<SYSTEM> <VERSION>

INFORMATIONSSÄKERHETSDEKLARATION *DEFINIERA* (ISD-D)

Inklusive 3 bilagor

Innehåll

1 Basfakta 8
1.1 Giltighet och syfte 8
1.2 Revisionshistorik 8
1.3 Terminologi och begrepp 8
1.4 Bilageförteckning 8
1.5 Referenser 8
2 Inledning 9
3 Översiktlig systembeskrivning 10
3.1 Avgränsningar 10
4 Sammanfattning 11
5 Realiserbarhetsbedömning 12
5.1 Ackrediterbarhet 12
5.2 Kostnadseffektivitet 12
5.3 Integration med system engineering 12
5.4 Projektrisker 12
5.5 PrL:s bedömning 12

Mallinformation 18FMV6730-4:1

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

Mallinstruktion

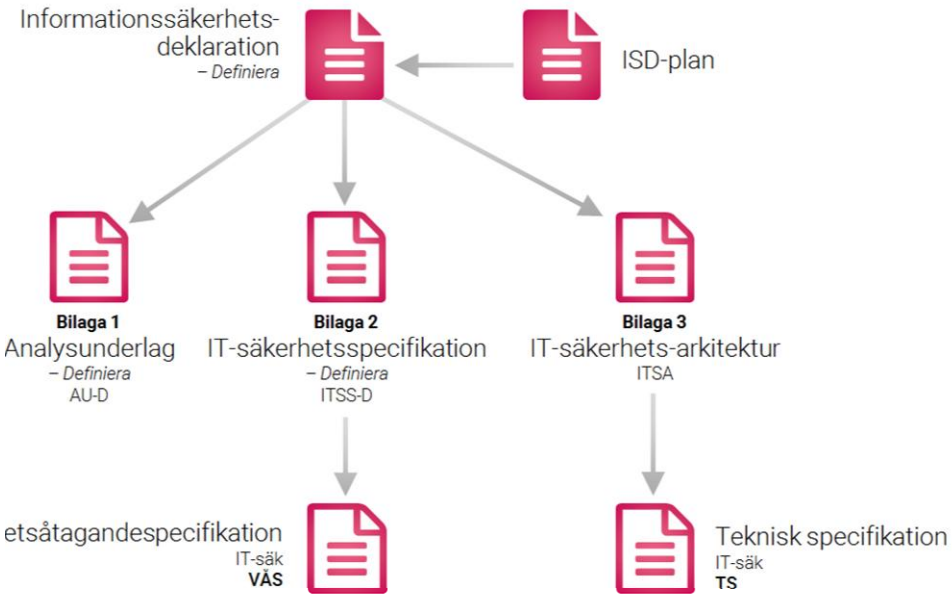
Denna mall ska användas för att ta fram dokumentet Informationssäkerhetsdeklaration *Definiera*, ISD-D. ISD-D utgör bedömning av realiserbarhet av aktuellt IT-system inför VHL FMV beslut S3 innan *Realisera*.

Det skarpa dokumentet börjar med kap 1 Basfakta. Sidorna innan dess innehåller beskrivningar kring vad ISD-D 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 *Definiera*

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



Figur 1 Dokumentstruktur Informationssäkerhetsdeklaration Definiera

Bilaga 1 - Analysunderlag *Definiera* (AU-D) utgör relevanta analyser avseende informations-säkerhetsaspekten ur ett systemperspektiv. Resultatet från AU-D i form av krav dokumenteras i bilaga 2 - IT-SäkerhetsSpecifikation (ITSS-D). Kraven och analyserna används för att ta fram bilaga 3 - IT-SäkerhetsArkitektur (ITSA).

Figur 1 Dokumentstruktur Informationssäkerhetsdeklaration Definieravisar relationen mellan ISD-D och upphandlingsunderlagen Teknisk specifikation (TS) och Verksamhetsåtagandespecifikation (VÅS). ISD-arbetet i *Definiera* ska resultera i TS och VÅS.

ITSS-D förser VÅS med krav på IT-säkerhetsarbete och ITSA förser TS med tolkade IT-säkerhetskrav.

ISD-plan, del av genomförandeprojektets projektplan, styr IT-säkerhetsarbetet och är ett viktigt indata till dokumentet Informationssäkerhetsdeklaration *Definiera* ISD-D. Upphandlingsunderlagen och ISD-plan är separata dokument och ingår inte i ISD-D.

