Erfarenheter från arbete med oberoende granskning och ISD metodstöd.

FÖRSVARETS MATERIELVERK

Innehåll

[1 Inledning 3](#_Toc417544255)

[1.1 Referenser 3](#_Toc417544256)

[2 ISD-processen generellt 4](#_Toc417544257)

[2.1 Projektarbetet 4](#_Toc417544258)

[3 ISD-plan 5](#_Toc417544259)

[3.1 Beskrivning av ackrediteringsobjektet och dess gränsytor 6](#_Toc417544260)

[3.2 Hänsyn till tidigare beslut och styrande dokument 6](#_Toc417544261)

[3.3 ISD-planen över tiden 7](#_Toc417544262)

[3.4 Uppfyllnad av ISD-plan 7](#_Toc417544263)

[4 Säkerhetsmålsättning/Användnings fall 8](#_Toc417544264)

[5 STAU1 8](#_Toc417544265)

[6 STAU2 8](#_Toc417544266)

[7 VÅS 9](#_Toc417544267)

[8 ISU 9](#_Toc417544268)

[9 STAU3 9](#_Toc417544269)

[10 STAU4 9](#_Toc417544270)

[11 ISD 10](#_Toc417544271)

[12 Granskning 10](#_Toc417544272)

[13 genomfört IT-säkerhetsarbete 11](#_Toc417544273)

# Inledning

Detta dokument beskriver erfarenheter som har erhållits av ISD-metodstöd genom arbete med ISD-processen såväl som granskningsinstans som under utövande av stöd för ISD i projekt.

Dokumentet berör följande delar ur ISD-processen:

* ISD-processen generellt
* ISD-plan
* STAU1
* STAU2
* STAU4
* ISD

Om andra delar ur ISD-processen anges beror detta på beroenden som bedömts finnas. Efterhand erfarenheter fås från alla delar i ISD-processen införs dessa i denna erfarenhetsrapport.

Rapporten ska stödjas av en matris[[1]](#footnote-1) i vilken olika typer av uppdrag beskrivs och lämpliga åtgärder för hur IT-säkerheten bör hanteras i uppdraget. Detta för att få en rimlig nivå på insatsen samt då vilka specifika underlag som ska/bör tas fram för det enskilda uppdraget. Det viktigaste i ISD-processen är att tidigt definiera Ackrediteringsobjektet och den Exponering som uppstår med stöd av användarfall i den miljö som systemet/produkten ska användas i. Vid granskning av underlag ingående i ISD-processen ska tydlig beskrivning av ackrediteringsobjektet och hur användning och omgivning (exponering) särskilt beaktas. För uppdrag av typen ”System-av-system” finns initialt ett väsentligt och gränssättande behov av att utifrån verksamhetens användarfall och miljöförutsättningar (säkerhetsmålsättning motsvarande) få korrekta underlag för vilka delsystem och/eller komponenter som har beslut och förutsättningar för att kunna brukas inom det angivna uppdraget.

I de uppdrag av typen System-av-system som varit föremål för granskning och/eller ISD-stöd har det visat sig ett stort behov av metodstöd för att omhänderta de gränssättande förutsättningar som denna uppdragstyp innebär. Det är väsentligt att i uppdragsställningen medge utrymme för att designa lösningar utifrån vilka förutsättningar som ingående delar har mot de krav som verksamheten och dess tänkta miljö ställer. Av dessa erfarenheter har ett specifikt metodarbete gjorts i syfte att stödja och guida uppdragstypen ”System-av-system” genom ISD-processen fram till att FMV ska kunna avge en ISD till FM för ett till uppgift och miljö anpassat sammansatt system. Stödet är utformat som metodbeskrivning, metodanvisning med tillhörande checklistor specifikt utformade till denna uppdragstyp, [Ref 1, 2].

