- Leverabler som krävs i varje leverans.
- Aktiviteter som krävs för att ta fram varje leverabel.
- Krav på säkerhetsarbete som krävs för att skapa ett säkert system.

ISD-planen ska hållas relativt kortfattad och behovet avgör omfattningen. Vid komplexa system kan det vara värt att dela upp det i flera underliggande ISD-planer istället för ett omfattande.

1.8 BEGREPP OCH FÖRKORTNINGAR

Förkortning	Förklaring
AK	Anskaffningskontor
BMS	Battle Management System
GTRS	Gemensamt Taktiskt Radio System
ISD-plan	IT-SäkerhetsDeklaration Plan för IT-säkerhetsarbetet enligt ISD- process
ISU-plan	IT-SäkerhetsUtlåtande Industrins motsvarighet till ISD-plan
SI-IA	Systemingenjör - Information Assurance
ITSS	IT-säkerhetsspecifikation

2 MALL FÖR ISD-/ISU-PLAN

2.1 INLEDNING

Detta är en mall för framtagning av ISD-/ISU-plan. Kursiv text är stödtext och hjälp för att fylla i ISD-ISU-planen. Medan övrig text ska kunna användas för det färdiga dokumentet. Följs mallen ska en färdig ISD-/ISU-plan erhållas.

Försättsbladet ska innehålla rubrik, fastställande av Chefsingenjör samt i förekommande fall godkännande av produktledare, med plats för deras underskrifter.

Denna plan omfattar ISD-/ISU-plan för IT-säkerhetsarbetet för *system xxxxx*.

2.1.1 Mål

Få kontroll över IT-säkerhetsarbetet i tidigt skede för *system xxxxx* så att rätt resurser, rätt indata m m kan sättas in i rätt skeden i processen. Det ska vara möjligt att redovisa den aktuella statusen för IT-säkerhetsarbetet i alla faser i projektets ISD-process.

2.1.2 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, prioritering och budgetering för det IT-säkerhetsarbete 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.
- Ackrediteringsarbetet följer ISD-plan.

2.1.3 Omfattning

För att skapa en första överblick ska detta avsnitt beskriva den aktuella ISD-planens omfattning.

Denna ISD-plan omfattar följande:

- Förutsättningar och avgränsningar.
- Utmaningar i IT-säkerhetsarbetet till exempel i form av exponering.
- 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.

2.1.4 Referenser

I detta avsnitt anges relevanta referenser för ISD-/ISU-planen.

2.1.5 Förkortningar och begrepp

Detta avsnitt ska beskriva den aktuella ISD-planens förkortningar och begrepp.

2.2 Förutsättningar och utmaningar för IT-säkerhetsarbetet

I detta avsnitt beskrivs de förutsättningar, utmaningar och avgränsningar som gäller och påverkar det aktuella IT-säkerhetsarbetet. 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.

2.2.1 Principer

Detta avsnitt beskriver om det finns specifika principer/förhållningssätt till IT-säkerhetsarbetet. Ett exempel på principer kan vara att ISD-planen rör ett system av system där detaljerade ISD-planer tas fram för varje delsystem, 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 IT-säkerhetsarbetet samt hur olika överlämningar av resultat ska ske.

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

Hänvisningar till projekts processer exempel utvecklingsprocesser som ska integreras med mera.

2.2.2 Avgränsningar

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

2.2.3 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 med mera.
- 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.

2.2.4 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?

2.2.5 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:

- Säkerhetsmålsättning.
- ITSS i de fall KSF ska användas.
- MUST KSF.
- Beslut från auktorisationsgruppen.
- Externa krav och beroenden såsom internationella krav och andra organisationers system.
- Styrning av val av system/komponenter.

2.2.6 Kravunderlag från FMV

De underlag som IT-säkerhetsarbetet ska baseras på från Försvarets materielverk ska anges i detta avsnitt. Exempel kan vara olika inriktningar som finns från ISD och SE såsom

- FMV Vägledning ISD och SE
- metodstöd
- instruktioner
- designregler
- mallar
- olika inriktningar
- styrning av val av system/komponenter.

