Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(15)

<SYSTEM> <VERSION>

IT-SÄKERHETSSPECIFIKATION *VIDMAKTHÅLLA* (ITSS-V)

Innehåll

Mallinformation 18FMV6730-7:1.2

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Mall för ITSS-V	DAOLO

Mallinstruktion

Denna mall ska användas för att ta fram dokumentet IT-säkerhetsspecifikation *Vidmakthålla*, ITSS-V. ITSS-V utgör bedömning av kravuppfyllnad avseende informationssäkerhet efter beslutad förändring av systemet.

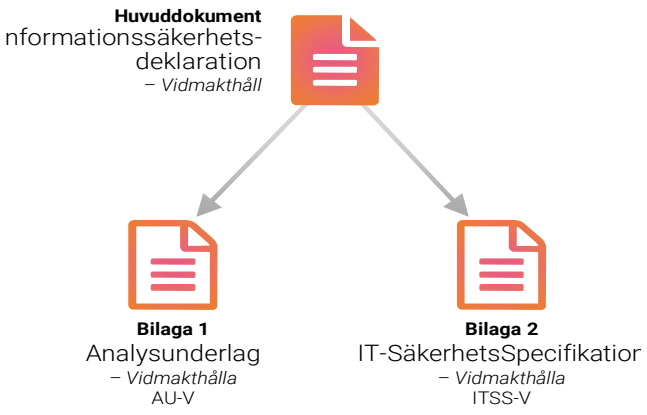
Det skarpa dokumentet börjar med kap 1 Basfakta. Sidorna innan dess innehåller beskrivningar kring vad ITSS-V är, arbetssätt, innehåll och att tänka på i arbetet. Dessa sidor tas bort i det skarpa dokumentet.

- 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 ITSS-V

Informationssäkerhetsdeklaration *Vidmakthålla* (ISD-V) består av ett huvuddokument och två bilagor. Huvuddokumentet utgör realiserbarhetsbedömningen av systemet med avseende på stor eller liten ändring och ändringens eventuella påverkan på systemets informations-säkerhetslösning.

Denna mall omfattar bilaga 2 ITSS-V och utgör den kravuppfyllnad med avseende på informationssäkerhet som ligger till grund för systemets ackreditering.



Figur 1 Dokumentstruktur Informationssäkerhetsdeklaration Vidmakthålla

ITSS-V omfattar:

- Sammanställning av säkerhetskrav (ändringar)
- Tolkning av säkerhetskrav/arkitektur (ändringar)
- Uppfyllande av säkerhetskrav (ändringar)
    - Motivering och bedömning
    - Avvikelse
- Krav på omgivningen
- Kvarvarande risk

Att tänka på i arbetet med att ta fram ITSS-V

Arbetet med att ta fram ITSS-V baseras på den uppdatering av informationssäkerhetskraven som bedömd förändring medför. Bedöms förändringen som stor, tas en ny ITSS-R fram och granskningen sker av ny kravställning. Bedöms det att en tilläggsackreditering genomförs görs granskningen av kravuppfyllnaden med utgångspunkt från genomförd deltaanalys, d.v.s. skillnaden mellan den senaste versionen av ITSS-R (vid flera versioner av förändringar ITSS-V) och önskad förändring.

Granskningen initieras av genomförandeprojektet och genomförs företrädesvis av rollen ISE. Vilka aktiviteter ISE ska genomföra beskrivs i separat ISE Granskningsinstruktion, bilaga 2 till 18FMV6730-8.

1 Basfakta

1.1 Giltighet och syfte

Detta kapitel ska entydigt identifiera systemet.

Detta dokument är IT-säkerhetsspecifikation *Vidmakthålla* (ISD-V) för <System> <version>.

Syftet med ITSS-V är att dokumentera granskning av kravuppfyllnad med avseende på informationssäkerhetskrav för det aktuella systemet. Bedömning av realiserbarhet dokumenteras i ISD-V.

1.2 Revisionshistorik

Detta kapitel ska entydigt identifiera detta dokument.

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

N/A

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

ITSS-V är en bilaga till huvuddokumentet ISD-V och omfattar sammanställning av informationssäkerhetskrav samt krav på omgivning. ITSS-V följer struktur på ITSS-R.