## Referenser

[Ref 1] Metodstöd för uppdrag System-av-system

[Ref 2] Checklistor med analysstöd[[2]](#footnote-2)

[Ref 3] Matris (xls), ISD uppdragsformer och krav på underlag[[3]](#footnote-3)

# ISD-processen generellt

## Projektarbetet

ISD-processen ska utgöra stöd för IT-säkerhetsarbetet i projekt. Processen ska anpassas till att stödja projekt där kompetensen för IT-säkerhetsarbete inte är så stor och där IT-säkerhetsarbetet inte har varit en självklar del. Processen ska belysa behovet och stödja genomförandet av det IT-säkerhetsarbete som krävs i det specifika projektet för att kunna överlämna dess resultat till FM.

Metoden avser att med stöd av beskrivningar, mallar, checklistor etc. stödja projekten med att initialt (tidigt) analyser och planera för hur IT-säkerhetsarbetet ska fortgå, vilka resurser som krävs och vilka leverabler som uppdraget ska innehålla. Detta samt roller och ansvar anges i en ISD-plan som granskas och fastställs av FMV. Projektledare driver nu med stöd av ISD-planen, IT-säkerhetsarbetet på ett tillräckligt strukturerat sätt. En bidragande orsak är att underlagen har metodstöd, mallar och granskas och att en del av dessa ska skrivas på av Teknisk Chef. Funktionen SystGL som ska finnas spridd och kopplad till olika verksamhetsområden understödjer projekten i ISD-processen och granskar underlag som ska skrivas på.

Det är positivt att roller i projektet tydliggörs i och med ISD-planen. ISD Metodstöd skapar förutsättningar för spårbarhet och bra kvalitet i IT-säkerhetsarbetet. Granskningar genomförs i syfte att förtydliga vad som ska göras och att krav och uppfyllnad av krav dokumenteras på ett för beslutsfattare och betraktare tydligt och spårbart sätt. ISD-processen ger förutom stöd för det projektinterna arbetet även bra förutsättningar för det färdiga systemets dokumentation och beslut för att kunna brukas i andra sammanhang alternativt utvecklas då behov uppstår. Erfarenheter har visat att system och/eller komponentutveckling bör/ska ta hänsyn till vilka användningsområden och miljöer som kan tänkas för att i utvecklingsarbetet skapa förutsättningar för uppdrag av typen ”System-av-system”. Detta kräver en kraftfullare initial analys innan uppdraget avgränsas och specificeras. Metodstöd [Ref 1, 2] stödjer detta arbetssätt.

Det är dock otydligt hur ISD-processen interagerar med FM:s IT-process, (IT-styrmodellen). Här är det viktigt att tumregler fastställs. Som exempel ges följande förslag:

* Finns en gällande tidigare fastställd säkerhetsmålsättning används DIT04.
* Finns ingen säkerhetsmålsättning framtagen genomförs FMVs användningsfall.
* Genomförs projekt enligt ISD-processen så finns tillräckliga underlag inför beslut

# ISD-plan

Mer och mer inses vikten av att ta fram ISD-plan för det IT-säkerhetsarbete som ska genomföras. Fortfarande är det ibland lite för komplicerat och inte tydligt en plan utan en beskrivning hur av systemet ser ut. IT-säkerhetsarbetet ska planeras i ISD-planen för att kunna omhänderta uppsatta, granskade och fastställda krav på säkerhet föranledd av den informationsmängd samt infrastruktur som verksamheten kräver i den miljö där verksamheten ska bedrivas. Vi måste trycka på att ISD-planen är en plan och att i den ska vad som ska göras tydligt beskrivas. Hur detta görs får senare verifieras mot de krav som gäller för denna lösning och/eller åtgärd i STAU och då slutligen i STAU 4.