2.3 ACKREDITERINGSOBJEKT

Detta avsnitt ska benämna vilka systemdelar som ingår i ackrediteringsobjektet. Avsnittet kan också innehålla en bild över systemen och dess delsystem. Det ska poängteras att 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.

2.3.1 Exponering

Detta avsnitt ska vara en övergripande bild över de tekniska externa beroenden som finns till ackrediteringsobjektet och som påverkar IT-säkerheten för systemet och dess exponering såsom 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.

2.3.2 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.

2.4 SÄKERHETSARBETE

2.4.1 Roller och uppgift

Ett IT-säkerhetsarbete kräver ett antal roller med olika profiler för att täcka upp IT-säkerhetsarbetets behov. Samtliga nedanstående roller är Point of Contact (PoC) inom respektive område mot MUST och SystGL:

- Ansvarig för helhetsarbetet (ackrediteringen) kan kallas Information Security Manager. Rollen bör vara medlem i projektledningen (dock inte projektledare) för att minimera risker för produkten i ett tidigt skede.
- Ansvarig för designarbetet för IT-säkerhet, kan kallas Information Security Architect.
- Ansvarig för verifiering (planering, genomförande och dokumentation) av kravställda säkerhetstester, Information Security Test Manager.

Uppgifterna som anges nedan är styrande. Tillägg kan göras men avsteg ska motiveras.

2.4.1.1 Information Security Manager

Uppgifterna för den roll som har ansvar för helheten (ovan kallad Information Security Manager) ska beskrivas i detta avsnitt.

Information Security Manager har bland annat följande uppgifter:

- Vara kontaktperson i säkerhetsfrågor i projektet, mot beställare samt andra externa gränsytor.
- Koordinera IT-säkerhetsarbetet och det arbete som sker i ISD-processen.
- Koordinera IT-säkerhetsarbetet i projektet och lyfta säkerhetsfrågorna till projektledning.
- Leda arbetet med riskhantering såväl för produkt som för projekt. Ansvarig är projektledare vilket förutsätter engagemang från projektet.
- Krav på verksamhetsåtagande, kan delegeras till Information Security Architect.
- Leda arbetet med projektsäkerhet. Ansvarig är projektledare vilket förutsätter engagemang från projektet.

2.4.1.2 Information Security Architect

Uppgifterna för den roll som har ansvar för designarbetet (ovan kallad Information Security Architect) ska beskrivas i detta avsnitt.

Information Security Architect har bland annat följande uppgifter:

- Säkerställa samstämmighet mellan den tekniska specifikationen och IT-säkerhetsarkitektur för systemet.
- Ansvara för kravnedbrytning från Säkerhetsmålsättning alternativt framtagning av användningsfall och KSF och harmonisera verksamhetens krav med MUST KSF.
- Ansvara för en övergripande IT-säkerhetsarkitektur.

2.4.1.3 Information Security Test Manager

Uppgifterna för den roll som har ansvar för testverksamheten (ovan kallad Information Security Test Manager) ska beskrivas i detta avsnitt.

Information Security Test Manager har bland annat följande uppgifter:

- Koordinera säkerhetstester så att de stämmer överens med det totala VoV-arbetet.
- Initiera säkerhetstester- oberoende värdering. Genomförs enligt processen inkluderande; Förberedelse, genomförande och uppföljning.

  Säkerhetstester är:

  – penetrationstester
  – funktionstester
  – kryptoverifiering
  – dokumentationskvalité.
- Ställa krav på säkerhetstester i samband med andra relevanta funktionella tester och specificera vilka frågor man vill ha svar på i ett säkerhetsperspektiv.

2.4.2 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. Nedan ges exempel på i projektet aktuella samverkanspartners.

Detta avsnitt ska beskriva behovet och formen för samverkan.