2.1 Syfte

ITSS-V är en bilaga till huvuddokumentet ISD-V och omfattar bedömning av kravuppfyllnad för <Systemnamn>. ITSS-V följer struktur på ITSS-D och ITSS-R för kontinuitet och återanvändning av information.

2.2 Kravnivå

I *Definiera* fastställd kravnivå enligt FM MUST KSF version XX för aktuellt system är: *Grund/Utökad/Hög*.

2.3 Systemöversikt

Systemöversikten ska kortfattat beskriva systemets användning och säkerhetsmekanismer samt dess övergripande systemarkitektur. Beskrivningen ska ge en översiktlig bild över systemets IT-säkerhetsförmåga och dess tänkta användning.

Använd systemöversikten i ITSS-R som utgångspunkt.

Figur Systemöversikt

Figur 2 Systemöversikt

3 Systembeskrivning

I detta kapitel ges en utförlig beskrivning av systemet. I beskrivningen definieras systemets förutsättningar, arkitektur, gränsytor samt säkerhetsförmågor.

Systemets arkitektur ska lista systemkomponenter och beskriva hur de tillsammans bygger upp systemet.

Systemets alla logiska och fysiska gränsytor ska beskrivas för att ge en bild av den attackyta de utgör.

Systemets säkerhetsförmågor ska beskrivas på en detaljnivå som är tillräcklig för att ge läsaren en allmän förståelse för dessa. Beskrivningen förväntas vara mer detaljerad än den som ges i kapitlet Inledning.

När systemets arkitektur och säkerhetsförmågor beskrivs skall det framgå vilka delar som tillhör systemet och vilka som är externa beroenden.

Systembeskrivningen hämtas från ITSS-R, och kompletteras/justeras vid behov.

3.1 Förutsättningar

Informationen i detta kapitel hämtas från ITSS-R, och kompletteras/justeras vid behov.

3.1.1 Avsedd användning av systemet

Beskriv den tänkta användningen av systemet ur användarens perspektiv i termer av bearbetning, lagring och överföring av information. Informationen i detta kapitel hämtas från ITSS-R, och kompletteras/justeras vid behov.

3.1.2 Systemets driftmiljö

Beskriv fysiskt skydd, tillträdesbegränsning och andra förutsättningar som är säkerhetsrelevanta. Informationen i detta kapitel hämtas från ITSS-R, och kompletteras/justeras vid behov.

3.1.3 Tänkta användare av systemet

Användarroller i systemet ska redovisas och eventuell gruppering av användare efter åtkomst till resurser och information ska identifieras. Information i detta kapitel kan hämtas från ITSS-D och ITSA, och kompletteras/justeras vid behov.

3.1.4 Information

Förteckna typ av information, mängd, skyddsvärde, sekretessklassning, eventuella andra hanteringsregler (t.ex. från lagkrav) kring information som lagras, bearbetas, överförs i eller utförs ut ur systemet. Information i detta kapitel kan hämtas från ITSS-R, och kompletteras/justeras vid behov.

3.2 Systemets arkitektur

För att kunna identifiera säkerhetskraven för systemet är det nödvändigt att specificera systemets övergripande arkitektur.

Arkitekturbeskrivningen ska identifiera systemets komponenter och beskriva hur de samverkar och vilka informationsflöden som finns.

Information i detta kapitel kan hämtas från ITSS-R, och kompletteras/justeras vid behov.

3.3 Systemets gränsytor

Systemets alla logiska och fysiska gränsytor ska identifieras och beskrivas. Beskrivningen ska, förutom definition av gränssnitt och fysisk placering, identifiera vilken information som är tänkt att utbytas vid gränsytan och hur utbytet är tänkt att ske.

Referens till den, eller de, komponent(er) i arkitekturbeskrivningen som utgör gränsytan, samt eventuella komponenter som är avsedda att skydda gränsytan eller kontrollera informationsutbytet däröver ska också ges.

Information i detta kapitel kan hämtas från ITSS-R, och kompletteras/justeras vid behov.

3.4 Säkerhetsförmågor

Medan systemarkitekturen beskriver systemets uppbyggnad och vilka komponenter som ingår i systemet, beskrivs här systemets säkerhetsförmågor och de säkerhetsfunktioner som systemet tillhandahåller.

Information i detta kapitel kan hämtas från ITSS-R, och kompletteras/justeras vid behov.

