<SYSTEM> <VERSION>

INFORMATIONSSÄKERHETSDEKLARATION *REALISERA* (ISD-R)

Inklusive 3 bilagor

Innehåll

Mallinformation 18FMV6730-6:1

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

Mallinstruktion

Denna mall ska användas för att ta fram dokumentet Informationssäkerhetsdeklaration *Realisera*, ISD-R.

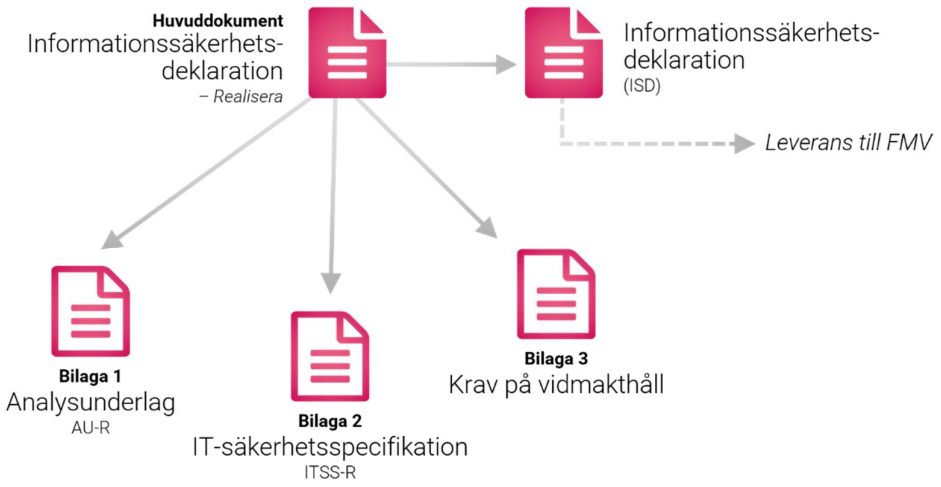
ISD-R är underlaget till Informationssäkerhetsdeklarationen ISD för aktuellt IT-system inför FMV VHL beslut S4.

Det skarpa dokumentet börjar med kap 1 Basfakta. Sidorna innan dess innehåller beskrivningar kring vad ISD-R 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 *System* med systemets namn.
- Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.

Omfattning av Informationssäkerhetsdeklaration *Realisera*

Informationssäkerhetsdeklaration *Realisera* (ISD-R) består av ett huvuddokument och tre bilagor. Huvuddokumentet (ISD-R) är underlag inför FMV:s Informationssäkerhetsdeklaration (ISD) till FM. I det fall IT-systemet ska vara föremål för återbruk, vidmakthåll eller är ett delsystem i en större helhet blir ISD-R ett internt FMV-dokument.



Figur 1Dokumentstruktur Informationssäkerhetsdeklaration Realisera.

Bilaga 1-Analysunderlag (AU-R) utgör de analyser som behöver genomföras inför ISD-R.

Bilaga 2-IT-SäkerhetsSpecifikation ITSS-R, motsvarar FM ITSS och utgör bedömningsunderlaget avseende kravuppfyllnad inför ISD-R. Beroende på omfattning/komplexitet på IT-systemet kan ITSS-R i sig omfatta flera bilagor t.ex. dokumentation av genomförda kompletterande tester.

Bilaga 3- Krav på Vidmakthållande VMH-R, anger krav på hur IT-systemet ska vidmakthållas för att bibehålla informationssäkerhetsnivån (dvs säkerhetskrav på omgivningen).

Informationssäkerhetsdeklaration (ISD)omfattar:

- Deklaration avseende bedömd kravuppfyllnad.
- Eventuella observationer i form av avvikelser från angivna IT-säkerhetskrav och dess konsekvenser.
- En deklaration om att IT-säkerhetslösningen för systemet är utformad med utgångspunkt från Försvarsmaktens krav på tolererbar risk.
- En deklaration om att det säkerhetstekniska underlaget för systemet (ITSS-R) är utformat enligt den norm som kravställts inom FMV.
- En deklaration om att IT- säkerhetsarbetet har följt fastställd ISD-plan.

