<SYSTEM> <VERSION>ISD-PLAN

Innehåll

[Mallinformation 4](#_Toc72305167)

[Versionshistorik för mallen 4](#_Toc72305168)

[Generell mallinstruktion 4](#_Toc72305169)

[Specifik mallinstruktion 4](#_Toc72305170)

[Dokumentstruktur Definiera-fasen 5](#_Toc72305171)

[Att tänka på i arbetet med framtagning av ISD-plan 5](#_Toc72305172)

[1 Basfakta 6](#_Toc72305173)

[1.1 Giltighet och version 6](#_Toc72305174)

[1.2 Terminologi 6](#_Toc72305175)

[1.3 Referenser 6](#_Toc72305176)

[1.4 Bilagor 7](#_Toc72305177)

[2 Inledning 8](#_Toc72305178)

[2.1 Syfte 8](#_Toc72305179)

[2.2 Informationssystemets referens 8](#_Toc72305180)

[3 Förutsättningar 9](#_Toc72305181)

[3.1 Styrande förutsättningar 9](#_Toc72305182)

[3.2 Avgränsningar 9](#_Toc72305183)

[3.3 Beroenden till andra tekniska system 10](#_Toc72305184)

[3.4 Beroenden till samverkanspartners 10](#_Toc72305185)

[3.5 Kravunderlag från Försvarsmakten 10](#_Toc72305186)

[3.6 Kravunderlag från FMV 11](#_Toc72305187)

[4 Ackrediteringsobjektet 13](#_Toc72305188)

[4.1 Definition av ackrediteringsobjektet 13](#_Toc72305189)

[4.2 Gränsytor och deras exponering 13](#_Toc72305190)

[5 Utmaningar 15](#_Toc72305191)

[6 Informationssäkerhetsarbete 17](#_Toc72305192)

[6.1 Tillsättning av ISD-roller 17](#_Toc72305193)

[6.2 Behov av intern samverkan 17](#_Toc72305194)

[6.3 Behov av extern samverkan 18](#_Toc72305195)

[6.4 Rutiner 18](#_Toc72305196)

[6.4.1 Projektsäkerhetsskydd 18](#_Toc72305197)

[6.4.2 Riskhantering 19](#_Toc72305198)

[6.4.3 Ändringshantering 19](#_Toc72305199)

[6.4.4 Progressuppföljning 19](#_Toc72305200)

[6.4.5 Dokumenthantering 19](#_Toc72305201)

[6.4.6 Kvalitetssäkring 20](#_Toc72305202)

[6.4.7 Leveransprocess 20](#_Toc72305203)

[7 Aktiviteter och tidplan 21](#_Toc72305204)

[7.1 Artefakter 21](#_Toc72305205)

[7.1.1 Kravnedbrytning och arkitektur 21](#_Toc72305206)

[7.1.2 Kravanalys 21](#_Toc72305207)

[7.1.3 Säkerhetstester 22](#_Toc72305208)

[7.1.4 Leverans till Försvarsmakten 22](#_Toc72305209)

[7.1.5 Övriga underlag 22](#_Toc72305210)

[7.2 Leveranser 22](#_Toc72305211)

[7.3 Aktiviteter 22](#_Toc72305212)

[7.4 Tidplan 25](#_Toc72305213)

# Mallinformation

## Versionshistorik för mallen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Datum | Version | Beskrivning | Ansvarig | Fastställd |
| 2021-05-18 | 1.0 | ISD 3.1 | Ulf Christensen |  |

## Generell mallinstruktion

* Detta kapitel är information om mallen och anvisningar avsedda att hjälpa författaren. Kapitlet ska raderas i sin helhet innan dokumentet färdigställs.
* Röd text (som denna) är en vägledning till författaren av dokumentet och ska raderas innan dokumentet färdigställs.
* Text som befinner sig innanför ”<“ och ”>” uppdateras eller tas bort. T.ex. ska <system><version> ersättas med ackrediteringsobjektets namn och version (d.v.s. det informationssystem som ska ackrediteras).
* Övrig svart text kan användas i det färdigställda dokumentet.

## Specifik mallinstruktion

* Denna mall används för att skapa ISD-plan i ISD-processens *Dentifiera*-fas.
* ISD-planen styr projektets informationssäkerhetsarbete med syfte att deklarera informationssystemets informationssäkerhet. Primärt görs informationssäkerhetsdeklarationen för Försvarsmakten och deras ackreditering, men kan också användas för informationssystem som inte ska överlämnas till Försvarsmakten eller för informationssystem som ska överlämnas till Försvarsmakten men inte ska ackrediteras.
* ISD-planen klargör genomförandeprojektets förutsättningar, vilka aktiviteter som ska genomföras, i vilken omfattning ISD-processen ska användas och vilka roller som behövs.
* Inom ISD-delprojektet är det ISM som ansvarar för framtagning, efterlevnad och uppdateringar av ISD-planen.
* ISD-planen ska synkroniseras med projektledarens projektplan.
* ISD-planen godkänns av FMV Projektledare och Produktledare, eventuellt i samråd med Systemgranskningsledaren (SystGL)

## Dokumentstruktur Definiera-fasen

Dokumentstrukturen för ISD-processens Definiera-fas illustreras nedan. ISD-planen styr ISD-arbetet som resulterar i ISD-D med tre bilagor.