Huvuddokumentet ISD-D omfattar:

- Framtagning av systembeskrivning av ackrediteringsobjektet.
- Slutsatser från bilagorna med viktiga aspekter tex:

    - Risker framtagna från risk- och sårbarhetsanalys
    - Specifika aspekter kring kravtolkning av MUST KSF som behöver lyftas upp för förståelse för realiserbarhetsbedömningen. Ex. loggfunktion implementeras i annat IT-system och är därför inte en säkerhetsfunktion i aktuellt IT-system.
    - Säkerhetskritiska gränsytor från ITSA
    - Återbruk av fastställda designregler
- Ytterligare aspekter kan läggas till vid behov
- Bedömning av realiserbarhet genomförs och dokumenteras inför upphandling och realisering.

Bilaga 1: AU-D omfattar:
- Utvärdering och eventuell utveckling av resultatet från *Identifiera* vid behov. Fler detaljer kring verksamheten och dess IT-system kan identifieras i *Definiera* vilket kan påverka kravarbetet och ge ytterligare underlag för bedömning avseende ackrediterbarhet.
- Fördjupad exponeringsanalys kopplat till ITSA
- Kompletterande Risk- och sårbarhetsanalys på framtagen IT-säkerhetsarkitektur.
- Ytterligare områden kan läggas till vid behov.

Bilaga 2: ITSS-D är det andra kravdokumentet i kedjan av krav för spårbarhet. ITSS-D ska vara utformat så att kravtolkning och kravnerbrytning av MUST KSF samt nerbrytning av tillkommande krav från verksamheten kan utläsas i kraven. ITSS-D omfattar:
- Vid behov, förtydligande av verksamhetens säkerhetskrav.
- Icke-funktionella krav (Assuranskrav) med avseende på IT-säkerhetsarbetet, som ska överföras till VÅS.
- Kravtolkning av MUST KSF, baserat på resultatet från AU-D.
- Ytterligare områden kan läggas till vid behov.

Bilaga 3: ITSA omfattar:
- IT-säkerhetsarkitektur för IT-system (ackrediteringsobjekt).
- kravfördelning var säkerhetsfunktionerna finns i IT-systemet,
- kravallokering från ITSS-D.
- Fastställda arkitektur- och designprinciper
- Funktionella krav (systemkrav) med avseende på IT-säkerhet, som ska överföras till TS

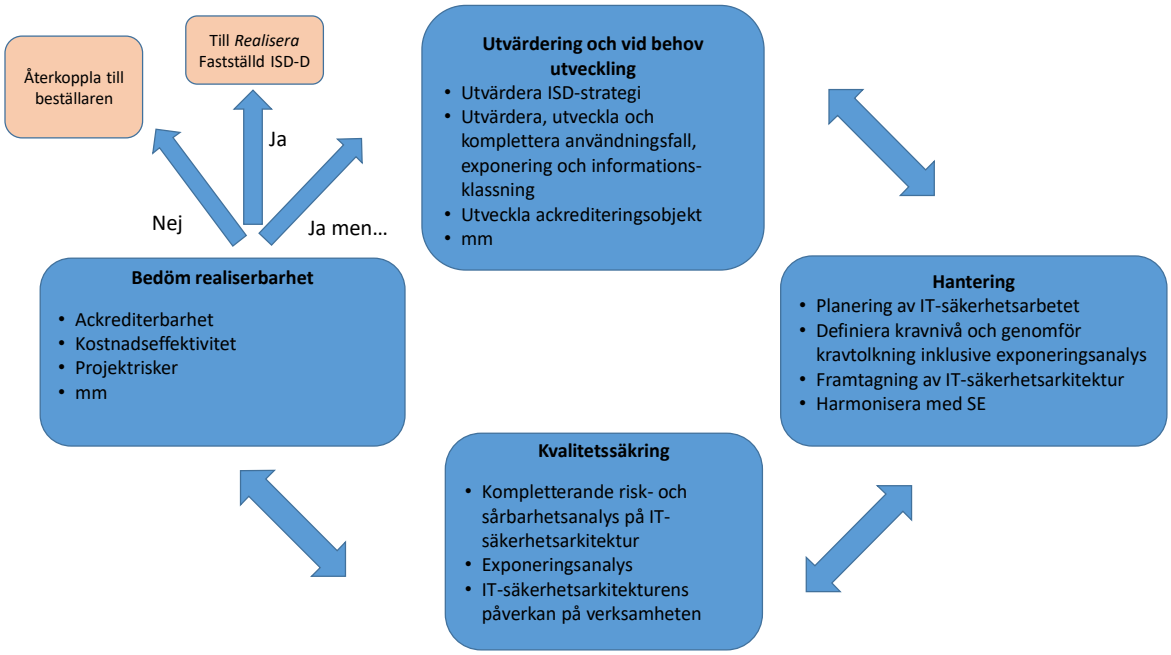
Att tänka på i arbetet med framtagning av Informationssäkerhetsdeklaration *Definiera (ISD-D)*

