Mall för ITSS 4/3

FÖRSVARETS MATERIELVERK

Fastställd av: Samråd av: Godkänd av:

Teknisk Chef SystGL IT-säk Produktledare

**INNEHÅLLSFÖRTECKNING**

[Mall för ITSS 4/3 1](#_Toc476302012)

[1 Sammanfattning 4](#_Toc476302013)

[2 Basfakta 5](#_Toc476302014)

[2.1 Giltighet och revision 5](#_Toc476302015)

[2.2 Granskning 5](#_Toc476302016)

[2.3 Referenser 5](#_Toc476302017)

[2.4 Bilagor 5](#_Toc476302018)

[2.5 Begrepp och förkortningar 6](#_Toc476302019)

[3 Inledning 7](#_Toc476302020)

[3.1 Syfte 7](#_Toc476302021)

[3.2 Ackrediteringsobjektets omfattning 7](#_Toc476302022)

[3.3 Avgränsning 7](#_Toc476302023)

[3.4 Tidigare ITSS och andra beslut 8](#_Toc476302024)

[4 Systembeskrivning 9](#_Toc476302025)

[5 Sammanställning av säkerhetskrav 11](#_Toc476302026)

[5.1 Installations- och konfigurationsanvisningar 11](#_Toc476302027)

[5.2 Handböcker 11](#_Toc476302028)

[5.3 Skydd av leverans 12](#_Toc476302029)

[6 Tolkning av säkerhetskrav/ Arkitektur 13](#_Toc476302030)

[7 Uppfyllande av säkerhetskrav 14](#_Toc476302031)

[7.1 Motivering och bedömning 14](#_Toc476302032)

[7.1.1 Tillkommande säkerhetskrav 14](#_Toc476302033)

[7.1.2 Funktionella säkerhetskrav enligt KSF 14](#_Toc476302034)

 [15](#_Toc476302035)

[7.1.3 Assuranskrav enligt KSF 15](#_Toc476302036)

[7.2 Avvikelser 15](#_Toc476302037)

[7.2.1 Tillkommande säkerhetskrav 15](#_Toc476302038)

[7.2.2 Funktionella säkerhetskrav enligt KSF 15](#_Toc476302039)

[7.2.3 Assuranskrav enligt KSF 15](#_Toc476302040)

[7.3 Krav på omgivningen 15](#_Toc476302041)

[7.3.1 Syfte 15](#_Toc476302042)

[7.3.2 Krav på omgivningen 15](#_Toc476302043)

[7.4 Kvarvarande risk 16](#_Toc476302044)

[8 Summerat underlag 17](#_Toc476302045)

**Så här används denna mall:**

* *Denna mall används för såväl ITSS 3 som ITSS 4. ITSS 3 är industrins ITSS. Det är leverans från industrin och är grunden för ITSS 4 som endast är en utveckling av ITSS 3. Mallen är skriven som om det vore ITSS 4, när den används för ITSS 3 måste ordet ”ITSS 4” på vissa ställen bytas ut mot ”ITSS 3”. ISD-deklaration måste då bytas ut mot ISU- utlåtande.*
* *Denna mall används även då återbruk av dokumentation och resultat från tidigare ITSS används (deltaanalys). En mer detaljerad instruktion kring tillvägagångssätt och resonemang kring återbruk finns i dokumentet FMV Vägledning ISD och SE 16FMV1109-5:1*
* *Instruktionen om vad som ska stå under varje rubrik anges kursivt. Denna text ska raderas innan dokumentet färdigställs.*
* *Text som inte är kursiv är text som kan användas också i det färdigställda dokumentet.*
* *Ersätt Systemnamn med systemets namn.*
* *Ersätt hänvisningar till referenser och bilagor inom [ ] med dess verkliga referens.*
* *Till dokumentet finns bilaga avseende kravuppfyllnad.*
* *Redigera dokumentets metadata genom att fylla i relevant information under ”Egenskaper” (eng. ”Properties”) så som namn på systemet och version på dokumentet. Uppdatera därefter fältkoder.*
* *Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.*
* *Radera denna sida.*

# Sammanfattning

*Kort sammanfattning av innehållet i dokumentet där exempelvis följande ska framgå:*