Exempel på samverkan:

- Projektledare (PL)– för att minimera risker för produkten i ett tidigt skede. Samverkan sker med Information Security Manager.
- SE System Engeneering – systemutformning - för att kunna avgöra om och hur designval påverkar säkerhetsfunktionaliteten i produkten. Samverkan sker med Information Security Architect.
- Produktion (internprojekt) – för att samverka kring aspekter som tas upp i *avsnitt 2.2.1*.
- Förvaltning – för att kunna från början ta hänsyn till hur systemet är tänkt att förvaltas. Samverkan sker med Information Security Manager.
- Systemsäkerhet – åtminstone i de fall där systemet har höga krav på system-säkerhet.
- Verifiering och Validering – planering och samverkan för verifiering och validering av IT-säkerhetsarbetet för samtliga faser.

2.4.3 Externa behov av 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 enligt av FMV kravställt verksamhetsåtagande och enligt ISU-plan.
- MUST – Det ska beskrivas när och under vilka former samverkan med MUST ska ske. Syftet är att tidigt planera in granskning av leverabler under hela utvecklingsprocessen.
- Internationella samarbetspartners i enlighet med upprättade avtal.
- Samverkan ska ske med andra delar på FMV som utvecklarsystem.
- Andra projekt inom egen domän i de fall samverkan ska ske med system/produkter utvecklade inom domän exempelvis LUFT.

2.4.4 Finansiering

För att rollerna i *avsnitt 2.4.1* ska kunna styra IT-säkerhetsarbetet i olika delprojekt behövs resurser (personer och ekonomi). Detta avsnitt ska redogöra för tillgängliga resurser för deras uppgift.

2.4.5 Rutiner för ändringshantering, uppföljning och leverans

2.4.5.1 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.

2.4.5.2 Uppföljningsprocess

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

2.4.5.3 Leveransprocess

Leveransprocessen ska beskriva under vilka former leverans ska genomföras av de leverabler som är output från ISD-planen. Avsnittet ska också beskriva vem som godkänner leverabler för leverans, t ex FMV CCB.

2.5 ARTEFAKTER

Detta avsnitt ska beskriva vilka leveranser som ska göras för IT-säkerhetsarbetet, vilka leverabler som är kopplade till vilka leveranser samt vilka aktiviteter som krävs för att ta fram identifierade leverabler.

Leveranserna ska integreras med projektets leveranser. Detta avsnitt ska beskriva de leverabler och aktiviteter som konkret formar IT-säkerheten i det aktuella ackrediteringsobjektet och dess dokumentation för att kunna genomföra ackreditering.

2.5.1 Leveranser

Detta avsnitt ska beskriva vilka leveranser som ska genomföras i projektet.

Leveranser för ISD-planen är ISD-processens faser enligt *avsnitt 1.1*

- kravdefinition
- kravnedbrytning/arkitektur
- produktion
- leverans FM.

Leveranser/milstolpar för ISD-processens produktionsfas är enligt Verksamhetsåtagandet och beskrivs i ISU-plan.

2.5.2 Leverabler

Detta avsnitt anger de leverabler som ingår i respektive leverans. Leverablerna som är angivna nedan är kopplade till ISD-processen enligt *avsnitt 1.1*.

2.5.2.1 Kravdefinition

Omfattar leverablerna ISD-plan och ITSS 1 (risker och TTEM). ISD-plan är enligt denna mall. ITSS är ett dokument som beskriver resultatet från analys av Säkerhetsmålsättning alternativt användningsfall och TTEM. Syftet med ITSS 1 är att ge förutsättningar för vilka aktiviteter som ska finnas med i ISD-planen. ITSS 1 ska innehålla en beskrivning av säkerhetsfunktionaliteten i systemet på en övergripande nivå samt spårbarhet mot TTEM och Säkerhetsmålsättning alternativt användningsfall samt identifierade risker.

2.5.2.2 Kravnedbrytning/Arkitektur

Omfattar leverablerna ITSS 2 Säkerhetsarkitektur, Teknisk specifikation och Verksamhetsåtagande. ITSS 2 beskriver den övergripande IT-säkerhetsarkitekturen för det aktuella systemet för att tillsammans med Teknisk specifikation (som är en nedbrytning dels från användningsfall och dels av MUST KSF) utgöra kraven till produktion. Den övergripande IT-säkerhetsarkitekturen är en designansats som hanteras vidare av industrin enligt kravställt verksamhetsåtagande.

