Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(12)

<SYSTEM> <VERSION>

INFORMATIONSSÄKERHETSDEKLARATION *IDENTIFIERA* (ISD-I)

Inklusive 2 bilagor

Innehåll

Mallinformation 18FMV6730-2:1

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

Mallinstruktion

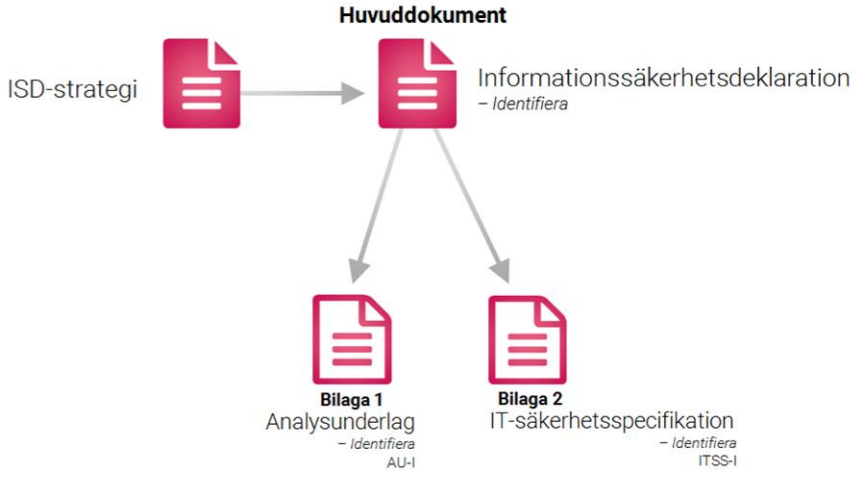
Denna mall ska användas för att ta fram dokumentet Informationssäkerhetsdeklaration *Identifiera*, ISD-I. ISD-I utgör bedömning av realiserbarhet ur ett informationssäkerhetsperspektiv av aktuellt IT-system inför VHL FMV beslut S2 innan *Definiera*.

Det skarpa dokumentet börjar med kapitel 1 Basfakta. Sidorna innan dess innehåller beskrivningar kring vad ISD-I är, arbetssätt, innehåll och att tänka på i arbetet. Dessa sidor tas bort i det skarpa dokumentet.

- 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 *Identifiera*

Informationssäkerhetsdeklaration *Identifiera* (ISD-I) består av ett huvuddokument och två bilagor, se dokumentstruktur i figur 1. Huvuddokumentet utgör realiserbarhetsbedömning av IT-systemet, och ska enbart innehålla de faktorer som ligger till grund för bedömning. Huvudparten av informationen som ligger till grund för realiserbarhetsbedömningen i *Identifiera* ska Försvarsmakten tillhandahålla i enlighet med H SÄK Infosäk. Kompletterande information hämtas från AU-I.



Figur 1Dokumentstruktur Informationssäkerhetsdeklaration ISD-I

Bilaga 1 – Analysunderlag *Identifiera* (AU-I) omfattar relevanta analyser avseende informationssäkerhetsaspekten ur ett verksamhetsperspektiv. Huvudparten av informationen som ligger till grund för realiserbarhetsbedömning i *Identifiera* ska Försvarsmakten tillhandahålla i enlighet med H SÄK Infosäk.. Kompletterande analyser genomförs och dokumenteras i AU-I. Resultatet från AU-I dokumenteras i bilaga 2 - IT-SäkerhetsSpecifikation (ITSS-I) i form av krav.

Bilaga 2 – IT-SäkerhetsSpecifikation ITSS-I omfattar de krav som genereras av AU-I.

Dokumentet ISD-strategi är ett viktigt indata till ISD-I som ska ge relevanta förutsättningar för arbetet såsom krav på återbruk av IT-system/komponenter, externa beroenden till andra projekt mm.