* *Ange vilket IT-system och eventuella delsystem som omfattas av dokumentet.*
* *Ange användningsområde för IT-systemet.*
* *Ange informationssäkerhetsklass för IT-systemet.*
* *Ange mot vilken kravmängd granskning har skett.*
* *Sammanfattning av resultatet av genomförd granskning.*

# Basfakta

## Giltighet och revision

| Datum | Utgåva | Status | Beskrivning | Handläggare | Fastställd av |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Granskning

|  |  |  |
| --- | --- | --- |
| Namn | Roll/organisation | Kompetensområde |
|  |  |  |
|  |  |  |

## Referenser

| Ref. | Dokumentnamn | Dok. id. |
| --- | --- | --- |
|  | ITSS 1 |  |
|  | ITSS 2 |  |
|  | ITSS 3 |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Bilagor

*I tabellen nedan anges exempel på bilagor.*

|  |  |  |
| --- | --- | --- |
| Nr | Dokumentnamn | Dokumentnummer |
|  | Systembeskrivning |  |
|  | Konfigurationsbeskrivningar |  |
|  | Test- och granskningsbeskrivningar |  |
|  | Säkerhetsarkitektur |  |
|  |  |  |

## Begrepp och förkortningar

| Begrepp | Förklaring |
| --- | --- |
| Ackreditering | Dels ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633), dels ett godkännande från säkerhetssynpunkt i övrigt av övriga IT-system. |
|  |  |
|  |  |
|  |  |

# Inledning

ITSS 4 är huvuddokumentet och beskriver resultatet av det informationssäkerhetsarbete som bedrivits under hela utvecklingscykeln. ITSS 4 ligger till grund för ISD-deklarationen.



*Figur* 1*: ISD-processen*

## Syfte

Syftet med ITSS 4 är att ge en beskrivning av systemet och dess säkerhetsfunktioner, den omgivning systemet är dimensionerat för, vilka säkerhetskrav omgivningen förväntas lösa ut samt ev. kvarvarande brister och hur dessa bör hanteras. Tillsammans med annan relevant dokumentation ska ITSS 4 alltså visa att systemet som helhet uppfyller Försvarsmaktens krav avseende informationssäkerhet.

## Ackrediteringsobjektets omfattning

*Under denna rubrik anges ackrediteringsobjektets omfattning inklusive ingående delsystem och miljö.*

Detta dokument avser underlag för ackreditering av…….

## Avgränsning

*Under denna rubrik anges ackrediteringsobjektets avgränsning, dvs vad som inte omfattas av denna ackreditering.*

Granskningar i detta dokument omfattar inte ……..

## Tidigare ITSS och andra beslut

*Beskriv förutsättningar från tidigare ITSS (ITSS 1, ITSS 2 och ITSS 3) samt om det framkommit ytterligare faktorer och beslut som påverkar ackrediteringsläget.*

*Tidigare framtagna ITSS ger underlag till ITSS 4. Hur visas i respektive avsnitt nedan. Se även dokumentet FMV Vägledning ISD och SE 13FMV5921-3:1.*

# Systembeskrivning

*Här ges en systemöversikt av det aktuella IT-systemet. Översikten ska framför allt innehålla vilka säkerhetsfunktioner som finns för det aktuella IT-systemet. I systemöversikten kan man hänvisa till en mer djuplodande systembeskrivning. Exempel på saker att kort beskriva:*

* *Verksamhet som IT-systemet ska användas i*
* *Användningsområde*
* *Hänvisning till en mer djuplodande systembeskrivning*
* *Vilka system det samverkar med*
* *Vilka säkerhetsfunktioner som finns i IT-systemet*
	+ *Behörighetskontroll*
	+ *Säkerhetsloggning*
	+ *Intrångsskydd*
	+ *Intrångsdetektering*
	+ *Skydd mot skadlig kod*
	+ *Skydd mot obehörig avlyssning*
	+ *Skydd mot röjande signaler*
* *Systembild*