Verksamhetsåtagande beskriver kraven på det åtagande som leverantören ska vara ansvarig för i processen såsom roller, ändringshantering, nedbrytning av säkerhetsarkitektur samt testverksamhet.

2.5.2.3 Leverans FM

Omfattar leverablerna ITSS 4 och ISD.

ITSS 4 är huvuddokumentet och Executive Summary 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.

2.5.2.4 ISD – IT-säkerhetsdeklaration

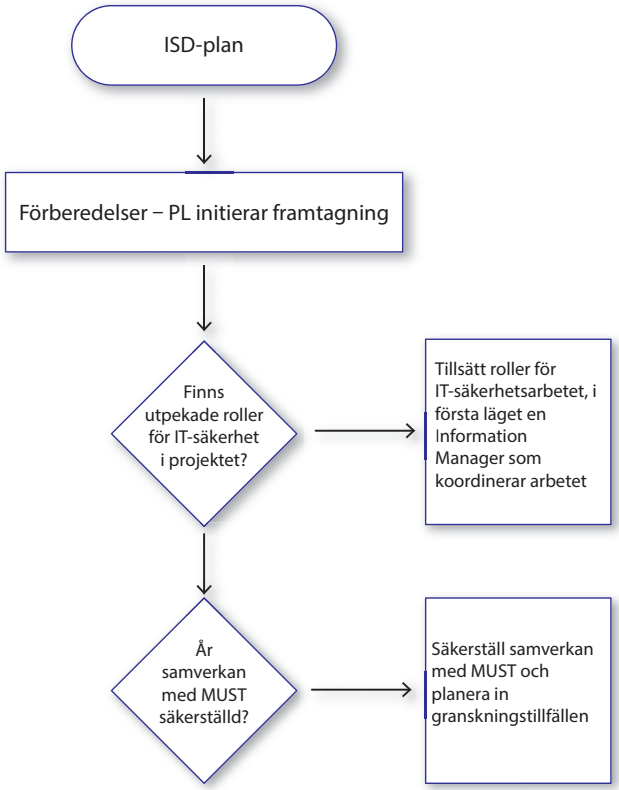
ISD är en deklaration där FMV deklarerar sitt designansvar för IT-säkerhetslösningen, kravuppfyllnad mot försvarsmaktens krav samt dokumentationen är utformad enligt gällande norm. Grunden för ISD är ITSS 4, vilket innebär att STAU 4 innehåller de bevis och granskningar som har genomförts.