Huvuddokumentet ISD-I omfattar:

- Beskrivning av verksamhet och system ur ett informationssäkerhetsperspektiv på den nivån att det stärker förståelsen för realiserbarhetsbedömningen
- Definition och beskrivning av ackrediteringsobjektet. Ackrediteringsobjektet är inte alltid samma sak som projektets ansvar avseende systemområde utan det kan vara en del av systemområdet.
- Viktiga slutsatser från bilagorna som stärker förståelsen för realiserbarhetsbedömningen.
- Bedömning av realiserbarhet ur ett informationssäkerhetsperspektiv, som baseras på ackrediterbarhet, kostnadseffektivitet, kvarvarande brister, projektrisker och integration av SE (System Engeneering) allt utifrån ett informationssäkerhetsperspektiv. Bedömningen ska ge förutsättningar inför genomförandeprojektet.

Bilaga 1: AU-I omfattar:

- Verksamhetsanalys såsom sekretessbedömning och krav på riktighet och tillgänglighet
- Regelverksanalys
- Säkerhetsanalys med identifiering av hot och sårbarheter samt riskhantering

Aktiviteterna ovan genomförs i säkerhetsmålsättningsarbetet på Försvarsmakten, enligt HSÄK Infoskydd. Vid behov omfattar AU-I kompletterande analyser såsom:

- Framtagning av användningsfall för framtagning av verksamhetens behov
- Hotanalys för framtagning av verksamhetens sårbarheter
- Exponeringsanalys

Bilaga 2: ITSS-I är det första kravdokumentet i kedjan av krav. ITSS-I ska vara utformat så att verksamhetens behov av informationssäkerhet kan utläsas i kraven. ITSS-I motsvarar FM ITSS. ITSS-I omfattar:

- Verksamhetens tillkommandekrav från bilaga 1-AU-I.
- Krav från regelverksanalys (om det är relevant)
- Övergripande kravtolkning görs ur ett verksamhetsperspektiv som ger underlag till tolkning av MUST KSF.

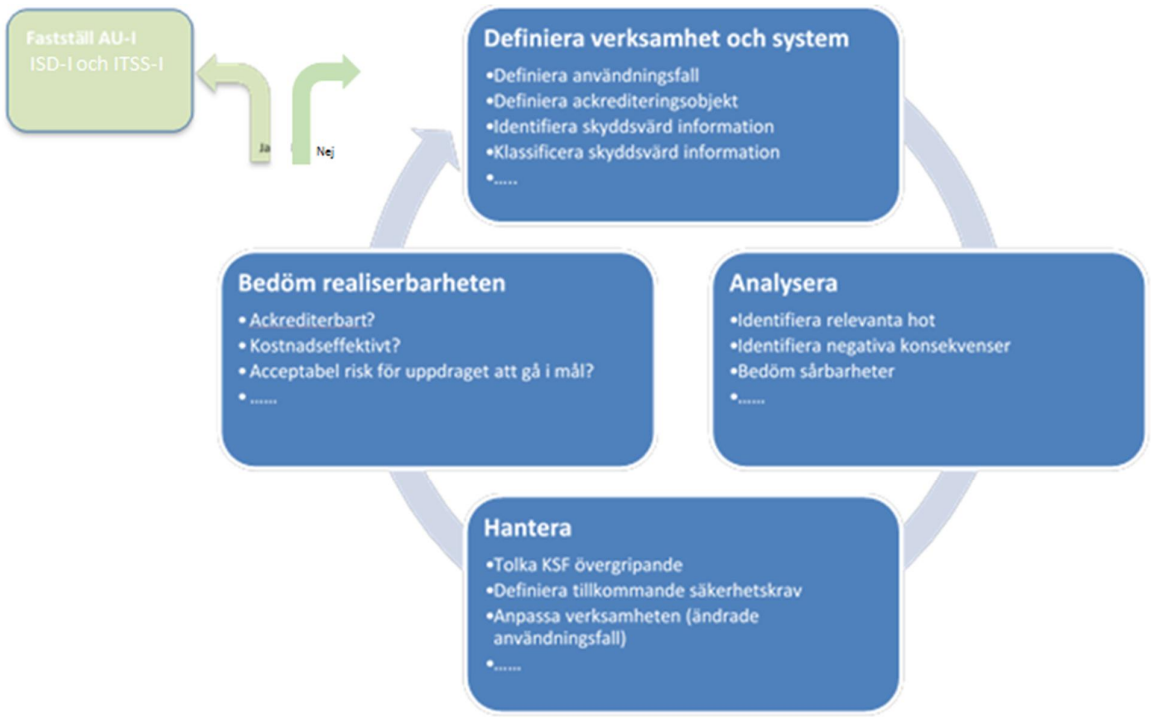
Att tänka på i arbetet med framtagning av Informationssäkerhetsdeklaration *Identifiera (ISD-I)*