* ISD-planen styr ISD-arbetet i genomförandeprojektet. Planen klargör förutsättningar och utmaningar, aktiviteter och leveranser med tidplan, vilka kompetenser som behövs, och vilken projektsamverkan som behöver finnas.
* ISD-D deklarerar realiserbarheten av informationssystemet utifrån informationssäkerhetens perspektiv.
* AU-D innehåller bl.a. de analyser som genomförts, redovisning av kravspårning, hantering av inte tillämpbara krav, förteckning över krav som ska hanteras av evalueraren samt redovisning över hur designreglerna omhändertagits.
* ITSS-D bygger vidare på ITSS-I (eller på FM ITSS om ingen ITSS-I finns) med tolkade och allokerade informationssäkerhetskrav, på en detaljnivå att kraven kan användas för upphandling och verifiering.
* ITSA dokumenterar säkerhetsarkitekturen som dels uppfyller informationssäkerhetskraven och dels harmoniserar med System Engineering-arbetet i projektet.

## Att tänka på i arbetet med framtagning av ISD-plan

Lämplig kompetens för att producera ISD-plan innehas av ISD-rollen ISM, med stöd av ISA och ISE.

# Basfakta

## Giltighet och version

ISD-planen styr FMVs informationssäkerhetsarbete i syfte att ta fram ett system som kan godkännas ur säkerhetssynpunkt.

| Datum | Version | Beskrivning | Ansvarig |
| --- | --- | --- | --- |
| <datum> |  | Första utgåva |  |
|  |  |  |  |
|  |  |  |  |

Tabell – Versionshistorik

## Terminologi

Se referens [1] för en generell förteckning över begrepp och förkortningar som används inom ISD-processen. Följande tabell innehåller specifika begrepp och förkortningar som används i detta dokument.

| Begrepp/förkortning | Definition/förklaring |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

Tabell – Begrepp och förkortningar

## Referenser

Använd kommentarskolumnen i tabellen för att ange t.ex. status, klassning, utgivande organisation, författare eller årtal.

*Exempel på tabell med referenser:*

| *Referens* | *Beteckning* | *Kommentar* |
| --- | --- | --- |
| 1. *ISD v3.1, Begrepp och förkortningar* | *20FMV5903-1:1.1* |  |
| 1. *ISD-processbeskrivning v3.1* | *20FMV5903-1:1* |  |
| 1. *Beslut om krav på godkända säkerhetsfunktioner version 3.1 (KSF v3.1)* | *FM2014-5302:1* | *2014-06-13* |
| 1. *Designregel Programvaror med underhåll* | *18FMV3960-2:1* | *2018-05-17* |
| 1. *Designregel Härdning av IT-system* | *18FMV3960-1:1* | *2018-05-04* |
| 1. *Designregel Försvarsmaktens Tid* | *18FMV1600-3:1* | *2018-09-28* |
| 1. *Designregel Användning av operativsystem från Microsoft* | *17FMV5736-1:1* | *2017-06-13* |
| 1. *Krav på loggning i Försvarsmaktens IT-system* | *FM2016-4365:1* | *2016-02-19* |
| 1. *Säkerhet vid virtualisering 2.0* | *FM2017-5296:2* | *2017-03-06* |
| 1. *Definition och villkor för säkerhetsdomäner* | *FM2017-5154:1* | *2017-03-09* |

| Referens | Beteckning | Kommentar |
| --- | --- | --- |
| 1. ISD v3.1, Begrepp och förkortningar | 20FMV5903-1:1.1 |  |
| 1. ISD-processbeskrivning v3.1 | 20FMV5903-1:1 |  |
|  |  |  |
|  |  |  |

Tabell – Referenser

## Bilagor

Om detta dokument har några bilagor ska dessa förtecknas i detta avsnitt. Annars radera nedanstående och skriv ”Inga bilagor.”

Detta dokument har följande bilagor:

* Bilaga 1: <titel på bilaga 1>
* ...

# Inledning

## Syfte

Syftet med ISD-processen är att stödja genomförandeprojektets informationssäkerhetsarbete med målet att deklarera informationssystemets informationssäkerhet.

ISD-planens syfte är att klargöra arbetet som krävs för att FMV ska kunna deklarera att Försvarsmaktens informationssäkerhetskrav är uppfyllda, att arbetet bedrivits enligt gällande version av ISD-processen och enligt fastställd ISD-strategi.

## Informationssystemets referens

Denna ISD-plan avser <system> <version>.

# Förutsättningar

I detta kapitel beskrivs de förutsättningar, avgränsningar och beroenden som påverkar det planerade informationssäkerhetsarbetet.

## Styrande förutsättningar

Tabell 4 listar de styrande förutsättningar för ISD-planen och det planerade ISD-arbetet.

I *Referens* kolumnen kan källan till förutsättningen noteras för spårbarhet.