Definiera är genomförandeprojektets kravhanteringsskede och det är FMV projektledare (PL) som är ansvarig. Arbetet Informationssäkerhetsdeklaration *Definiera* omfattar aktiviteter såsom:

- Inhämtning och utvärdering av förutsättningar från *Identifiera* och PrL, vid behov görs ytterligare utveckling av den informationen.
- Kravhantering av IT-säkerhetsaspekterna på IT-systemet sker i samverkan med SE. Kraven tolkas mot verksamhetsbehoven så att rätt kravnivå sätts. Med utgångspunkt från det, formas en IT-säkerhetsarkitektur (ITSA) och en övergripande teknisk lösning för IT-systemet. I arbetet med att ta fram IT-säkerhetsarkitekturen visar också på krav på omgivning. Detta avser krav på angränsande IT-system, tex om vissa säkerhetsfunktioner ska lösas via omgivningen eller i samband med integration med andra system. Detta ger viktiga indata till leverantör inför upphandling så att rätt IT-system utvecklas.
- Kompletterande risk- och sårbarhetsanalys och exponeringsanalys görs på definierad IT-säkerhetsarkitektur för att bedöma kvarvarande risker. Exponeringsanalys för det aktuella IT-systemet är en vital aktivitet för att komma rätt i kravnivå och i förlängningen kunna leverera ett ackrediterbart IT-system.
- Realiserbarhetsbedömning ur ett informationssäkerhetsperspektiv genomförs med avseende på ackrediterbarhet, kostnadseffektivitet, integration med system engineering samt projektrisker. Notera att realiserbarheten inte är samma sak som ackrediterbarhet. Ett IT-system kan bedömas ackrediterbart men till priset av en hög kostnad och det blir då inte realiserbart. Resultatet dokumenteras i huvuddokumentet ISD-D.

Arbete måste göras inkrementellt i flera steg och det kan finnas fall där frågan måste tillbaka till Försvarsmakten eller till PrL i *Identifiera*, se Figur b. Utifrån varje ansats bedöms realiserbarhet och beslut tas om det finns behov av att fortsätta pröva nya lösningar. Görs bedömningen att det är realiserbart, men att det behövs göras vissa omvärderingar ur något perspektiv, tas ett nytt tag kopplat till verksamhetsbehov, kravtolkning och IT-säkerhetsarkitektur för att finjustera kravnivå inför realiserbarhetsbedömningen. Görs bedömningen att verksamheten kommer att påverkas mot ställda krav sker en återkoppling till PrL.

Blir realiserbarhetsbedömningen positiv fastställs ISD-D, upphandling sker och arbetet går över till *Realisera*.



Figur 2 Inkrementellt arbetssätt i Definiera

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

Aktiviteter i *Definiera* hanteras främst av PL, och vid behov, med stöd av rollerna Information Security Manager (ISM) och Information Security Architect (ISA).

1 Basfakta

1.1 Giltighet och syfte

Detta dokument är Informationssäkerhetsdeklaration Definiera (ISD-D) för <System> <version> inför FMV VHL S3-beslut.

Syftet med ISD-D är dels att dokumentera beslut avseende bedömning av realiserbarhet, dels att formulera krav och säkerhetsarkitektur inför upphandling. Kraven i Bilaga 2 (ITSS-D) och Bilaga 3 (ITSA) är underlag till VÅS respektive TS.

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-D
Bilaga 2. ITSS-D
Bilaga 3. ITSA