Huvuddokumentet ISD-R omfattar:

- Sammanfattning och slutsatser inhämtade från respektive bilaga.
- En realiserbarhetsbedömning av TC och SystGL
- Ett fastställande av såväl ISD-*R* som av Informationssäkerhetsdeklaration (ISD).
- Hur avvikelser från kravuppfyllnaden ska hanteras.
- Information avseende yttrandet från oberoende granskning som genomförts av SystGL.
- mm

Bilaga 1: AU-R omfattar:

- Analys av leverantörens underlag.
- Riskanalys på resterande brister.
- Krav på omgivning.
- mm

Bilaga 2: ITSS-R omfattar:

- Systembeskrivning
- Sammanställning av säkerhetskrav
- Säkerhetskrav på omgivningen
- Tolkning av säkerhetskrav
- Uppfyllande av säkerhetskrav
- mm

Bilaga 3: Krav på vidmakthållande

- Säkerhetskrav på omgivningen

Att tänka på i arbetet med framtagning av Informationssäkerhetsdeklaration *Realisera* (ISD-R)

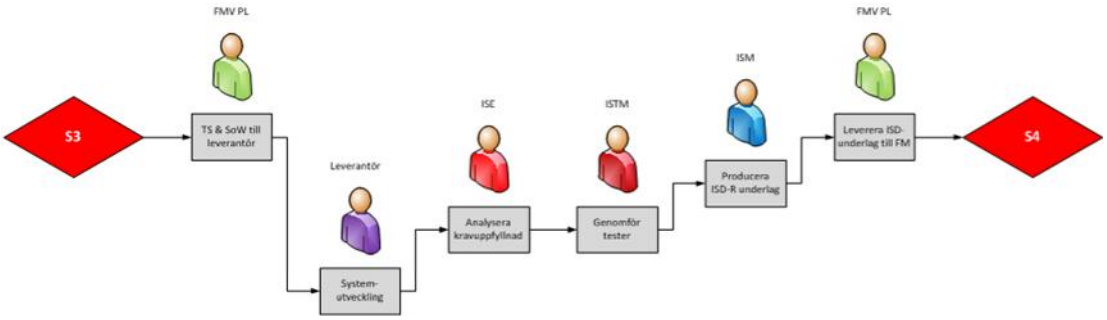
Realisera är genomförandeprojektets utvecklingsskede och leverans. FMV PL är ansvarig men stöd kan tas ifrån rollerna; ISM (Information Security Manager), ISE (Information Security Evaluator) och ISTM (Information Security Test Manager) där ISE genomför huvuddelen av arbetet.

I *Realisera* utgör huvuddokumentet ISD-R underlag för IT-systemets Informations-säkerhetsdeklaration vilken dokumenteras i separat dokument (ISD). I det fall IT-systemet ska användas för återbruk och/eller system av system internt för FMV, utgör huvuddokumentet ISD-R ackrediteringsunderlaget.

Figur 2 Aktiviteter i Realiserabeskriver arbetsordningen och övergripande aktiviteter såsom:

- Analysera kravuppfyllnad avseende informationssäkerhet och dess hållbarhet för leverans. I arbetet med bedömning av kravuppfyllnaden ska analys ske av kvarvarande eventuella brister (restriskanalyser), och vilka konsekvenser dessa brister kan få.
- Genomför kompletterande tester. Bedömning av kravuppfyllnad omfattar även bedömning av hur verifiering av kraven har genomförts och vid behov kan ytterligare tester behöva genomföras.
- Producera ISD-R underlag och ISD, anskaffa yttrande från SystGL och önskvärt är även samråd från MUST. Leveransen till FM kan även omfatta krav på omgivning dvs. FMV deklarerar att informationssäkerhetskraven är uppfyllda under förutsättning att FM uppfyller angivna krav på omgivning i form av fysisk skydd, krav på driftmiljö etc.
- Leverera ISD-underlag till FMV

Vid positivt resultat från yttranden från SystGL fortsätter projektet till fastställande av TC och leverans till FM, eventuellt efter komplettering av underlaget. Vid negativt resultat från yttranden kan större åtgärder krävas av projektet.



Figur 2 Aktiviteter i Realisera

Nedan beskrivs aktiviteter för respektive roll. Observera att angivna aktiviteter är typiska val av aktiviteter för ISD-R. Det är genomförandeprojektets behov som styr vilka aktiviteter som ska genomföras.