*Exempel på tabell för styrande förutsättningar:*

| Nr. | Förutsättning | Beskrivning | Referens |
| --- | --- | --- | --- |
| 1 | Version av ISD-process | Tidigare ackrediteringsunderlag har tagits fram med stöd av v2.3. Detta informationssäkerhetsarbete ska bygga på tidigare underlag och anpassas till v3.1 där så bedöms fördelaktigt ur projektriskhänseende. | [xxx] |
| 2 | KSF version | Tidigare ackrediteringsunderlag har baserats på KSF 2. Nya versionen av systemet ska uppfylla KSF 3.1. | [xxx] |
| 3 | Särskild säkerhetsskyddsbedömning (SSB) (tidigare benämnt Säkerhetsmålsättning) | Ingen ny SSB kommer att tillföras från Försvarsmakten. Istället genomför FMV förnyad verksamhets-, regelverks-, hot- och riskanalys inom ramen för ISD-arbetet och som dokumentareas i AU-I. | [xxx] |
| 4 | Omfattning | Systemet ska tilläggs-ackrediteras med avseende på TEID-inloggning på terminalerna. Detta innebär ackrediteringsunderlaget ska omfatta tillägget och belysa dess säkerhetspåverkan på befintligt ackrediterat system. | [xxx] |
| 5 | Användarupplevelse | Likartade lösningar avseende säkerhetsförmågor ska användas på de båda IT-systemen för att göra det användarvänligt då de nyttjas av samma personal. | [xxx] |

| Nr. | Förutsättning | Beskrivning | Referens |
| --- | --- | --- | --- |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
|  |  |  |  |

Tabell – Styrande förutsättningar för ISD-arbetet med referens till var de identifierats

<skriv mer om förutsättningar här vid behov>

## Avgränsningar

Detta avsnitt beskriver de avgränsningar som gäller. T.ex. om ISD-arbetet inte ska omfatta någon del av ett system. När avgränsningarna listas behöver de även motiveras.

Stöd till detta kapitel kan hämtas från ISD-strategin.

Följande komponenter omfattas inte av det planerade ISD-arbetet:

<Skriv här>

## Beroenden till andra tekniska system

Detta avsnitt ska beskriva hur beroenden ser ut till andra tekniska system.

*Exempel på faktorer som kan påverka informationssäkerhetsarbetet är:*

* *Redan godkända komponenter/system/delsystem som är en del av lösningen. Dessa kan påverka de aktiviteterna som behöver genomföras i ISD-arbetet bl.a. i form av analys över möjligheten till återbruk av redan befintlig dokumentation.*
* *Krav på godkännande mot andra projekt eller informationssystem. Det är viktigt att klargöra vem som har ansvar för godkännandet och framtagningen av dokumentationen i det fall informationssystem som utvecklats i annat projekt ska användas.*
* *Tidsberoenden till andra informationssystem eller projekt.*
* *Externa gränsytor som inte kan påverkas inom ramen för eget projekt.*

Förklara beroendet och hur det behöver hanteras.

Undvik tekniska beskrivningar i detta avsnitt.

<Informationssystemet> har beroenden till följande projekt och tekniska system: <Skriv här>.

## Beroenden till samverkanspartners

Detta avsnitt beskriver vilka beroenden som finns till samverkanspartners inom ISD-arbetet, och hur dessa tas omhand. Aspekter att ta hänsyn till är:

* Vilka krav på IT-säkerhet ställer samverkanspartners?
* Vilka krav på IT-säkerhet ställer Försvarsmakten och FMV på samverkanspartners?

Samverkansparter kan t ex vara

* Leverantör
* Systemintegratör

Ange om möjligt point-of-contact för varje samverkanspartner.

För redogörelse för behov av extern samverkan, se avsnitt 6.3.

<Skriv här>

## Kravunderlag från Försvarsmakten

De underlag från Försvarsmakten som informationssäkerhetsarbetet ska baseras på anges i detta avsnitt.

Enligt Försvarsmaktens processer (FM IT-process och FM BM TS) är det styrande kravunderlaget avseende informationssäkerhet *Särskild säkerhetsskyddsbedömning (SSB)* inklusive ITSS för informationssystemet.

SSB benämns ibland för *Säkerhetsmålsättning(SM)* eller *Informationssäkerhetsmålsättning*. ITSS kan vara en bilaga till SSB eller vara ett självständigt dokument. ITSS kan med fördel benämnas FM ITSS för att skilja Försvarsmaktens och FMVs ITSS-dokumentation åt.

Även andra kravunderlag från Försvarsmakten med påverkan på informationssäkerhetsarbetet kan förekomma.

*Exempel:*

* *Systemmålsättning (SMS1 och SMS2, eller SMS2F)*
* *Beslut från Försvarsmakten processer (FM IT-process (G-beslut), FM BM TS – (BOx-beslut), och tidigare ackrediteringsbeslut)*
* *Externa krav och beroenden såsom internationella krav och andra organisationers system*
* *Styrning av val av system/komponenter*
* *Designregler/designprinciper för t.ex. virtualisering och säkerhetsloggning.*

Underlagen kan vara av olika styrande karaktär på ISD-arbetet. Ange i kolumnen *Styrande*, aktuell status på dokumentet, t.ex. *styrande*, *stödjande* eller *orienterande*. Förklara begreppen som används vid behov.