Förslag på förbättringar och förtydliganden i metodbeskrivning och mallar är:

* Inför metodstöd ”System-av-system” med tillhörande checklistor i ISD metodstöd
* Tillför de delar av erfarenhetsrapporteringen som utgör stöd för utvecklingsprojekten
* Att tydliggöra ackrediteringsobjektet är väldigt viktigt och det sparar tid och pengar i slutänden. Hur detta kan göras kan ytterligare beskrivas i mall och metodbeskrivning
* Projekten är inte så bra på att anpassa ISD-planen efter vad som faktiskt ska göras i projektet. Den första utgåvan tenderar att bli för komplex. Metoder och mallar bör utvecklas och innehålla stöd och information kring detta. ISD-planen ska beskriva hur man avser att bedriva säkerhetsarbetet i det aktuella projektet, vilka leverabler som anses behövas av de som finns angivna i ISD-processen etc.
* Ta med i metodbeskrivningen och mallarna att det är viktigt att läsa in de tidigare besluten som fattats
* Om STAU 1 finns ta med den i granskningen av ISD-planen. STAU 1 och ISD-planen ska stämma
* ISD-plan och Säkerhetsskyddsplan ska alltid finnas tillhands (inte i arkivet)

Förslag på insattser och åtgärder för att stödja och utveckla IT-säkerheten i projekten:

* Informera och utbilda kontinuerligt om ISD-processen och kopplingen till FM behov
* Stöd projekten initialt så att ISD-planen blir praktisk och täckande
* Delge erfarenheter tidigt så att uppdragsställningar medger att uppdraget kan genomföras på ett resurs och tidsekonomiskt sätt (speciellt system-av-system)
* Dokumentera i underlagen till var i ISD-planen dessa hör för bättre spårbarhet
* Följ upp arbetet mot ISD-planen och dokumentera avsteg av vikt

## Beskrivning av ackrediteringsobjektet och dess gränsytor

Erfarenheter som har dragits från genomförda granskningar är att överlag så brister planerna när det gäller att beskriva själva ackrediteringsobjektet och dess gränsytor. Även i de projekt där Combitech har tagit fram ISD-planer har det varit svårt att från projektledare få fram vad ackrediteringsobjektet består av. Först efter det att projektet har pågått en tid har det framkommit vad det egentliga ackrediteringsobjektet är och då har ISD-planen behövt revideras. I vissa fall har ett relativt komplext ackrediteringsobjekt med flertalet gränsytor beskrivits från början där det visade sig efter hand att med rätt avgränsning blev uppgiften mycket enklare. Slutsatsen är att det är viktigt att klargöra ackrediteringsobjektet i början, det kan spara mycket tid och även pengar.

Förslag till förbättring:

För att få fram bra ingångsvärden för ISD-plan kan STAU1 behöva tas fram parallellt eftersom det i den görs en kravtolkning baserat på verksamhetsbeskrivning och säkerhetsanalys.

I samband med STAU1 ges en tydligare bild kring gränsytor och miljö och användandet av systemet vilket också tydligare ger utmaningar och förutsättningar. Metodbeskrivning och mallar kan tydliggöra ytterligare vad det är för information som måste fram avseende ackrediteringsobjektet.

Matris som angivits i kap 1 ska visa på utifrån uppdraget typ[[4]](#footnote-4) vilka underlag som ska och kan tas fram samt vilka underlag som behövs som källa och referenser till dessa.

## Hänsyn till tidigare beslut och styrande dokument

Det är viktigt att i ackrediteringsarbetet, speciellt vid uppdateringar av ett redan ackrediterat system, ta hänsyn till tidigare beslut. Detsamma gäller att ha kontroll på vilka styrande dokument som har varit del i utvecklingen.

Kring uppdrag av typen ”System-av-system” framkommer ständigt behov av spårbara dokumenterade beslut om auktorisation och dess villkor. Vid utveckling av nya system och/eller komponenter eller vidareutveckling av befintliga system behöver påpekas att underlag och beslut med villkor ska utformas så att dessa kan bedömmas utifrån möjligheten att brukas direkt eller behov av förändring/beslut för att ingå i kommande utveckling av ”System-av-system”. Det har varit svårt/omöjligt att sammantaget få ett användbart (korrekt) underlag på vad delsystem och/eller komponenter är godkända för. Någon form av databas med gällande status måste finnas tillgänglig för att bedöma förutsättningar för uppdragen ”System-av-system”.

Förslag till förbättring:

I mallarna och i metodbeskrivningen skriva in de mest vanliga grundläggande dokument som ska tas hänsyn till innan ett ackrediteringsarbete genomförs.