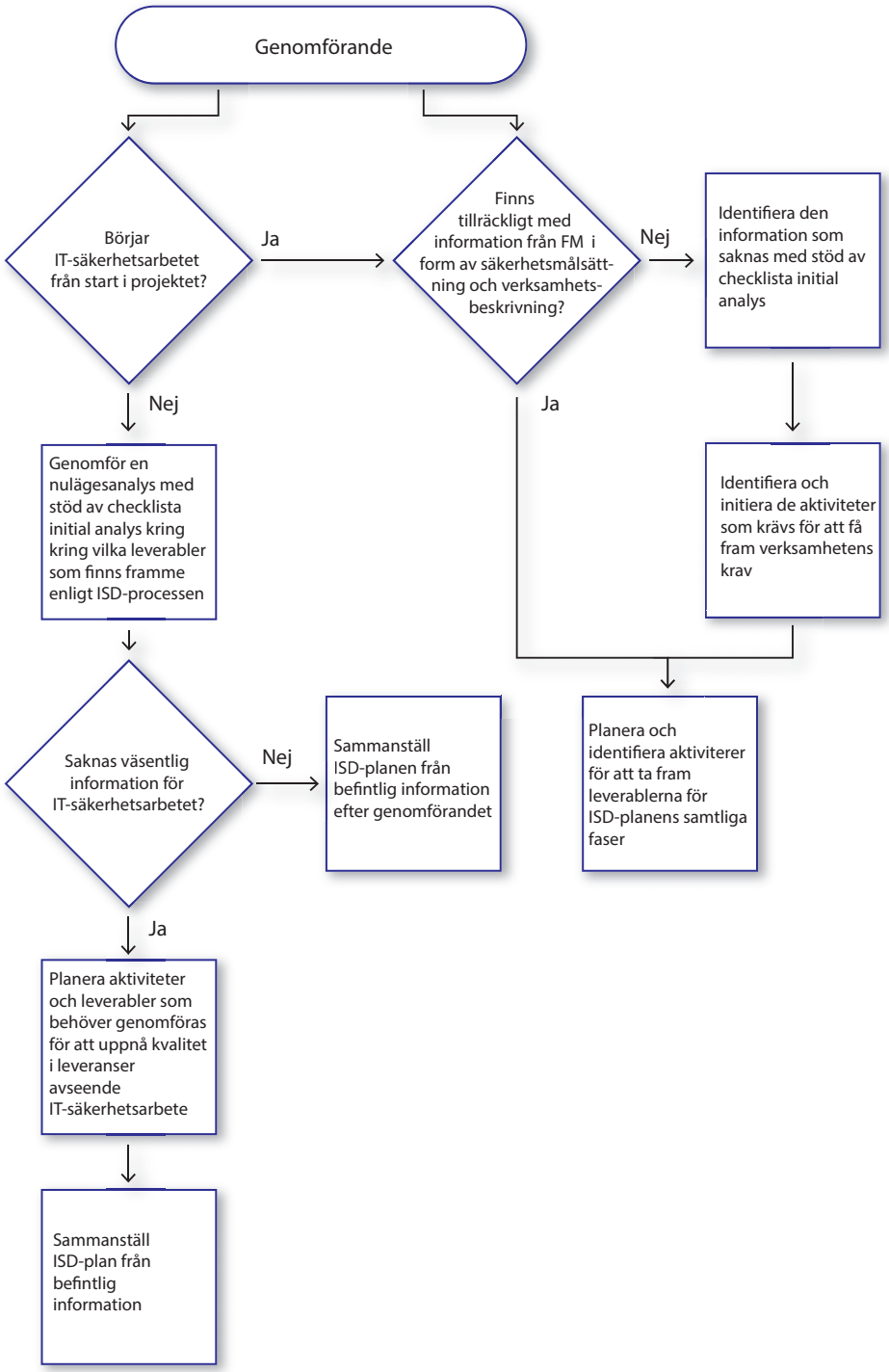
2.5.3 Aktiviteter

I detta avsnitt beskrivs de aktiviteter som måste genomföras för att få fram identifierade leverabler och, vem som är ansvarig för att genomföra aktiviteterna. Exempel på aktiviteter är:

- Aktiviteter som måste genomföras för att kunna ta fram nödvändiga leverabler för IT-säkerhetsarbetet och därmed till ackrediteringsarbetet såsom
  - framtagning av ISD-plan
  - workshop för framtagning av verksamhetens behov
  - kravnedbrytning
  - designarbete
  - med mera.
- Behov av granskningsaktiviteter – evalueringar.
- Krav och behov av oberoende granskning.
- Tidplan.

Bilaga 1 Flödesbeskrivning




Genomförande
Börjar IT-säkerhetsarbetet från start i projektet?
Ja
Finns tillräckligt med information från FM i form av säkerhetsmålsättning och verksamhetsbeskrivning?
Nej
Identifiera den information som saknas med stöd av checklista initial analys
Nej
Ja
Genomför en nulägesanalys med stöd av checklista initial analys kring kring vilka leverabler som finns framme enligt ISD-processen
Identifiera och initiera de aktiviteter som krävs för att få fram verksamhetens krav
Saknas väsentlig information för IT-säkerhetsarbetet?
Nej
Sammanställ ISD-planen från befintlig information efter genomförandet
Planera och identifiera aktiviterer för att ta fram leverablerna för ISD-planens samtliga faser
Ja
Planera aktiviteter och leverabler som behöver genomföras för att uppnå kvalitet i leveranser avseende IT-säkerhetsarbete
Sammanställ ISD-plan från befintlig information

Bilaga 2 Mallar

I den digitala utgåvan finns följande word-mall

- Mall för ISD-/ISU-plan.

Chefsingenjör ska skriva under den färdiga ISD-/ISU-planen.