*Exempel.*

| *Dokument* | *Dokumentnummer* | *Styrande* |
| --- | --- | --- |
| *Särskild säkerhetsskyddsbedömning (SSB) xxx* | *Referens [xx]* | *Styrande* |
| *G1-beslut xxx* | *Referens [xx]* | *Styrande* |
| *Krav på loggning i Försvarsmaktens IT-system* | *Referens [xx]* | *Styrande* |
| *Säkerhet vid virtualisering 2.0* | *Referens [xx]* | *Styrande* |
| *Definition och villkor för säkerhetsdomäner* | *Referens [xx]* | *Styrande* |

Tabell 5 listar Försvarsmaktens underlag som används för informationssäkerhetsarbetet.

| Dokument | Dokumentnummer | Styrande |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Tabell – Kravunderlag från Försvarsmakten

<Skriv eventuellt mer information här>

## Kravunderlag från FMV

Idetta avsnitt anges FMVs underlag som informationssäkerhetsarbetet ska baseras på.

*Exempel:*

* *ISD-strategi*
* *Vägledning för utveckling av säkra system*
* *Instruktioner*
* *Designregler*
* *Mallar*
* *Olika inriktningar*
* *Styrning över val av informationssystem/komponenter*
* *Styrning över vilka krav som ska ställas på leverantörens kompetens.*

Underlagen kan vara av olika styrande karaktär på ISD-arbetet. Ange i kolumnen *Styrande* aktuell statuspå dokumentet, t.ex. *styrande*, *stödjande* och *orienterande*. Förklara begreppen som används vid behov.

*Exempel.*

| *Dokument* | *Dokumentnummer* | *Styrande* |
| --- | --- | --- |
| *Processbeskrivning ISD 3.1* | *Referens [xx]* | *Stödjande* |
| *Ackrediteringsunderlag xxx* | *Referens [xx]* | *Orienterande* |
| *Klassificeringsguide xxx* | *Referens [xx]* | *Styrande* |
| *Designregel Programvaror med underhåll* | *Referens [xx]* | *Styrande* |
| *Designregel Härdning av IT-system* | *Referens [xx]* | *Styrande* |
| *Designregel Försvarsmaktens Tid* | *Referens [xx]* | *Styrande* |
| *Designregel Användning av operativsystem från Microsoft* | *Referens [xx]* | *Styrande* |

Tabell 6 listar underlag från FMV som används för informationssäkerhetsarbetet.

| Dokument | Dokumentnummer | Styrande |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Tabell – Kravunderlag från FMV

<Skriv eventuellt mer information här>

# Ackrediteringsobjektet

Detta kapitel definierar ackrediteringsobjektet och dess gränsytor.

## Definition av ackrediteringsobjektet

Detta avsnitt ska lista och kortfattat beskriva de systemdelar som ingår i ackrediteringsobjektet och de som ligger utanför. Avsnittet ska också innehålla en bild över informationssystemet och dess delsystem (om det är aktuellt med uppdelning/segmentering).

Beskrivningen ska vara övergripande för att skapa en förståelse informationssystemet och de delar som ingår i ackrediteringsobjektet. Den faktiska system- och verksamhetsbeskrivningen tas inte fram i ISD-planen.

Ett sätt att illustrera ackrediteringsobjektet är att beskriva tre zoner som ligger inuti varandra:

1. **Innersta zonen - ackrediteringsobjektet**

Innersta zonen innehåller det tekniska i informationssystemet som ska ackrediteras. Exempelvis programvara, operativsystem, datorhårdvara, nätverksutrustning, aktiva kort och brandväggar. Komponenter placerade i denna zon, som inte redan är godkända, kommer att kravställas och evalueras i ISD-arbetet.

1. **Omgivningen**

Zonen som omger ackrediteringsobjektet innehåller driftmiljön för informationssystemet. Exempelvis andra system med gränsytor till informationssystemet, entiteter som interagerar med informationssystemet, organisationer som äger/ansvarar/driftar och underhåller informationssystemet med alla dess instruktioner, manualer och rutinbeskrivningar. Ackrediteringsobjektet har ett beroende till denna driftmiljö tack vare att vissa informationssäkerhetskrav realiseras här eller på grund av interagerande system.

1. **Utanför omgivningen**

Yttersta zonen innehåller system, roller, organisation, rutiner m.m. som inte har någon påverkan eller interaktion med informationssystemet. Men det är lämpligt att förtydliga att dessa är avgränsade från ackrediteringsobjektet och dess omgivning.

<Beskriv ackrediteringsobjektet här>

## Gränsytor och deras exponering

Detta avsnitt listar informationssystemets externa gränsytor och dess exponering både logiskt och fysiskt. Syftet är att ge en bild av hur systemet är exponerat och dimensionerande exponering. Även om en mer detaljerad specifikation av externa gränssnitt sker i andra aktiviteter kan beskrivningen här underlätta vid definieringen av kritiska aktiviteter för informationssäkerhetsarbetet.

*Notera att detta inte är samma som exponeringsnivån (E1-E4) som används i KSF 3.1 och som bör vara angiven i Särskild säkerhetsskyddsbedömning (SSB) /FM ITSS för informationssystemet.*

Detta avsnitt beskriver hur informationssystemet exponeras mot andra informationssystem och fysiskt av personer.

<Beskriv systemets/ackrediteringsobjektets exponering här>

# Utmaningar

Detta kapitel ska beskriva de utmaningar som ISD-projektet identifierat under projektets genomförande.

