Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(11)

<SYSTEM> <VERSION>

ANALYSUNDERLAG

REALISERA (AU-R)

Innehåll

1 Basfakta 5
1.1 Giltighet och syfte 5
1.2 Revisionshistorik 5
1.3 Terminologi och begrepp 5
1.4 Bilageförteckning 5
1.5 Referenser 5
2 Inledning 6
2.1 Omfattning och avgränsningar 6
3 ISE Analyser och granskningar 7
3.1 Dokumentgranskning 7
3.2 Utvecklingssäkerhet 8
3.3 ISE Analyser 8
3.3.1 Systemets säkerhetsarkitektur 8
3.3.2 Publik sårbarhetsanalys 8
3.3.3 Attackytor 8
3.3.4 Oberoende Sårbarhetsanalys 9
3.4 Test 9
3.4.1 Verifiering av leverantörens tester 9
3.4.2 Kompletterande testfall 9
3.5 Kontroll 9
3.6 Egenkontroll 10
4 Kvarvarande brister 11
4.1 Identifiering av kvarvarande brister 11
4.2 Restriskanalys 11
4.3 Övriga analyser kring kravuppfyllnad i ITSS-R 11

Mallinformation 18FMV6730-6:1.1

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

Mallinstruktion

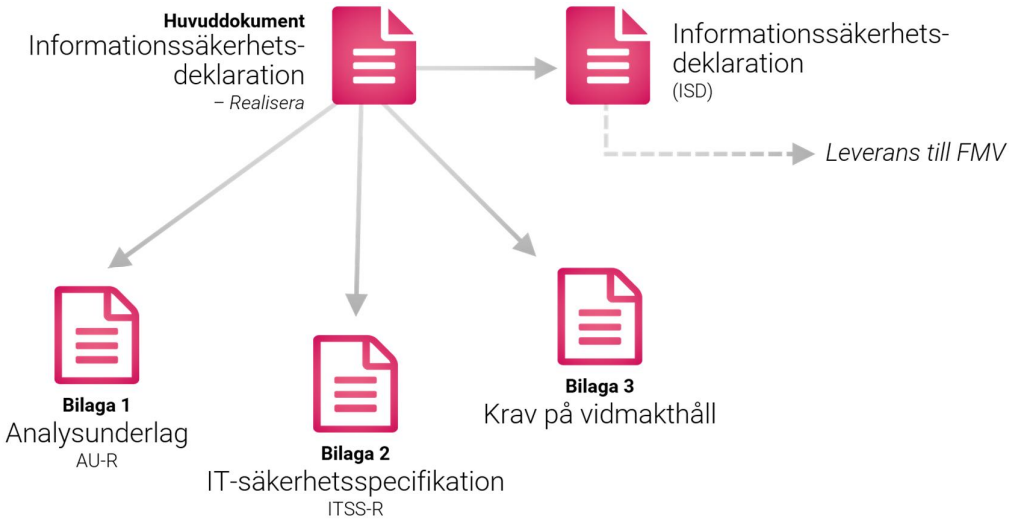
Denna mall ska användas för att ta fram dokumentet Analysunderlag *Realisera* som är en bilaga till ISD-R. ISD-R är underlaget till Informationssäkerhetsdeklarationen för aktuellt IT-system inför VHL FMV beslut S4.

Det skarpa dokumentet börjar med kap 1 Basfakta. Sidorna innan dess innehåller beskrivningar kring vad AU-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 anges i en punktlista under respektive rubrik. Gulmarkerad text ska raderas innan dokumentet färdigställs.
- Text som är skriven utan punktlista är text som kan användas också i det färdigställda dokumentet.
- Ersätt Systemnamn med ackrediteringsobjektets namn.
- Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.

Omfattning av Analysunderlag *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. Denna mall utgör bilaga 1 - AU-R.



Figur 1 Dokumentstruktur Informationssäkerhetsdeklaration Realisera

Bilaga 1: AU-R omfattar:

- ISE Analys av leverantörens underlag
- ISE oberoende analyser
- ISE Restriskanalys och dess konsekvenser för IT-systemet
- mm

Att tänka på i arbetet med framtagning av Analysunderlag *Realisera* (AU-R)

Analysunderlaget *Realisera* (AU-R) ska stödja FMV:s realiserbarhetbedömning i ISD-R och Informationssäkerhetsdeklaration (ISD) inför leverans till FM. Analysunderlaget i *Realisera* är därför inte ett underlag vars resultat dokumenteras i ITSS-R, såsom syftet med analysunderlagen AU-I och AU-D, utan till stora delar en analys av resultatet från bedömningen av kravuppfyllnad i ITSS-R. AU-R omfattar också analysen av leveransen från leverantören. Analyserna genomförs företrädesvis av rollen ISE (Information Security Evaluator).