Aktiviteter för FMV PL:

- Initiering av aktiviteter i *Realisera* och vid behov initiering av roller för genomförande.
- Bedömning av resultatet genererade av rollerna ISE och ISTM.
- Initiera yttrande och oberoende granskning av SystGL.
- Ta fram ISD-R.
- Ta fram Informationssäkerhetsdeklaration (ISD) till FM.
- Initiera och sök utlåtande från MUST för ITSS-R.
- Initiera och förbered granskning i FMV CCB.
- Bedöma och dokumentera krav på hur IT-systemet ska vidmakthållas efter leverans med bibehållen informationssäkerhetsnivå.
- Sätt upp kriterier för vilka förändringar som ska ge upphov till omackreditering, av IT-systemet samt hur dessa förändringar ska hanteras.
- Färdigställ leverans

Aktiviteter för ISE (för detaljer, se ISE granskningsinstruktion, bilaga 2 till 18FMV6730-8):

- Analys och bedömning av leverantörens underlag. Leverantören ska leverera och visa på kravuppfyllnad för i TS ställda IT-säkerhetskrav. Kravuppfyllnaden ska vara verifierad enligt FMVs ställda krav i VÅS. Underlaget ska vara av den kvaliteten att FMV kan återanvända merparten i sin leverans till FM. Bedömning görs även avseende på avvikelser mot krav, testtäckning mm. Analysen dokumenteras i Bilaga 1 AU-R.
- Analysera och genomföra kravuppfyllnad mot av FMV kompletterande informationssäkerhetskrav. Dokumenteras i ITSS-R.
- Initiera framtagning av ITSS-R. Här sker även dokumentation av krav på omgivning i de fall informationssäkerhetskraven inte löses med IT-systemets tekniska säkerhetslösning. Genomförs av rollen ISE (Information Security Evaluator) och dokumenteras i bilaga 3, VMH-R.
- Definiera kompletterande test i det fall det finns tveksamheter kring kravuppuppfyllnad och om det finns specifika IT-säkerhetslösningarna som behöver testas mer. Tester genomförs av ISTM (Information Security Test Manager).
- Analysera kvarvarande brister och bedöm konsekvenserna. Dokumenteras i AU-R.
- Påvisa att informationssäkerhetsarbetet har genomförts i enlighet med genomförandeprojektets ISD-plan.

Aktiviteter för ISM:

- Koordinera informationssäkerhetsarbetet i *Realisera*
- Sammanställ resultatet från ISE:s och ISTM:s aktiviteter och ta fram underlag till PL för bedömning av IT-säkerhetslösningen inför deklaration
- Stödja PL i paketering av underlag till CCB

Aktiviteter för ISTM:

- Koordinering av testverksamhet i det fall kompletterande tester är beslutade att genomföras för att ytterligare kvalitetssäkra bedömningen av kravuppfyllnad.
- Genomförande av identifierade tester

- Analysera och dra slutsatser från genomförda tester
- Producera testrapport
- Vid behov samverka med FMV T&E

1 Basfakta

1.1 Giltighet och syfte

Detta dokument är Informationssäkerhetsdeklaration *Realisera* (ISD-R) för <System> <Version> inför FMV VHL S4-beslut.

Syftet med Informationssäkerhetsdeklaration *Realisera* är att visa på att det aktuella IT-systemet levereras till FM enligt de, för IT-systemet, ställda IT-säkerhetskrav. Syftet är också att påvisa att informationssäkerhetsarbetet har genomförts i enlighet med genomförandeprojektets ISD-plan samt att levererat IT-system uppfyller de ställda IT-säkerhetskraven verifierade med de för kraven relevanta metoder.

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	Kommentarer/ Anmärkningar
<term>	<Definition>	
<term>	<Definition>	
<term>	<Definition>	