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

Ange de planerade åtgärder som identifierats för att hantera utmaningarna, och notera dessa i aktivitetsplanen (*senare i ISD-planen*)

*Exempel.*

| *Nr* | *Utmaning* | *Åtgärd* |
| --- | --- | --- |
| *1.* | *ISD-Strategi saknas vilket gör att bl.a. följande frågor finns:*  *- Inriktningar: Användning av redan godkända FMV-komponenter, återbruk och designregler/-principer*  *- Krav på samverkande system*  *- Gemensamma säkerhetsfunktioner*  *- FMVs roll avseende vidmakthållande av ackrediteringsobjektet*  *- Intern samverkan FMV: TC, CI och/eller SI, SystGL IT-Säk, FMV T&E och övriga*  *- Extern samverkan: Enheter på Försvarsmakten* | *Klarlägg förutsättningar med FMV PrL så snart som möjligt (inför initialt godkännande av denna plan)* |
| *2.* | *Beroende till externa säkerhetsfunktioner, exempelvis analys av säkerhetsloggar och skydd mot skadlig kod.* | *Säkerställ redan under Definiera-fasen att verksamheten har möjlighet att tillföra funktionerna.* |
| *3.* | *FM ITSS är just nu inte fastställd. Allt ISD-arbete som görs innan denna är fastställd baseras på ett utkast. Om det uppstår signifikanta ändringar kommer det orsaka merarbete och försening i projektet.* | *Tillse att FM ITSS blir fastställd så fort som möjligt* |
| *4.* | *ISD-arbetet korrelerar just nu inte med projektets master-projektplan, vilket kan innebära att system­leverantören inte implementerar rätt säkerhets­funktioner.* | *Tillse att planer synkroniseras snarast möjligt och håll dem uppdaterade och korrelerade under projektets gång* |
| *5.* | *Tilltänkt systemleverantör saknar tillräcklig bemanning, erfarenhet och kompetens inom IT-säkerhetsområdet.* | *Utred möjligheten att välja annan leverantör, tydliggör FMVs krav för Leverantören, planera för utökat antal avstämningspunkter med Leverantören, och/eller planera för att FMV ska ge omfattande stöd till leverantören* |
| *6.* | *MOA är möjligtvis inte fullständigt insatt i arbetet som bedrivs och vad som krävs ur ett informationssäkerhetsperspektiv för att så småningom få beslut om ackreditering* | *Möte med MOA och klarlägga vad som krävs för att gå i mål avseende processer (IT-processen, BMTS) och kontakter med MUST* |
| *7.* | *Projektet och ISD-delprojektet är till största del upplagt enligt vattenfallsmodellen. Detta är naturligt och enligt processen men ger risk att misstag, missförstånd och ändringar i omvärlden fångas upp för sent för att inte få konsekvenser* | *Integrera verifiering av assuransaktiviteter med leverantörens utvecklingsplan så att det mesta redan är verifierat vid leverantörens leverans.*  *Planera in avstämningar med slutkunden under projektets gång för att presentera designbeslut som tagits och fånga upp förändringar i verksamheten.* |

Inom ramen för ISD-processen har ett antal utmaningar i Tabell 7 identifierats för <informationssystemet>. Utmaningarna kan komma att resultera i projekt- eller säkerhetsrisk.

| Nr | Utmaning | Åtgärd |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Tabell – Utmaningar med åtgärder för att riskminimera

Utmaning som resulterar i en risk som saknar fullständig åtgärd behöver bevakas och hanteras under projektets gång. Rutin för riskhantering ska definieras och efterlevas enligt avsnitt XXX. Kvarstående risker ska också analyseras i AU-x och redovisas i ISD-x.

# Informationssäkerhetsarbete

## Tillsättning av ISD-roller

Ett informationssäkerhetsarbete kräver ett antal roller med olika profiler för att täcka upp projektets behov.

En beskrivning av rollerna och deras aktiviteter finns i ISD-processen 3.1, referens [2].

Detta avsnitt namnger de personer som arbetar i respektive ISD-roll, med ansvar och uppgifter enligt ISD-processens beskrivning, referens [2].

<Skriv eventuellt mer information här, t.ex. om det ska tillämpas avvikande ansvar för rollerna jämfört med hur det är definierat i processbeskrivningen>

Inom ISD-projektet är individerna i Tabell 8 utsedda att arbeta i respektive ISD-roll. Ett ’X’ i ansvarig-kolumnen betyder att denna individ också är ensamt huvudansvarig i rollen. Den som är huvudansvarig är också FMV Projektledares *point-of-contact* till ISD-projektet

| Roll | Namn | Organisation | Ansvarig |
| --- | --- | --- | --- |
| ISM |  |  | X |
| ISM |  |  |  |
| ISA |  |  | X |
| ISA |  |  |  |
| ISE |  |  | X |
| ISE |  |  |  |
| ISTM |  |  | X |
| ISTM |  |  |  |

Tabell – Tillsättning av ISD-rollerna. Kryss i Ansvarig-kolumnen betyder huvudansvaret inom rollen.

Förändring av tillsatta roller kräver en uppdatering av ISD-planen.

## Behov av intern samverkan

Ett informationssäkerhetsarbete kräver nära samarbete med andra delar i ett projekt för att IT-säkerhetsfunktionerna ska integreras i utvecklingsarbetet med informationssystemet. Olika sätt att designa informationssystemet kan påverka hur IT-säkerhetsfunktionerna implementeras.