4 Sammanställning av säkerhetskrav

Här hänvisas till dokument där tidigare genomförd kravdefinition finns. Kravsammanställning har dokumenterats i ITSS-D och eventuellt ändrats i ITSS-R.

Beskriv endast krav som ändrats i detta kapitel. Har inga ändringar gjorts, så hänvisa till ITSS-R.

4.1 Funktionella Säkerhetskrav

Endast eventuella förändringar av den ursprungliga kravsammanställningen ska dokumenteras i detta kapitel. Behåll ursprunglig kravidentitet och beskriv förändringen av grundkravet.

4.2 Assuranskrav

Endast eventuella förändringar av den ursprungliga kravsammanställningen ska dokumenteras i detta kapitel. Behåll ursprunglig kravidentitet och beskriv förändringen av grundkravet.

4.3 Tillkommande säkerhetskrav

Endast eventuella förändringar av den ursprungliga kravsammanställningen ska dokumenteras i detta kapitel. Behåll ursprunglig kravidentitet och beskriv förändringen av grundkravet.

5 Säkerhetskrav på omgivningen

Syftet med Säkerhetskrav på omgivningen är att identifiera de säkerhetskrav som ställs på systemets driftmiljö.

Kraven är förtecknade i VMH-R, dvs bilaga 3 till ISD-R.

I detta beskrivs om det under *Vidmakthålla* har framkommit att det krävs förändringar i kraven som ställs på systemets driftmiljö. Förändringar kan exempelvis uppkomma om tidigare identifierade brister har hanterats, eller om förutsättningar för driften har ändras.

Behåll ursprunglig kravidentitet och beskriv förändringen av grundkravet.

6 Tolkning av säkerhetskrav

Tolkning av säkerhetskraven för systemet innebär att kraven definieras på ett systemspecifikt sätt så att de konkret kan omsatts av systemet. De tolkade kraven är, via ITSA, omsatta i funktionella krav på systemet i TS respektive icke-funktionella krav på leverantörs åtagande i VÅS/SOW.

De tolkade säkerhetskraven är inför ackreditering av systemet förtecknade i ITSS-R och är grunden för kravuppfyllnad avseende MUST KSF samt tillkommande säkerhetskrav.

I de fall kravbilden förändrats under *Vidmakthållande*, ska de förändrade tolkade kraven förtecknas i detta kapitel. Observera att en förändring av de tolkade kraven kräver en ny uppfyllnadsanalys i nästa kapitel.

6.1 Funktionella säkerhetskrav

Endast eventuella förändringar av den ursprungliga kravsammanställningen ska dokumenteras i detta kapitel. Behåll ursprunglig kravidentitet och beskriv förändringen av grundkravet.

6.2 Assuranskrav

Endast eventuella förändringar av den ursprungliga kravsammanställningen ska dokumenteras i detta kapitel. Behåll ursprunglig kravidentitet och beskriv förändringen av grundkravet.

6.3 Tillkommande säkerhetskrav

Endast eventuella förändringar av den ursprungliga kravsammanställningen ska dokumenteras i detta kapitel. Behåll ursprunglig kravidentitet och beskriv förändringen av grundkravet.

7 Uppfyllande av säkerhetskrav

Uppfyllande av säkerhetskrav visar hur alla funktionella och icke-funktionella krav listade i kapitlet Tolkning av säkerhetskrav är uppfyllda av systemet och leverantören.

Evalueraren ISE ska utifrån denna beskrivning, och med stöd av Systembeskrivningen (eller motsvarande underlag), kunna förvissa sig om att alla säkerhetskrav är fullständigt uppfyllda av systemet.

Notera också att för samtliga funktionella och icke-funktionella krav kan det finnas flera leverantörer (beroende på systemarkitekturen). I dessa fall ska samtliga TS- och VÅS/SoW-krav användas i respektive kravs rationale.

Den ursprungliga uppfyllnadsanalysen är dokumenterad i ITSS-R, inför systemets ackreditering.

Om det under *Vidmakthållande* har skett förändringar, antingen i kravtolkning eller kravallokering (inom systemet, eller till omgivande driftmiljö) ska denna förändring analyseras i detta kapitel.