1.4 Bilageförteckning

Bilaga 1. AU-R
Bilaga 2. ITSS-R
Bilaga 3. VMH-R

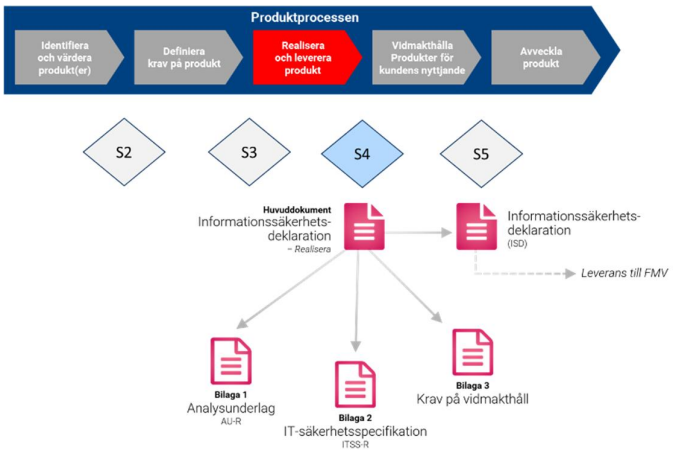
1.5 Referenser

Dokumenttitel	Dokumentbeteckning	Utgåva nr
[1] ISD 3.0 Begrepp och förkortningar	18FMV6730-8:1.1	1
[2] ISE Granskningsinstruktion	18FMV6730-8:1.2	1
[3] SystGL Granskningsinstruktion	18FMV6730-8:1.3	1

Tabell 2 - Referenser

2 Inledning

Detta dokument utgör Informationssäkerhetsdeklaration *Realisera* för <System> inför FMV VHL S4-beslut.



Figur 3 ISD-R i Realisera

Dokumentet är huvuddokumentet som sammanställer analyser och bedömd kravuppfyllnad från tillhörande bilagor. Den formella informationssäkerhetsdeklarationen till FM dokumenteras i Informationssäkerhetsdeklaration (ISD).

Inledningen ska ge den bakgrundsinformation kring IT-systemet som krävs för att läsaren tydligt ska veta vilket IT-system deklarationen avser samt om förutsättningar gäller för vidare läsning.

3 Sammanfattning av AU-R och ITSS-R

Detta avsnitt ska innehålla en sammanfattning av de dimensionerande aspekterna inför deklarationen såsom:

- Riskanalys på kvarvarande brister och dess betydelse för leveransen.
- Sammanfattning av resultatet från granskningen utförd av ISE när det gäller kravuppfyllnad av IT-säkerhetskrav på IT-systemet men även kravuppfyllnad avseende dokumentation, utvecklingsmiljö, leveransprocess mm, se mall för AU-R bilaga 1.
- Krav på omgivning utifrån FMVs informationssäkerhetsperspektiv (IT- och driftmiljö inklusive fysisk och organisatorisk miljö) som är vitalt för kravuppfyllnaden.

3.1 Systemets säkerhetsfunktioner

Säkerhetsfunktioner är beskriva i ITSS-D, med eventuella kompletteringar eller ändringar i ITSS-R, och ligger till grund för kraven i TS. I ITSS-R granskas hur dessa är implementerade och eventuella brister identifieras. Restriskanalys efter genomförda granskningar är dokumenterad i AU-R.

Sammanfatta resultatet av kravuppfyllnad av säkerhetsfunktioner och restriskanalysen.

3.2 Leverantörens åtagande

Krav på leverantörens åtagande, avseende informationssäkerhet, är beskriva i ITSS-D, med eventuella kompletteringar eller ändringar i ITSS-R, och ligger till grund för kraven i VÅS. I ITSS-R granskas hur dessa är genomförda och eventuella brister identifieras.

Sammanfatta resultatet av kravuppfyllnad av leverantörens åtagande avseende informationssäkerhet.

3.3 ISE Analyser

I AU-R återfinns resultatet av ISE oberoende granskningar, vilka är specificerade i ISE Granskningsinstruktion (ref [2]).

Sammanfatta resultatet av ISE analyser.

3.4 SystGL yttrande

För in SystGL yttrande avseende oberoende analyser av informationssäkerheten i systemen, leverantörens åtagande samt kvalitén på ISD-underlagen.

Stöd till detta yttrande kan hämtas i ISE Granskningsinstruktion (referens [2]) och SystGL Granskningsinstruktion (referens [3]).

4 Ackrediterbarhetsbedömning

Detta avsnitt ska ange huruvida aktuellt IT-system (ackrediteringsobjekt) bedöms ackrediterbart.

4.1 Kvarvarande brister

Bedömning av kvarvarande brister inför leverans. Observera att detta avsnitt kan vara föremål för sekretessklassning.

4.2 PrL:s bedömning

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

Ackrediterbarhetsbedömning är genomförd 20xx-xx-xx

PrL

SystGL IT-Säk