Detta avsnitt beskriver de roller som ISD-projektet behöver 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.*
* *System Engeneering (SE) – systemutformning - för att kunna avgöra när designval påverkar säkerhetsfunktionaliteten i produkten. Samverkan sker med ISA.*
* *Slutanvändare – representant för slutanvändarna som ingår i projektet. Samverkan sker med ISA.*
* *Produktion (internprojekt).*
* *Förvaltning – för att kunna från början ta hänsyn till hur informationssystemet ska vidmakthållas. Samverkan sker med ISM.*
* *Systemsäkerhet – där systemet har krav på systemsäkerhet. Samverkan sker med ISA.*
* *Verifiering och Validering – planering och samverkan för verifiering och validering av informationssäkerhetsarbetet. Samverkan sker med ISM.*

<Skriv här>

## Behov av extern samverkan

Detta avsnitt beskriver samverkan med de externa samverkanspartners som påverkar informationssäkerhetsarbetet.

*Exempel på externa samarbetspartners är:*

* *FM MOA (materielområdesansvarig) – representerar kunden och anvisar om eventuellt ytterligare kontaktytor inom Försvarsmakten. För vissa vapenslagsstaber har MOA även eget stöd av IT-säkerhetshandläggare.*
* *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. Observera att eventuellt samarbete med MUST eller någon annan på Försvarsmakten ska vara anvisat av MOA.*
* *FM CIO (representant) - Observera att eventuellt samarbete med FM CIO eller någon annan på Försvarsmakten ska vara anvisat av MOA.*
* *Systemgranskningsledare (SystGL)*
* *Leverantör – samverkan sker i enlighet med av FMV kravställd VÅS*
* *Slutanvändare – Av FMV Projektledare anvisad användargrupp eller enskilda slutanvändare för användbarhetstester m.m.*
* *Internationella samarbetspartners i enlighet med upprättade avtal*
* *Lab som genomför RöS-mätningar*
* *Samverkan ska ske med andra delar på FMV som utvecklar informationssystem*
* *Samverkan med FMV T&E som ansvarar för test och evaluering av informationssystem*
* *Andra projekt där samverkan ska ske med system/produkter utvecklade inom annan domän*

<Skriv här>

## Rutiner

Detta avsnitt beskriver ISD-projektets rutiner.

Det är en fördel om så många rutiner som möjligt är gemensamma med huvudprojektet. Risk finns annars att ISD-arbetet exkluderar sig självt från projektet. Hänvisa i förekommande fall till projektgemensamma rutiner. Det viktiga är att alla som arbetar i ISD-projektet vet vad som gäller för de olika administrativa rutinerna.

### Projektsäkerhetsskydd

Säkerhetsskyddet i ISD-projektet styrs av följande:

* <Lista alla dokument som styr projektsäkerhetsskyddet t.ex. FMV säkerhetskyddskrav på projektet och klassningsguide>

ISD-delprojektets säkerhetsskyddsansvarig är: <namn på ansvarig som ingår i ISD-arbetet>

Eventuella frågor om FMVs säkerhetskyddskrav och anmälan av eventuella säkerhetsincidenter ställs till FMV Projektledare.

### Riskhantering

Risker som identifieras behöver hanteras och ska ske enligt följande rutin:

<beskriv hur riskhantering ska gå till>

### Ändringshantering

Detta avsnitt ska beskriva processen för ändringshantering, samt hur uppföljning och leverans ska ske. Styrande är att varje ändring i designen ska redovisas i en ändringshanteringsgrupp. För varje sådan ändring ska en bedömning göras över vilken säkerhetspåverkan och i vilken grad den har.

Ändringshanteringsprocessen ska också:

* Beskriva vem som är ansvarig.
* Beskriva vem som bedömer ändringsbehovet.
* Beskriva hur ändringsbehovet kan stämmas av med beställaren.
* Beskriva vem som fattar beslut om ändringen.
* Beskriva vem som dokumenterar ändringar.
* Beskriva vem som analyserar ändringars påverkar på IT-säkerheten.

Dessutom ska det beskrivas hur bedömningen integreras med övrig ändringshantering för projektet så att rätt beslut ska kunna fattas och ändringen realiseras.

Ändringshanteringsprocessen ska också ange vilka dokument som omfattas. Om inte ISD-underlagen går in i ett projektövergripande konfigurationsledningssystem, bör detta kapitel avgränsas till ISD-artefakterna.

<Skriv här>

### Progressuppföljning

Rutin för progressuppföljning av ISD-arbetet mot FMVs Projektledare behöver beskriva vad som ska följas upp, hur ofta och i vilken form.

<Skriv här>

### Dokumenthantering

Dokumenthantering av ISD-artefakterna och deras referenser är centralt i ISD-arbetet. Beskriv här hur det ska fungera för ISD-delprojektet.

<Skriv här>

### Kvalitetssäkring

Kvalitetssäkring i ISD- projekt sker genom att följa upp hur informationssäkerhetsarbetet bedrivs. Klarlägg vad som ska följas upp och vem som har ansvar för informationssäkerhetsarbetet i syfte att säkerställa kvalitet.