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

- Analys av leverantörens underlag. Leverantören ska leverera och visa på kravuppfyllnad för 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.
- Analys av bedömd kravuppfyllnad i ITSS-R och eventuella kvarvarande brister
- Definiera behov avseende kompletterande tester och informera ISTM Information Security Test Manager
- Identifiera krav på omgivning

1 Basfakta

1.1 Giltighet och syfte

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

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

Detta dokument har inga bilagor.

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

Tabell 3 - Referenser

2 Inledning

Inledningen ska ge en tydlig bakgrund för läsaren för att öka förståelsen för genomförda analyser.

2.1 Omfattning och avgränsningar

Ange omfattning och eventuella avgränsningar för analyserna.
Se ISE Granskningsinstruktion, referens [2], för omfattning avseende granskningsaktiviteter.

3 ISE Analyser och granskningar

I upphandling kravställs leverantören med avseende på hur IT-säkerhetsarbetet ska bedrivas, hur det ska dokumenteras m.m. för att underlätta för FMV i arbetet med kravuppfyllnad och bedömning av IT-säkerhetslösningen. Detta avsnitt dokumenterar analysen av underlaget från leverantören med avseende på nivå på kravuppfyllnad och hur kravuppfyllnaden kan verifieras. I det fall underlaget från leverantören inte bedöms ge det stöd i bedömningen av kravuppfyllnaden som krävs ska leverantören kontaktas och en plan ska tas fram som beskriver hur upprättande av dokumentationen ska genomföras.

3.1 Dokumentgranskning

Omfattningen av dokumentgranskningen bestäms av vald kravnivå. Beskrivning av dessa aktiviteter beskrivs i ISE Granskningsinstruktion, ref [2]. Resultatet av dokumentgranskningarna kan dokumenteras här eller i ITSS-R.

ISE ska verifiera att informationen i leverantörens underlag möter alla krav på innehåll och presentation.

Underlag som kan vara aktuella att granska är:

- Beskrivning av utvecklingsmiljön
- Beskrivning av konfigurationsledningssystem
- Leveransrutiner
- Processer för hantering av säkerhetsrelevanta brister
- Beskrivning av systemets gränsytor
- Dataflödesanalyser
- Designdokumentation
- Installations- och konfigurationsanvisningar
- Drift- och förvaltningsdokumentation
- Administrativa rutiner avseende
    - Behörighetsadministration
    - Säkerhetsattribut
    - Intrångsdetektering
    - Säkerhetsuppdateringar
    - Konfigurationsstyrning
    - Utbildning
- Testdokumentation avseende
    - Funktionella krav
    - Penetrationstest
- Avvikelseanalys
- Sårbarhetsanalys

Dokument	Kommentar till analys	Utlåtande

Tabell 4 Dokumentgranskning

3.2 Utvecklingssäkerhet

ISE ska verifiera att leverantören tillämpar dokumenterade rutiner och processer avseende

- Utvecklingssäkerhet
- Konfigurationsledning
- Livscykelmodell

Utvecklings-säkerhet avseende	Kommentar till analys	Utlåtande
Utvecklingssäkerhet		
Konfigurations-ledning		
Livscykelmodell		

Tabell 5 Site-Visit

3.3 ISE Analyser

3.3.1 Systemets säkerhetsarkitektur

ISE ska analysera beskrivningen av systemets säkerhetsarkitektur och verifiera att det inte går att kringgå systemets säkerhetsfunktioner.

Analys avseende	Kommentar till analys	Utlåtande

Tabell 6 Systemets Säkerhetsarkitektur

3.3.2 Publik sårbarhetsanalys

ISE ska använda tillgängliga källor för att komplettera leverantörens dokumentation, t.ex. publik sårbarhetsinformation.