7.1 Funktionella säkerhetskrav

Detta kapitel utgör analys avseende förändrad kravuppfyllnad av de funktionella säkerhetskraven. Det är viktigt att klargöra att systemövergripande säkerhetsfunktioner såsom behörighetskontroll, behörighetspolicy, säkerhetsloggning , säker tid osv uppfylls enligt den arkitektur som beskrivs i ITSA.

Förändrad kravuppfyllnad kan exempelvis härledas till:

- Tillkommande krav (nytt KravID)
- Förändrat krav (eller annan tolkning av kravet), med bibehållet KravID
- Förändrad kravallokering
- Förändrad systemlösning som hanterar tidigare identifierad brist.

Följande ska anges i uppfyllande av de funktionella säkerhetskraven.

- KravID - refererar till det (ev ändrade) tolkade funktionella säkerhetskravet.
- Kravtext (tolkat krav) – ange kravtextext
- Uppfylls genom (rationale) – här beskriver ISE hur systemkravet uppfylls givet den arkitektur som beskrivs i Systembeskrivning och ITSA. Ange också referens till källa där bakgrund till rationale kan sökas.
- Utlåtande – avser ISE bedömning avseende kravuppfyllnad:
  - Uppfyllt
  - Ej uppfyllt
  - Uppfyllt, men ställer krav på Vmh
- Verifiering (ref) – referens till testfall för att verifiera ISE utlåtande.

KravID	Kravtext (tolkat krav) **Beskriv ev förändring**	Uppfylls genom (rationale) Med referens **Beskriv ev förändring**	Utlåtande	Verifiering (ref)

Tabell 4 – Uppdaterad kravuppfyllnad – funktionella säkerhetskrav

7.2 Assuranskrav

Detta kapitel utgör analys avseende förändrad kravuppfyllnad av de icke-funktionella säkerhetskraven (assuranskraven).

Förändrad kravuppfyllnad kan exempelvis härledas till:

- Tillkommande krav (nytt KravID)
- Förändrat krav (eller annan tolkning av kravet), med bibehållet KravID
- Struket krav
- Tillkommande assuransunderlag för att hanterar tidigare identifierad brist.

Följande ska anges i uppfyllande av de funktionella säkerhetskraven.

- KravID - refererar till det (ev ändrade) tolkade funktionella säkerhetskravet.
- Kravtext (tolkat krav) – ange kravtextext
- Uppfylls genom (rationale) – här beskriver ISE hur systemkravet uppfylls givet den arkitektur som beskrivs i Systembeskrivning och ITSA. Ange också referens till källa där bakgrund till rationale kan sökas.
- Utlåtande – avser ISE bedömning avseende kravuppfyllnad:
  - Uppfyllt
  - Ej uppfyllt
  - Uppfyllt, men ställer krav på Vmh
- Verifiering (ref) – referens till testfall för att verifiera ISE utlåtande.

KravID	Kravtext (tolkat krav) **Beskriv ev förändring**	Uppfylls genom (rationale) Med referens **Beskriv ev förändring**	Utlåtande	Verifiering (ref)

Tabell 5 – Uppdaterad kravuppfyllnad – icke-funktionella säkerhetskrav

7.3 Sammanfattning kravuppfyllnad

Detta kapitel sammanfattar utfallet från genomförd kravgranskning och ligger till grund för ackrediterbarhetsbedömningen i ISD-V.

7.3.1 Brister

Identifierade brister sammanställs i AU-V, där även en konsekvensanalys av dessa brister ska genomföras och dokumenteras.

7.3.2 Krav på användning/VMH

I detta avsnitt sammanställs de krav som anses vara uppfyllda, men som kräver åtgärder för vidmakthållande. Detta kan t ex vara krav på viss utbildning eller kompletterande fysiskt skydd.

De identifierade åtgärderna förs därefter över till VMH-R, bilaga 3 till ISD-R, Krav på miljön, som innehåller den totala kravmängden avseende omgivande miljö. Bilaga 3 kan användas som stöd vid lokal ackreditering i systemets faktiska driftmiljö

Nr	Ref till KravID	Krav på vidmakthållande

Tabell 6 – Krav på vidmakthållande

7.4 Slutsatser

I detta avsnitt gör ISE en samlad bedömning av samtliga granskningsaktiviteter avseende förändringar i kravuppfyllnaden.