I metodbeskrivningen för ISD-planen finnas med vilka frågor man ska ställa när man ska komma igång. I dessa ingår då även vilka krav en omgivande struktur (omgivande system, användarfall och verksamhetsmiljö) kan komma att ställa på just detta ”delsystem och/eller komponent”

## ISD-planen över tiden

Arbetet med ISD-processen på FMV är relativt nytt och man är inte ännu så bra på att anpassa ISD-planen mot vad som ska göras i projektet över tiden. Den första utgåvan är ofta lite mer komplicerad än nödvändig, även för ”enklare” ackrediteringsobjekt. Ju längre in i projektet arbetet kommer desto klokare blir man kring IT-säkerhetsarbetet och ISD-planen kan behöva justeringar. En risk finns att ISD-planen det blir något som görs i början av uppdraget och sedan blir en hyllvärmare. Lösningen är att utforma varje ISD-plan individuellt och tydligt så att den utgör ett verkligt stöd för projektets IT-säkerhetsarbete.

Förslag till förbättring:

Uppdatera metodbeskrivningen med uppmaningen till ett levande dokument och att ett analysarbete görs innan ISD-plan upprättas. En matris i xls.-format är framtagen som stöd för vilka underlag som bör göras i olika typer av uppdrag [Ref 3].

Det kanske ska finnas med i mallen om FMV ska vara leverantör eller beställare.

## Uppfyllnad av ISD-plan

Under IT-säkerhetsarbetet utförs de i ISD-planen angivna åtgärderna och underlag tas fram. Tider, åtgärder, förändringar och tillägg till ISD-planen blir den dokumentation som med rapporter från granskningar och tester samt STAU 4 stödjer FMV:s avgivande av ISD. Inriktning är att STAU genomgående ska användas och att då genomfört IT-säkerhetsarbete bäst beskrivs genom en granskad STAU 4 i tillämliga delar.

Avvikelse: En Rapport över genomfört IT-säkerhetsarbetet utgående från hur ISD-planen såg ut gjordes i samband med avgivande av ISD för ett uppdrag innehållande programvaror tillhörande sensorer avsedda för FM Hälso & Sjukvårdssystem. Metodansvarig ISD är av den åsikten att detta fungerade men skapade ytterligare underlag som bara var lämpligt i vissa uppdragstyper.

Förslag till förbättring:

Skapa inget nytt underlag (Rapport över genomfört IT-säkerhetsarbete) utan använd STAU 4 i tillämpliga delar. I ISD ska det tydligt framgå att projektet följt den Fastställda ISD-planen och om avvikelser skett ska det framgå vad som inte genomförts enligt Fastställd ISD-plan och varför samt vilka ”konsekvenser” detta medfört. Rapporter från granskningar och tester bifogas för att Styrka ISD tillsammans med STAU4. STAU 4 kan då beroende på komplexitet och nivå av säkerhet variera betydligt i omfattning. För förståelse och spårbarhet (främst för omgivning och framtida utveckling) ska samma typ av dokument och med samma benämning användas.

# Säkerhetsmålsättning/Användnings fall

Kvaliteten på användningsfall är ibland inte i enlighet med det som krävs för att få fram IT-säkerhetsaspekter för systemet. Metodstödet för användningsfall har heller inte använts i så stor utsträckning än.

Förslag på förbättring:

Det skulle kunna tydliggöras i metodbeskrivningen var i mallarna man kan hitta informationen kring exponering (externa gränsytor, typ av användare, internationell samverkan mm). Kanske en checklista som stöd? Se exempel i metodstöd System-av-system.

# STAU1

Bra som research. Det kommer fram saker i STAU1 arbetet som det kanske måste till en aktivitet för projektet, ex det kanske saknas något för att ta fram STAU1. Saknas det något ska det finnas en aktivitet i ISD-planen för att få fram informationen. Det kan hända att man behöver interagera mellan dessa två ett antal gånger.