Här behöver även en rutin för kvalitetssäkring av leverabler från ISD-arbetet beskrivas för att uppnå en förutsägbar kvalitetsnivå.

<Skriv här>

### Leveransprocess

Leveransprocessen ska beskriva under vilka former leveranser ska ske till FMVs Projektledare från ISD-projektet.

Avsnittet kan också beskriva vem som godkänner dessa artefakter för vidare leverans inom FMV, t.ex. projektets CCB eller designledningens CCB.

<Skriv här>

# Aktiviteter och tidplan

En generell beskrivning över vilka aktiviteter som ska genomföras och artefakter som ska tas fram finns i *ISD-Processen 3.1,* referens [2]. Detta kapitels beskrivning anpassas för att stödja det aktuella genomförandeprojektet.

Detta kapitel beskriver de leveranser som ska göras inom ISD-arbetet och vilka artefakter som är kopplade till vilka leveranser. Här framgår också vilka aktiviteter som krävs för att ta fram identifierade artefakter och när i tiden dessa ska vara genomförda.

Leveranserna integreras med projektets leveranser så att tidplanen för informationssäkerhetsarbetet korrelerar med projektets huvudtidplan. Ansvarig för detta är ISM.

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



Figur 1 – Förhållandet mellan aktiviteter, artefakter och leveranser

## Artefakter

### Kravnedbrytning och arkitektur

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

Ange även vilka artefakter som används för att dokumentera *funktionella* respektive *icke-funktionella* säkerhetskrav. Typiskt görs detta i *Teknisk Specifikation* (TS) respektive *Verksamhetsåtagandespecifikation* (VÅS). Observera att ISD-arbetets krav ska arbetas in i projektets TS/VÅS.

<Skriv här>

### Kravanalys

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

<Skriv här>

### Säkerhetstester

Ange de artefakter som projektet avser att ta fram inom ramen för säkerhetstester för att verifiera och eventuellt komplettera analysen över kravuppfyllnaden.

<Skriv här>

### Leverans till Försvarsmakten

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

<Skriv här>

### Övriga underlag

Ange vilka övriga artefakter som produceras inom ISD-arbetet.

*Exempel: Separata analysunderlag, utredningar, m.m.*

<Skriv här>

## Leveranser

ISD-projektet avser att genomföra leveranserna enligt Tabell 9 nedan. <Utöver detta levereras arbetsutgåvor för granskning, samt samråd vid milstolparna som definieras i avsnitt 7.4 *Tidplan*. Även andra leveranser kan förekomma vid behov.>

*Exempel på leveranser:*

| *Nr* | *Leverans* | *Innehåll* |
| --- | --- | --- |
| *1.* | *Plan* | *ISD-plan för initialt fastställande. Kartlägger arbetsinsatsen för informationssäkerhetsarbetet.* |
| *2.* | *Informationssäkerhetskrav* | *ISD-D, med bilagor samt kravtexter till TS och VÅS avseende informationssäkerhet.* |
| *3.* | *Ackrediteringsunderlag* | *ISD och ISD-R, med bilagor. Hur den satta kravbilden uppfylls och krav på användning och vidmakthåll.* |

| Nr. | Förutsättning | Beskrivning | Referens |
| --- | --- | --- | --- |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
|  |  |  |  |

Tabell – Leveranser

<Skriv eventuellt mer information här>

## Aktiviteter

Nedan aktiviteter är obligatoriska för ISD-arbetet:

* Producera väl underbyggt underlag för realiserbarhetsbedömningar genom nyttjande av mallarna för de olika Analysunderlagen (AU-I, AU-D osv.)
* Dokumentera spårbarhet i kravarbetet
* Dokumentera spårbarheten av granskningen över kravuppfyllnad
* Dokumentera designbeslut
* Deklarera informationssäkerheten

Realiserbarhetsbedömningar ska göras även om informationssystem inte ska ackrediteras.

Som *ansvarig* och *Stöd* i tabellen nedan ska någon av de definierade ISD-rollerna anges: ISM, ISA, ISE eller ISTM.