*Figur 2:Exempel på systemöversikt - PS-871*

En mer utförlig systembeskrivning återfinns i:

| Dokumentnamn | Dokumentbeteckning | Beskrivning | Status |
| --- | --- | --- | --- |
| Systembeskrivning |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Sammanställning av säkerhetskrav

*Här hänvisas till dokument där tidigare genomförd kravdefinition finns. Kravdefinition har t.ex. genomförts i ITSS 1, ITSS 2 och ibland även i ITSS 3. Eventuellt finns även ytterligare dokumentation med kravdefinition som i sådana fall ska anges här.*

*I KSF 3 så ingår Installations- och konfigurationsanvisningar, handböcker samt Skydd av leverans i assuranskraven och då redovisas detta i ITSS 1, ITSS 2 etc.*

Kravdefinition för *Systemnamn* återfinns i följande dokument:

|  |  |
| --- | --- |
| Dokumentnamn | Dokumentbeteckning |
| *ITSS 1 Systemnamn* |  |
| *ITSS 2 Systemnamn* |  |
|  |  |

## Installations- och konfigurationsanvisningar

*Detta avsnitt ska beskriva installations- och konfigurationsanvisningar som är dimensionerande för IT-säkerheten i systemet. Ytterligare detaljer beskrivs i dokument i tabellen nedan. Saknas installations och konfigurationsanvisningar kan man fundera över kvaliteten i genomfört verifieringsarbete. Avser kravdefinitionen KSF 3 så skall denna rubrik tas bort.*

Installations- och konfigurationsanvisningar för *Systemnamn* återfinns i följande dokument:

| Dokumentnamn | Dokumentbeteckning | Beskrivning | Status |
| --- | --- | --- | --- |
|  |  |  |  |

## Handböcker

*Avser kravdefinitionen KSF 3 så skall denna rubrik tas bort.*

Följande handböcker för *Systemnamn* finns tillgängliga eller är under framtagning:

| Dokumentnamn | Dokumentbeteckning | Beskrivning | Status |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Skydd av leverans

*Detta avsnitt ska beskriva om det finns särskilda krav på skydd av leveransen från leverantören till användaren t.ex. i form av plombering, checksummor och annat integritetsskydd.*

*Avser kravdefinitionen KSF 3 så skall denna rubrik tas bort.*

Leveransbeskrivning för *Systemnamn* redovisas i följande dokument:

|  |  |
| --- | --- |
| Dokumentnamn | Dokumentbeteckning |
|  |  |

# Tolkning av säkerhetskrav/ Arkitektur

*Detta avsnitt ska beskriva de dimensionerande IT säkerhetsaspekterna vid kravnedbrytning samt utformning av säkerhetsdesign och – arkitektur.*

Följande dokument för *Systemnamn* beskriver tolkning av säkerhetskrav samt uppbyggnad av säkerhetslösningen/ arkitekturen:

| Dokumentnamn | Dokumentbeteckning | Beskrivning | Status |
| --- | --- | --- | --- |
| ITSS 2 |  |  |  |
| SYD |  |  |  |
|  |  |  |  |

# Uppfyllande av säkerhetskrav

*Kravuppfyllnadsmatris ska finnas i detta avsnitt, ej i bilaga.*

## Motivering och bedömning

*Detta avsnitt ska innehålla kravuppfyllnad mot säkerhetskrav. Om kravuppfyllnaden klassas försvarssekretess ska kravuppfyllnad redovisas i bilaga.*

*Krav ID – löpnummer för tillkommande krav alt KSF- kravnummer. Tillkommande krav placeras med fördel först i tabellen och därefter KSF kraven*

*Krav – kravtexten*

*Verifieringstyp – Med vilken metod har kravet verifierat och referens (verifieringsrapport)*

*Uppfyllnad – Hur är kravet uppfyllt och var i designen finns säkerhetsfunktionen.*

*Bedömning – uppfyllnadsnivå*

### Tillkommande säkerhetskrav

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Krav ID | Krav | Uppfyllnad | Verifieringstyp och referens | Bedömning |
| *K1* |  |  |  |  |
| *K2* |  |  |  |  |
| *K3* |  |  |  |  |
| *Etc.* |  |  |  |  |