STAU 1 ska normalt alltid finnas för att utgöra det dokument varifrån information var kraven hämtas ska finnas. Det är särskilt viktigt att inhämta vid vidareutveckling och behov av förändringar (tillägg till beslut).

Förslag på förbättring:

Utveckal ISD-planen och STAU 1 mer parallellt och befäst konsistensen mellan dessa underlag.

Ta alltid fram en STAU 1 för ett uppdrag oavsett hur enkelt det framstår.

# STAU2

STAU2 blir mer och mer viktig för framtiden och för användandet av KSF 3. I och med att den tekniska arkitekturen blir en viktig parameter för att hitta rätt kravnivå enligt KSF 3.1 kan det finnas en fördel med att ta fram STAU2 och låta den driva fram de tekniska kraven som ska skrivas in i den tekniska specifikationen. I befintlig metodbeskrivning tas den tekniska specifikationen fram och sen gör en kravallokering av IT-säkerhetskraven på en IT-arkitektur. Denna tanke har även framkommit i IT-säkerhetsarbetet i projekt Sweccis.

Förslag på förbättring:

Tillägg till metodbeskrivning; skriv in avstämning med MUST. I alla utvecklingsuppdrag innehållande ISD-processen ska underlaget STAU1/2 finnas för att dokumenterat spåra från STAU4 som även finns i alla dessa uppdrag som slutprodukt och stöd för att avge en ISD. Kraven i SATU 2 ska föras in i specifikation samt i SoW som underlag för leverantör. STAU 2 är spårbarheten varifrån dessa krav kommer. Infoga hjälptext för att föra över krav från STAU 2 till TS samt SoW.

# VÅS

Det som står i Vägledning ISD och SE behöver utvecklas ytterligare i separat metodstöd. Metodstödet skulle kunna vara genetisk för alla projekt. I ISD-processen poängteras det att detta är viktigt för att få bra kvalitet från leverantören avseende IT-säkerhetsarbete. Därför är det viktigt att metodstöd finns.

Förslag på förbättring:

Färdigställ mallar och utveckla texten för VÅS i vägledningen.

# ISU

Ingen erfarenhet från verksamheter.

Förslag på förbättring:

En granskningsvägledning med vad som ska deklareras och hur skrivningen ska se ut för att utgöra ett tydligt och bindande/tillförlitligt underlag (leverantörens IT-säkerhetsutlåtande).

Mall i likhet med ISD bör tas fram och tydligt ange vad det är som utlåtandet avser samt hur detta ska utformas.

# STAU3

Ibland är FMV själva leverantörer av system och i det fallet är frågan om det ska fram en STAU3 eller om det ska direkt ta fram en STAU4. Hittills få erfarenheter av detta så viktiga underlag som utgör fakta som stöd för ISU och som efter granskning (FMV verifiering av kravuppfyllnad) ska utgöra underlaget för STAU 4. Om extern leverantör så får de kraven via TS och SoW. STAU 3 kan i de fallen behöva stöd till leverantören för att skapa goda förutsättningar för STAU 4.

Förslag på förbättring:

Samverkan med leverantören och stöd för att få ett tydligt och bra underlag för STAU 4. Ska vid behov styras tydligt i ISD-planen under principer alternativt dokumenteras i Rapport genomfört IT-säkerhetsarbete. Utveckla metodbeskrivning hur försäkra god spårbarhet mellan STAU 2 via TS och SoW till STAU 3 och slutligen FMV:s STAU 4.

# STAU4

STAU4 är relativt lätt för projekten att förhålla sig till eftersom det är likt gamla TAU. Det upplevs som en kvalitetshöjning på arbetet. Eftersom ISD-processen innebär att man arbetar metodiskt och har arbetat igenom kravtolkning, kravnedbrytning blir arbetet ”enklare” när man arbetar med STAU4.

Förslag på förbättring:

ITSS – tydliggör relationen mellan STAU och ITSS.

Förtydliga i metodbeskrivningen vad som ska beskrivas i STAU4 om det rör sig om en förändring av systemet samt om en deltaanalys är genomförd.