I *Identifiera* skapas förutsättningar för genomförandeprojektet baserat på input från Försvarsmakten. Informationssäkerhetsarbetet består av att beskriva och analysera en mängd olika aspekter och detta bör göras inkrementellt i flera steg tillsammans med Försvarsmakten. Ansatser görs utifrån tänkbara lösningar med avseende på verksamheten.. *Identifiera* har fortfarande inte en detaljerad lösning, men ansatserna provas utifrån den kunskap som finns vid tillfället, för att sedan utvecklas i *Definiera* då detaljer kring den tekniska lösningen har utvecklas i mer detalj. Utifrån varje ansats bedöms realiserbarheten och beslut tas om det finns behov att fortsätta pröva nya lösningar eller om realiserbarhetsbedömning kan genomföras för vidare arbete i *Definiera*.

Figur 2 - Arbetssätt för framtagnng av informationsäkerhetsdeklaration Identifiera visar ett arbetssätt för *Identifiera* för att få fram verksamhetens krav och behov ur ett informationssäkerhetsperspektiv såsom:

- Definition av verksamhet och system genom att definiera ackrediteringsobjekt, resultatet dokumenteras i huvuddokumentet ISD-I.
- Inhämta verksamhetens behov från Försvarsmaktens säkerhetsmålsättningsarbete. I de fall kompletterande analyser behövs identifieras användningsfall och skyddsvärda tillgångar. Resultatet dokumenteras i bilaga 1 AU-I.
- Krav på omgivande system anges.
- Hantera resultatet i möjligaste mån kopplat till kravtolkning MUST KSF samt tillkommande krav. Resultatet dokumenteras i bilaga 2 ITSS-I
- Bedöma realiserbarheten inklusive ackrediterbarhet då detta inte är samma sak. Ett IT-system kan bedömas ackrediterbart men till priset av en hög kostnad och det blir då inte realiserbart. Resultatet dokumenteras i huvuddokumentet ISD-I.

Processen kan behöva genomföras flera gånger för att återkoppla resultatet från varje steg där nya upptäckter kan resultera i omprövningar av verksamhetens behov och krav.



Figur 2 - Arbetssätt för framtagnng av informationsäkerhetsdeklaration Identifiera

Det är viktigt att det finns en dialog mellan FM och FMV. Dialogen ska resultera i att FM skall förstå att rätt krav på förutsättningar är lämnade till FMV. FM:s Säkerhetsmålsättning och ITSS ska användas som indata till ISD-I. Finns inte dessa underlag kan antingen FMV gå tillbaka till FM och begära underlagen eller driva arbetet med att ta fram underlagen med hjälp av FM.

Ackrediteringsobjektet och eventuella avgränsningar är definierade så detaljerat det är möjligt i detta skede. Exempel på avgränsning är angränsande system som inte ingår, delkomponenter som inte anses vara IT-system/relevanta ur IT-säkerhetspunkt osv. Hänsyn ska även tas till avgränsningar eller särskild hantering avseende material som hanteras i särskild ordning med hänsyn till dess informationssäkerhetsklassning. Viktigt är att klargöra vilka informationssäkerhetskrav som omgivningen omhändertar och som det tekniska systemet därför inte behöver omhänderta. Det är viktigt att det framgår i dokumentet vilket system som är aktuellt samt dess versionsnummer.

Nedan beskrivs aktiviteter för respektive roll. Observera att angivna aktiviteter är typiska val av aktiviteter för ISD-I. Genomförandeprojektets behov styr vilka aktiviteter som ska genomföras.
FMV PrL:

- Granskning av indata från FM.
- Återkoppling till FM vid behov
- Komplementering av underlag från FM vid behov genom analyser
- Ta fram ISD-I med AU-I och ITSS-I
- Genomför realiserbarhetsbedömning
- Initiera ett eller flera projekt för genomförande
- Ta fram projektdirektiv

1 Basfakta

1.1 Giltighet och syfte

Detta dokument är Informationssäkerhetsdeklaration *Identifera* (ISD-I) för <Systemnamn> <version> inför FMV VHL S2-beslut.