Analys avseende	Kommentar till analys	Utlåtande

Tabell 7 Publik sårbarhetsanalys

3.3.3 Attackytor

ISE ska analysera, med hjälp av leverantörens dokumentation och övrig tillgänglig information, systemets komponenter och gränsytor och kartlägga deras beroenden i syfte att identifiera attackytor och eventuella svagpunkter i arkitekturen.

Analys avseende	Kommentar till analys	Utlåtande

Tabell 8 Attackytor

3.3.4 Oberoende Sårbarhetsanalys

ISE ska genomföra en oberoende, metodisk och semiformell sårbarhetsanalys av systemet baserad på all tillgänglig information och erfarenhet för att identifiera potentiella sårbarheter i systemet.

Analys avseende	Kommentar till analys	Utlåtande

Tabell 9 Oberoende sårbarhetsanalys

3.4 Test

3.4.1 Verifiering av leverantörens tester

ISE ska, om denne finner det nödvändigt, upprepa ett representativt antal av systemutvecklarens tester och bekräfta att systemutvecklarens testresultat för dessa testfall överensstämmer med testspecifikationen.

Testfall	Resultat av verifiering	Utlåtande

Tabell 10 Verifiering av leverantörens tester

3.4.2 Kompletterande testfall

ISE ska analysera systemutvecklarens testfall och komplettera dessa testfall med egna testfall.

ISE eller ISTM ska genomföra de egna testfallen, dokumentera resultatet och bekräfta att systemet fungerar enligt specifikation.

ISE eller ISTM ska genomföra praktiska tester av systemet för att avgöra om de identifierade potentiella sårbarheterna kan utnyttjas i den tänkta användningen av systemet.

Testfall	Testresultat	Utlåtande

Tabell 11 Kompletterande tester

Om de kompletterande testerna blir omfattande ka de med fördel dokumenteras i ett separat underlag. För i så fall in resultatet av de kompletterande testerna i tabellen ovan.

3.5 Kontroll

ISE ska tillämpa åtgärderna i installationsdokumentation för att verifiera att systemet kan mottagas och installeras på ett säkert sätt genom att följa beskrivningen av dem.

Kontroll	Resultat	Utlåtande
Leveransrutiner		
Installations-anvisningar		

Tabell 12 Kontroller

3.6 Egenkontroll

ISE ska verifiera att alla evalueringsaktiviteter är genomförda med godkänt resultat.

Egenkontroll	Resultat	Utlåtande
Evalueringsaktiviteter		

Tabell 13 Kontroller

4 Kvarvarande brister

Efter genomförd kravuppfyllnad dokumenterad i Bilaga 2-ITSS-R kan det finnas krav som inte är uppfyllda av IT-systemets tekniska IT-säkerhetsfunktioner och detta innebär kvarvarande brister efter leverans.

Detta avsnitt dokumenterar analysen av dessa brister samt förslag på åtgärder. Åtgärderna kan innebära införande av krav på omgivning d.v.s. kraven uppfylls inte med den tekniska lösningen utan tex med en fysisk lösning.

4.1 Identifiering av kvarvarande brister

Nedanstående tabell beskriver identifierade brister.

Brist nr	Beskrivning

Tabell 14 Kvarvarande brister

4.2 Restriskanalys

ISE ska genomföra restriskanalys för att identifiera kvarvarande osäkerheter kring systemets IT-säkerhetsförmågor.

Analys av konsekvenser avseende identifierade brister genomförs och dokumenteras nedan. Förslag på åtgärd kan vara krav på omgivning. Förslag på krav på omgivning dokumenteras och förs in i bilaga 3, VMH-R som en förutsättning för överlämning till FM.

ISE ska dokumentera resultatet av restriskanalysen i en form och med ett språkbruk som är tydligt och ger den avsedda mottagaren rätt underlag inför beslut om ackreditering.

Nedanstående tabell beskriver identifierade brister, dess konsekvenser samt förslag på åtgärd.

Brist nr	Beskrivning
Beskrivning:	
Konsekvens:	
Förslag på åtgärd:	

Tabell 15 Restriskanalys

4.3 Övriga analyser kring kravuppfyllnad i ITSS-R

Detta avsnitt är en placeholder för behov av andra typer av analyser som kan behöva genomföras av resultatet från ITSS-R. Analyserna kan exempelvis vara behov av kompletterande tester, kommentarer kring testtäckning mm.