# ISD

Erfarenheten är att projekten inte vet hur deklarationen ska skrivas. Det är ytterst viktigt att punkterna som ska ingå i ISD verkligen utgör det som krävs samt är tydligt verifierade i texten. ISD ska stödjas av lämpliga underlag/dokument.

En del av de tidigare ISD har innehållit mer information då detta har funnits behov för. I denna har även erfarenheter redovisats under en punkt ”Erfarenhetsåtermatning”. Detta för att förbättra och förtydliga processen och dess underlag samt ge dokumenterade förklaringar för varför åtgärder gjort eller inte gjorts. Ett sådant exempel är Ledsyst MALI som till stor del utgör erfarenheter av uppdrag av typen ”System-av-system”.

Förslag på förbättring:

-En tydligare mall och förslag på vilka punkter en ISD kan innehålla och hur texten bör formuleras.

-I mallen peka på exempel som kan vara ytterligheter och/eller förslag/exempel på vad som ansetts tillföra processen information i överlämnandet till FM.

# Granskning

Detta stycke avser den granskning av underlag som genomförs av funktionen Syst GL för att kunna författa ett yttrande till TC före dennes fastställande av ISD-plan och ISD.

Granskningsprotokollet:

Spårbarhet till yttrandets punkter, Dokumentation, Metodik, Kravhantering och Teknik.

Ge positiva synpunkter och förslag på innehåll och förbättringar i projektets dokumentation vid kommentarer i protokollet.

Finns inga exempel och projektet inte förstår alt inte håller med så blir det ingen åtgärd.

Alternativ granskning:

Om granskning med anmärkningar inte ger önskvärt resultat eller är svåra att utforma på ett entydigt sätt kan metoden workshop var en lösning att förmedla synpunkter och upprätta underlaget med. Workshop har bl.a. används för uppdragen Ledsyst MALI samt DSTI.

Syst GL yttrande/rekommendation till TC

Den text som finns i yttrandet ska kunna spåras till granskningsprotokollet och innehålla kriterier för rekommendation i SystGL bedömning som stöd till TC för påskrift/avgivande av ISD.

Förslag på förbättring:

-Entydighet i granskningsprotokoll och på vems uppdrag granskning ska ske (PL eller SystGL)

-Versionshantering av protokoll och upphovsman för anmärkningar samt hur synpunkter är omhändertagna fram till påskrift av TC.

-Tydligare och mer informativ/konstruktiva åtgärdsförslag för att underlätta för PL. PL har ju ändå ansvaret för innehållet och genomförandet i projektet.

# genomfört IT-säkerhetsarbete

ISD-planen görs initialt, fasställs och uppdateras eventuellt efterhand och vid behov, dock är det en plan. I STAU 4 som ska bära sig själv beskrivs vilka och hur angivna säkerhetsmål är uppfyllda. I STAU 4 återfinns de brister som kvarstår utgående från att alla mål ska vara uppfyllda och med förslag på hur dessa ska hanteras. I ISD som FMV avger till FM ska det tydligt framgå att arbetet följt den fastställda ISD-planen, att säkerhetsmålen är uppfyllda, de kvarvarande bristerna redovisas med förslag på åtgärder och att FMV anser att det som levereras till FM är utvecklat och framtaget på ett för FM godkänt vis. ISD styrks av STAU 4 till vilken bifogas rapporter från i uppdraget genomförda granskningar och tester.

1. xls.matris (tabell) med definierade uppdragtyper, dess behov av underlag försedda med tips och erfarenheter [↑](#footnote-ref-1)
2. Tillhör Metodstöd [Ref 1] och införas i ”ISD Vägledning ISD och VoV” under ”Checklistor VoV och granskning” [↑](#footnote-ref-2)
3. Matris visande styrningar/förslag på vilka underlag som ska tas fram för olika typer av uppdrag [↑](#footnote-ref-3)
4. Olika typer av uppdrag från Utveckling av nya system – godkännandet av befintliga programvaror har olika behov av framtagning av underlag enligt ISD-processen samt av underlag som SYD, gransknings- och test-rapporter etc. [↑](#footnote-ref-4)