Syftet med ISD-I är att dokumentera beslut avseende bedömning av realiserbarhet baserat på verksamhetens behov avseende på informationssäkerhet.

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

Bilaga 1. AU-I
Bilaga 2. ITSS-I

1.5 Referenser

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

Tabell 3 - Referenser

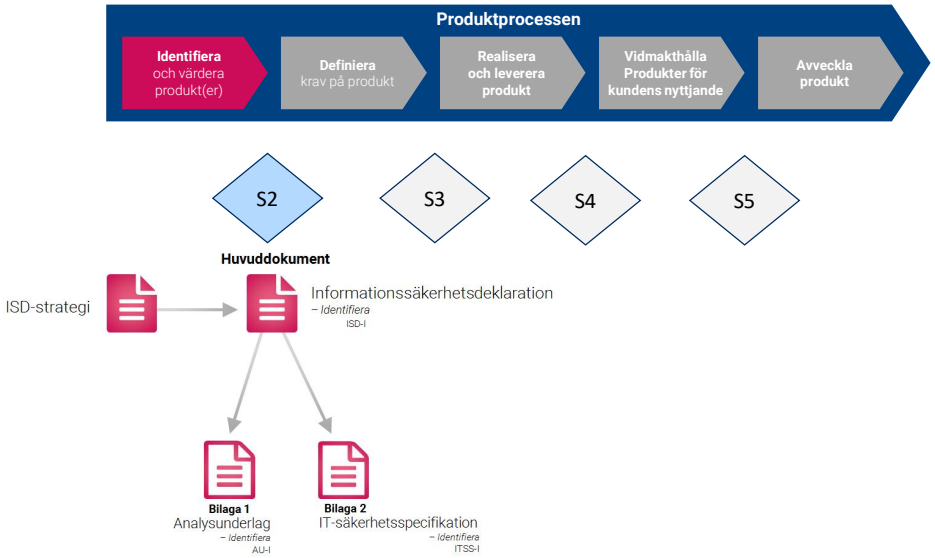
2 Inledning

I *Identifiera* fångas verksamhetens behov med avseende på informationssäkerhet. Arbetet i *Identifiera* skapar förutsättningar för genomförandeprojektet att leverera realiserbara IT-system.

Detta dokument utgör bedömning av Realiserbarhet ur ett informationssäkerhetsperspektiv för <System> <Version> inför FMV VHL S2-beslut.

Realiserbarhetsbedömningen baseras på:

- Att FMV förstår de verksamhetskrav som ställts av FM.
- Verksamhetens krav på sekretess, tillgänglighet och riktighet framgår i underlaget och att de säkerhetspåverkande faktorerna har lyfts upp såsom exponering.
- Ackrediteringsobjektet och eventuella avgränsningar är definierade så tydligt som det går i detta skede.
- Det finns ett resonemang och motivering avseende den informationsklass som ges informationen som ska flöda i IT-systemet.
- Exponeringsanalysen från ett verksamhetsperspektiv t.ex. vilken fysisk miljö IT-systemet ska verka i, hur många användare som är tänkt att använda IT-systemet.
- Beslut kring återbruk av godkända komponenter baseras på analyser
- Avvägning mot kostnad/nytta
- Projektriskerna bedöms acceptabla



Figur 3: ISD-processen - Identifiera och dokumentstruktur

3 Definition av verksamhet och system

3.1 Övergripande verksamhetsbeskrivning

Detta avsnitt ska ge en övergripande beskrivning av verksamheten på ett sådant sätt att det ger en läsbar förståelse över vilken verksamhet det aktuella IT-systemet ska stödja. Detaljer finns ytterligare i bilaga 1-AU-I.