<Skriv eventuellt mer information här>

*Aktiviteterna som är listade i tabellen nedan är exempel.*

| *Nr.* | *Aktivitet* | *Beskrivning* | *Resultat, artefakt* | *Ansvarig* | *Stöd* |
| --- | --- | --- | --- | --- | --- |
| *1* | *Planera* | *Skapa en första utgåva av detta dokument som beskriver allt grundläggande och som kan användas fastställas och användas av FMV Projektledare för att synka med övriga delprojekt. Detaljer fylls på efterhand i uppdateringar.* | *ISD-plan (detta dokument)* | *ISM* | *ISA* |
| *2* | *ISD projektledning* | *Löpande arbete för att föra ISD-arbetet framåt, med arbetsfördelning, uppföljning, rapportering, planering och riskhantering* | *Progressrapporter*  *Uppdaterad ISD-plan*  *Uppdaterad risklista* | *ISM* |  |
| *3* | *Krav- och arkitekturarbete 1* | *Påbörja precisering och allokering av kraven från FM ITSS samt påbörja säkerhetsarkitekturen. Övriga ingångsvärden såsom FMV designregler ska också arbetas in. Resultatet används som ingångsvärde till dialog med leverantören för att synka krav och design.* | *Utkast på ITSS-D och ITSA* | *ISA* | *ISM* |
| *4* | *Krav- och arkitekturarbete 2* | *I dialog med leverantören (och ev andra intressenter) slutförs precisering och allokering av krav i ITSS-D och ITSA. Resultatet sammanfattas i ISD-D. FMV Projektledare ansvarar för godkännande/fastställande.* | *Fastställda ISD-D, ITSS-D och ITSA* | *ISA* | *ISM* |
| *5* | *Ta ut krav till TS och VÅS* | *Ta ut kravtexter som ska ges till leverantör och synka språk och terminologi med övrigt innehåll i TS och VÅS. Arbetas in tillsammans med ansvarig författare av TS och VÅS.* | *Infosäkkrav till TS och VÅS* | *ISA* | *ISM* |
| *6* | *Granska anbud* | *Granska leverantörens anbud ur ett ISD-perspektiv.* | *Utlåtande ur ett ISD-perspektiv* | *ISA* | *ISM* |
| *7* | *Stöd leverantören* | *Ge leverantören stöd under deras utveckling genom att svara på frågor, diskutera lösningar, hantera förändringar, specificera lämpligt upplägg av assuransdokumentation etc.* | *Löpande stöd* | *ISE* | *ISM* |
| *8* | *Granska uppfyllnad assuranskrav* | *Granska leverantörens redovisning av uppfyllande av assuranskrav i VÅS. Genomför site-visit. Identifiera tveksamheter och brister. Denna aktivitet bör genomföras till största delen redan under tiden som utvecklingen pågår hos leverantören.* | *Utkast på AU-R* | *ISE* | *ISM* |
| *9* | *Granska uppfyllnad funktionella krav* | *Granska leverantörens redovisning av uppfyllande av infosäkkrav i TS. Identifiera tveksamheter och brister.* | *Utkast på ITSS-R* | *ISE* | *ISM* |
| *10* | *Genomföra säkerhetstester* | *Definiera testfall, genomför tester och identifiera brister.* | *Testdokumentation* | *ISTM* | *ISE, ISM* |
| *11* | *Omgranskning* | *Utför omgranskning och test av leverantörens eventuella uppdateringar* |  | *ISE* | *ISM* |
| *12* | *Bedöm säkerheten* | *Färdigställ dokumentationen inklusive krav på användning och på vidmakthåll. Gör en sammanfattande bedömning av styrkan på säkerhetsförmågorna. FMV Projektledare ansvarar för godkännande/fastställande.* | *Fastställd ISD, ISD-R, ITSS-R och AU-R* | *ISM* | *ISE* |

I Tabell 10 anges de identifierade aktiviteter som krävs för att genomföra ISD-arbetet.

| Nr. | Aktivitet | Beskrivning | Resultat, artefakt | Ansvarig | Stöd |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Tabell – Aktiviteter

<Skriv eventuellt mer information här>

## Tidplan

Tidplanen för ISD-projektet hanteras i <ange var den dagliga planeringen av ISD-arbetet hanteras> och uppdateras vid behov. Tabell 11 anger milstolpar som ISD-projektet är beroende av eller levererar till. Milstolparna är synkroniserade och överenskomna i projektet. Ändringar på dessa milstolpar ska stämmas av med projektet eftersom det berör andra parter.

*Milstolparna som är ifyllda i tabellen nedan är exempel.*

| *Nr.* | *Milstolpe* | *ISD-leverans* | *Tidpunkt* |
| --- | --- | --- | --- |
| *1* | *Utkast på ISD-plan klar för FMV godkännande* | *Plan* | *xxxx-xx-xx* |
| *2* | *FM SSB fastställd* |  | *xxxx-xx-xx* |
| *3* | *Krav- och arkitekturarbete tillsammans med leverantör startar* |  | *xxxx-xx-xx* |
| *4* | *Utkast på ISD-D, ITSS-D och ITSA klara för extern granskning (FMV infosäk, FMV oberoende granskning och MUST)* |  | *xxxx-xx-xx* |
| *5* | *Utkast på ISD-D, ITSS-D och ITSA klara för fastställande av FMV* | *Informations-säkerhetskrav* | *xxxx-xx-xx* |
| *6* | *Informationssäkerhetskrav till TS & VÅS fastställda* |  | *xxxx-xx-xx* |
| *7* | *Leverantörens utvecklingsarbete startar* |  | *xxxx-xx-xx* |
| *8* | *Leverantören levererar utvecklat system* |  | *xxxx-xx-xx* |
| *9* | *Granskning av leverantörens kravuppfyllnad klar (inklusive site visit men ej analys och test)* |  | *xxxx-xx-xx* |
| *10* | *Säkerhetstestning startar (här behövs tillgång till utrustning och kompetens)* |  | *xxxx-xx-xx* |
| *11* | *ISD-R med bilagor och ISD klara för extern granskning (FMV infosäk, FMV oberoende granskning och MUST)* |  | *xxxx-xx-xx* |
| *12* | *ISD och ISD-R fastställda och klara för överlämning till Försvarsmakten* | *Ackrediterings-underlag* | *xxxx-xx-xx* |

| Nr. | Milstolpe | ISD-leverans | Tidpunkt |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabell – Tidplan

<Skriv eventuellt mer information här>