###

### *Funktionella säkerhetskrav enligt KSF*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Krav ID | Krav | Uppfyllnad | Verifieringstyp och referens | Bedömning |
| *SFGK\_FEL* | *Säkerhetsfunktionen ska kunna upprätthålla ett säkert tillstånd vid fel* |  |  |  |
| *SFGK\_TID* | *Säkerhetsfunktionen ska använda systemets gemensamma tid* |  |  |  |
| *Etc.* |  |  |  |  |

### *Assuranskrav enligt KSF*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Krav ID | Krav | Uppfyllnad | Verifieringstyp och referens | Bedömning |
| *SASS\_INL* | *ITSS Inledning* | *Detta dokument* |  |  |
| *SASS\_SYS* | *Systembeskrivning* | *Se ref x* |  |  |
| *etc.* |  |  |  |  |

## Avvikelser

*Detta avsnitt ska innehålla dels en statistik över avvikelser men även en bedömning av vilka avvikelser som prioriteras.*

### Tillkommande säkerhetskrav

*<Skriv här>*

### *Funktionella säkerhetskrav enligt KSF*

<Skriv här

### *Assuranskrav* *enligt KSF*

*<Skriv här*

## Krav på omgivningen

### Syfte

*Krav på omgivningen är de krav som FMV ställer på FM för att FMV ska kunna deklarera kravuppfyllnad. Exempel på sådant krav kan vara krav på fysiskt skydd eller manuella rutiner. Krav på omgivningen kan även vara på de integrationsprojekt som ska integrera Systemnamn i System av System.*

Syftet med detta avsnitt är att beskriva de krav på användning som har identifierats i samband med granskning av *Systemnamn* mot KSF krav på säkerhetsfunktioner.

### Krav på omgivningen

| **Pos** | **Källa** | **Text** |
| --- | --- | --- |
|  |  |  |
| 1.
 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

##

## Kvarvarande risk

I detta avsnitt sammanställs kvarstående risker som identifierats utifrån identifierade avvikelser och som rör **FMVs leverans**. De risker som beskrivs ska vara ett stöd inför Försvarsmaktens ackrediteringsbeslut.

|  |  |  |  |
| --- | --- | --- | --- |
| Nr | Avvikelse | Påverkan | Bedömd risk |
| 1 |  |  |  |

# Summerat underlag

| Dokument | Sammanfattning | Avvikelser | Dok.nr. |
| --- | --- | --- | --- |
| Kravdefinition | Kravfångst återfinns i dokument enligt förteckning i avsnitt x |  |  |
| Systemöversikt / Systembeskrivning | En översiktlig samt fördjupad systembeskrivning återfinns i systembeskrivning för *Systemnamn*, ref. [x]  |  |  |
| Säkerhetsfunktioner och säkerhetsmekanismerBeskrivning av säkerhetsfunktionerna –* *säkerhetsloggning*
* *behörighetskontroll*
* *skydd mot röjande signaler*
* *skydd mot obehörig avlyssning*
* *skydd mot skadlig kod*
* *intrångsskydd*
* *intrångsdetektering*
* *övriga säkerhetsfunktioner*
 | Beskrivningen av säkerhets­funktionerna återfinns i systembeskrivning för *Systemnamn*, ref. [x]  |  |  |
| Installations- och konfigurationsanvisningar | Installations- och konfigurationsanvisningar finns framtagna för *Systemnamn* |  | Se avsnitt 5.1 i detta dokument |
| Handböcker | Användarhandledning för *Systemnamn* finns framtagen. |  | Se avsnitt 5.2 i detta dokument |
| Skydd av leverans | Skydd av leverans för *Systemnamn* finns framtagen. |  | Se avsnitt 5.3 i detta dokument |
| Uppfyllande av säkerhetskrav | Granskning av *Systemnamn* mot säkerhetskrav återfinns i avsnitt 7 |  | Se avsnitt 7 i detta dokument  |
| Avvikelser (sammanfattning över kvarstående brister inkl åtgärdsplan) | Brister från granskningarna sammanställs i avsnitt 7.2Krav på omgivning återfinns i avsnitt 7.3 |  | Se avsnitt 7.2 och 7.3 i detta dokument |