Den övergripande beskrivningen kan omfatta:

- Identifierade användningsfall med beskrivning på uppgift som ska lösas från verksamheten
- Informationsklassificeringar och utmaningar kring detta
- Dimensionerande aspekter ur ett realiserings- och ackrediteringsperspektiv såsom exponering, externa gränsytor, system av system, internationell samverkan

Nivå på beskrivningen beror på hur mycket information det finns i detta skede. Saknas information görs beskrivningen mer i detalj i *Definiera.*

3.2 Identifiering av ackrediteringsobjekt

Detta avsnitt ska:

- Beskriva det eller de aktuella ackrediteringsobjekt/en, dvs. IT-system som är i fokus för informationssäkerhetsarbetet.
- Ange ackrediteringsobjektets omfattning inklusive ingående delsystem och miljö. Ackrediteringsobjektets omfattning ska förklara vad det är som ska ackrediteras.

Nivå på beskrivning av ackrediteringsobjektet beror på hur mycket information det finns kring det tänkta IT-systemet.

3.2.1 Avgränsningar

Under denna rubrik anges eventuella avgränsningar för ackrediteringsobjektet dvs. vad som inte omfattas av detta informationssäkerhetsarbete. En väl definierad avgränsning underlättar ackrediteringen av systemet. Tex redan godkända signalskyddsprodukter ingår inte i ackrediteringsobjektet och ska inte omfattas av informationssäkerhetsarbetet.

4 Realiserbarhetsbedömning

Detta avsnitt ska ange huruvida aktuellt ackrediteringsobjekt bedöms realiserbart ur ett informationssäkerhetsperspektiv inför FMV VHL S2-beslut och för att gå vidare till *Definiera*. Bedömningen görs med utgångspunkt från verksamhetsbeskrivning och analyserna i bilaga 1- AU-I.
Information kan också inhämtas från ISD-strategin.
Realiserbarhetsbedömningen görs med fördel tillsammans med SystGL IT-säk.

4.1 Bedömning av indata från FM

Bedömning görs avseende förekomst av och innehåll i indata (kravkällor) från FM.
Klargör om det behövs komplettering av indata, och om så är fallet bedömd omfattning och tidsåtgång. Eventuell komplettering av kravkällor kan antingen göras i *Identifiera* eller i *Definiera*.

4.2 Ackrediterbarhet

Ackrediterbarhet är en bedömning av hur IT-systemet på en övergripande nivå bedöms kunna uppfylla ställda informationssäkerhetskrav i balans med verksamhetsbehov, övriga IT-systemegenskaper, kostnad och tid.
Finns det beroende till andra komponenter/system för att åstadkomma ackrediterbarhet ska det i bedömningen även ingå huruvida rätt komponent med adekvat säkerhetsfunktionalitet finns tillgänglig i rätt tid.

4.3 Kostnadseffektivitet

Detta avsnitt ska motivera om realiserbarhetsbedömningen har genomförts med hänsyn till kostnadsdrivande aspekter såsom:

- informationsklassning – är den genomförd och motiverad
- återbruksmöjligheter av komponenter
- behov av högassuranskomponenter
- utveckling kontra kostnader
- komplexitet
- hög exponeringsnivå
- m.m.

4.4 Integration med system engineering

Detta avsnitt ska beskriva om det finns aspekter från övriga IT-systemområden inom system engineering som behöver lyftas i samband med realiserbarhetsbedömningen. Det kan vara beslut om specifika plattformar, COTS etc.
Information kan inhämtas från ISD-strategin.

4.5 Projektrisker

Detta avsnitt ska beskriva och bedöma de risker, ur ett informationssäkerhetsperspektiv, som finns i projektet som behöver tas hänsyn till och som uppmärksammas i analyserna. Tex avsaknad av komponenter som behövs för ackrediterbarhet, motstridiga verksamhetsbehov m.m.

4.6 PrL:s bedömning

Baserat på ovanstående bedömningar och analyser, samråd med SystGL, *bedöms/bedöms inte* *system X version Y* vara realiserbart och ackrediterbart.

Följande risker har identifierats och ska tas om hand i *Definiera:*

Realiserbarhetsbedömning är genomförd 20xx-xx-xx

PrL xxxxxxxx

SystGL IT-säk