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>

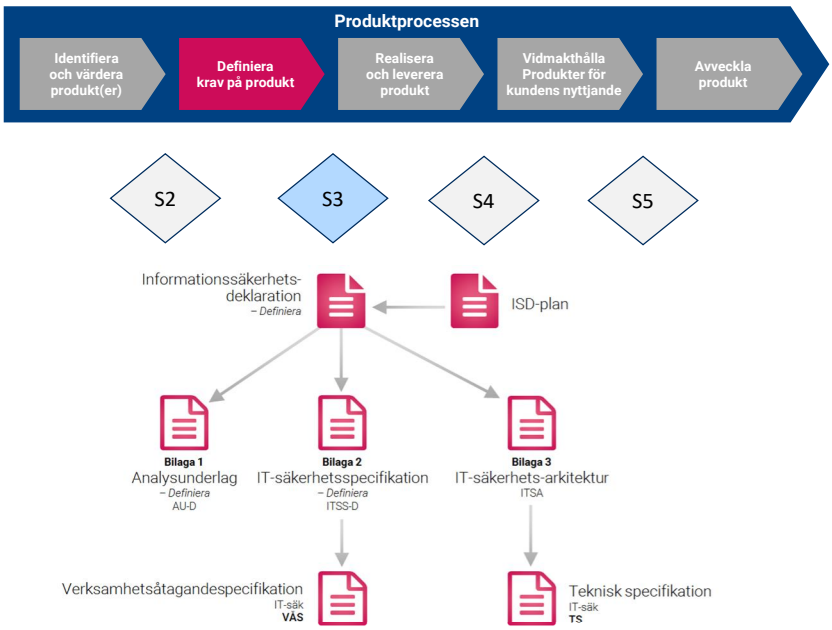
Tabell 3 - Referenser

2 Inledning

Definiera är genomförandeprojektets primära kravhanteringsskede. I *Definiera* kravställs IT-säkerhetsaspekterna, kraven tolkas mot verksamhetsbehoven och med utgångspunkt från det så formas IT-systemets IT-säkerhetsarkitektur. *Definiera* formar den tekniska lösningen för systemet.

Realiserbarhetsbedömningen har baserats på att:

- upphandlingsunderlaget till leverantör baseras på att realiserbarhet av systemet är bedömt på relevanta analyser och kravtolkningar.
- IT-säkerhetsarkitekturen visar på att avvägningar har genomförts för att minska exponering som i sin tur innebär kostnadseffektivitet och minimering av projektrisker.
- IT-säkerhetsarbetet är harmoniserat med övrigt SE-arbete för att de rätta avvägningarna mot ex funktionalitet ska kunna göras.
- IT-säkerhetsarkitekturen visar på system av system i det fall det är aktuellt.
- fastställda designregler används och återbrukas i det fall där det är möjligt. Designreglerna ska underlätta för bedömning av realiserbarheten.



Figur 1: Definiera och dokumentstruktur

3 Översiktlig systembeskrivning

Detta avsnitt ska fördjupa beskrivningen (vid behov med utgångspunkt från resultatet från *Identifiera)* av det aktuella ackrediteringsobjektet, dvs det IT-system som är i fokus för informationssäkerhetsarbetet.

- Bestäm vilka IT-säkerhetskrav som ackrediteringsobjektet ska uppfylla och vad som ska hanteras av krav på omgivningen.
- Systembeskrivningen ska innehålla IT-systemets säkerhetsfunktioner
- Återbrukbara komponenter/IT-system
- Gränsytor till andra IT-system
- GFE (Government Furnished Equipment)
- Fastställda designregler

3.1 Avgränsningar

Under denna rubrik anges ackrediteringsobjektets avgränsning. En väl definierad avgränsning underlättar ackrediteringen av systemet.

4 Sammanfattning

Detta avsnitt ska ge en sammanfattning av bilaga 1 – AU-D och bilaga 3 – ITSA. Sammanfattningen ska innehålla de aspekter som har stor påverkan på realiserbarhetsbedömningen såsom:

- verksamhetsbehov som är dimensionerande för IT-säkerheten och som berör genomförd kravtolkning
- risker
- kostnadsdrivande krav
- användande av fastställda designregler/principer
- hur bedömning av exponerings- och konsekvensnivån är genomförd
- återbruk av komponenter

5 Realiserbarhetsbedömning

Detta avsnitt ska ange huruvida aktuellt ackrediteringsobjekt bedöms realiserbart ur ett informationssäkerhetsperspektiv inför FMV VHL S3-beslut och för att gå vidare till *Realisera*. Bedömningen görs med utgångspunkt från analyserna i bilaga 1-AU-D och bilaga 3- ITSA.

5.1 Ackrediterbarhet

Ackrediterbarhet är en bedömning av hur IT-systemet 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 finns tillgänglig i rätt tid

5.2 Kostnadseffektivitet

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

- Säkerhetslösningen – är den balanserad?
- informationssäkerhetsklassificering – är den genomförd och motiverad?
- återbruksmöjligheter av komponenter
- behov av högassuranskomponenter
- m.m.

5.3 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-Plan.

5.4 Projektrisker

Bedömning av kvarvarande projektrisker inför Realisera:

- Är säkerhetslösningen i harmoni med System Engineering lösningen?
  - Vilka eventuella konsekvenser på systemets funktionella krav blir det givet den tänkta säkerhetsarkitekturen (utifrån krav på ackrediterbarhet)?
  - Vilka bedömningar har gjorts för att åtgärda dessa konsekvenser?

5.5 PrL:s bedömning

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

Realiserbarhetsbedömning är genomförd 20xx-xx-xx

PrL xxxxxxxx

SystGL IT-säk