Mall för ITSS 1

FÖRSVARETS MATERIELVERK

INNEHÅLLSFÖRTECKNING

[Mall för ITSS 1 1](#_Toc476298707)

[1 Sammanfattning 4](#_Toc476298708)

[2 Allmänt 5](#_Toc476298709)

[2.1 Syfte 5](#_Toc476298710)

[3 Basfakta 6](#_Toc476298711)

[3.1 Giltighet och revision 6](#_Toc476298712)

[3.2 Granskning 6](#_Toc476298713)

[3.3 Referenser 6](#_Toc476298714)

[3.4 Begrepp och förkortningar 6](#_Toc476298715)

[4 Översiktlig systembild 7](#_Toc476298716)

[5 Förutsättningar 8](#_Toc476298717)

[5.1 Ackrediteringsobjektets omfattning 8](#_Toc476298718)

[5.2 Avgränsning 8](#_Toc476298719)

[6 Säkerhetskrav 9](#_Toc476298720)

[6.1 Tillämpning av KSF 3 9](#_Toc476298721)

[6.1.1 Konsekvensnivå 10](#_Toc476298722)

[6.1.2 Exponeringsnivå 10](#_Toc476298723)

[6.1.3 Kravnivå 10](#_Toc476298724)

[6.2 Exponering 11](#_Toc476298725)

[6.2.1 Antagande om fysiskt skydd 11](#_Toc476298726)

[6.2.2 Antagande om organisatorisk skydd 11](#_Toc476298727)

[6.2.3 Externa gränsytor 12](#_Toc476298728)

[6.3 Assurans 12](#_Toc476298729)

[6.4 Kravtolkning av Försvarsmaktens krav 12](#_Toc476298730)

[7 FMV:s interna krav 14](#_Toc476298731)

[7.1 Övergång till ITSS 2 i ISD-processen 14](#_Toc476298732)

**Så här används denna mall:**

* *Denna mall ska användas för ITSS 1. För ITSS 2, ITSS 3 och ITSS 4 används andra mallar, dvs denna mall utvecklas inte för efterföljande ITSS.*
* *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.*
* *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 vilken kravmängd (t.ex. MUST KSF, säkerhetsmål) som är input till dokumentet.*
* *Sammanfattning av resultatet av genomförd kravfångst t.ex. om viss information saknas för gå vidare i processen.*

# Allmänt

Det säkerhetstekniska ackrediteringsunderlaget 1 (ITSS 1) ingår som en del av IT-säkerhetsdeklarationen (ISD) för *Systemnamn*.



Figur 1: ISD-processen.

## Syfte

Syftet med ITSS 1 är att fånga de krav som finns från Försvarsmakten samt att genomföra tolkning av krav. Kravfångsten i ITSS 1 blir sedan det dokument som utvecklingen sker utifrån. ITSS 1 är ett dokument som initialt visar på de dimensionerande faktorerna såsom hur ett system exponeras mot omvärlden. En genomtänkt ITSS 1 är en förutsättning för ISD-planen. ITSS 1 kan även vidareutvecklas i ITSS 2.

# Basfakta

## Giltighet och revision

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

## Granskning

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

## Referenser

| Ref. | Dokumentnamn | Dok. id. |
| --- | --- | --- |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |
| 1.
 |  |  |

## 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. |
|  |  |
|  |  |

# Översiktlig systembild

*Här ges en översiktlig systembild över samverkan med externa system och parter. Detta arbete ska inte vara omfattande och djuplodande utan ska ge en snabb översikt utifrån den systembild som Försvarsmakten har utgivit.*

# Förutsättningar

## Ackrediteringsobjektets omfattning

*Under denna rubrik anges ackrediteringsobjektets omfattning inklusive ingående delsystem och miljö. Ackrediteringsobjektets omfattning ska förklara vad det är som ska ackrediteras? Om det ska ackrediteras? Ska det auktoriseras?*

Detta dokument avser ackreditering av…….

## Avgränsning

*Under denna rubrik anges ackrediteringsobjektets avgränsning, dvs. vad som inte omfattas av denna ackreditering. En väl definierad avgränsning underlättar ackrediteringen av systemet.*

Granskningar i detta dokument omfattar inte ……..

# Säkerhetskrav

*I detta kapitel görs kravfångsten. All information från detta kapitel blir input till arbetet med IT-säkerhetsarkitektur (ITSS 2) och teknisk specifikation. I ITSS 2 kan ITSS1 kompletteras och vidareutvecklas. I detta avsnitt görs inga analyser utan en minimal utveckling från FM-krav.*

## Tillämpning av KSF 3

*I detta beskrivs resultatet från den säkerhetsanalys där skyddsvärda tillgångar identifieras och prioriterats. I avsnittet redogörs för den ingående kravmassan bestående av Försvarsmaktens (MUST) krav på säkerhetsfunktioner, version 3, kopplat mot respektive område framtagna för detta system. I KSF 3 ingår en modell för hur ramverket ska tillämpas mot ett IT-system. Modellen kan översiktligt beskrivas enligt figuren nedan.*

*Figur 2: KSF 3 modellen*

*Enligt modellen ovan skall konsekvens-, exponerings- och kravnivåer fastställas (sker i detta dokument). Bedömd konsekvensnivå och exponeringsnivå bestämmer tillsammans vilken kravnivå systemet tillhör, avseende funktionella säkerhetskrav och assuranskrav i KSF 3.*

*Även identifiering av säkerhetsrelaterade IT-komponenter samt fastställande av komponentassuransnivåer skall göras (sker i ITSS2). Slutresultatet av hela tolkningen sammanställs och redogörs (av FM) i en ITSS. Hela processen är iterativ och medför att det är först när en framtagen säkerhetsarkitektur finns som det går att fastställa exponeringen och därmed krav. Detta synliggörs via pilen längst ned som leder från ITSS tillbaka till Start.*

*I detta beskrivs resultatet från den säkerhetsanalys där skyddsvärda identifieras och prioriterats. Bedömd konsekvensnivå och exponeringsnivå bestämmer tillsammans vilken kravnivå systemet tillhör, avseende funktionella säkerhetskrav och assuranskrav i KSF 3.*

### Konsekvensnivå

*Vid en informationsklassificering identifieras vilken skyddsvärd information som hanteras av systemet. Med hjälp av en informationsklassificering kan sedan en konsekvensnivå identifieras. Konsekvensnivån för ett system identifieras utifrån vilken konsekvens som uppstår om ett systems skyddsvärda tillgångar röjs. Konsekvenserna innebär informationsförlust av antingen sekretessklassificerade uppgifter eller hemliga eller utrikesklassificerade uppgifter.*

*Ett system som är avsett att hantera information i informationssäkerhetsklass upp till t.ex. HEMLIG/SECRET hamnar på konsekvensnivå 4 utifrån en femgradig skala. För mer information kring konsekvensnivå, se aktuellt KSF 3-dokument.*

### Exponeringsnivå

*Exponeringsnivån avser bedömningen av hur ett system exponeras i avseende till någon aktörs möjlighet att påverka systemet. Exponeringsnivån bedöms utifrån hur system exponeras vid både fysisk och digitalt informationsbyte samt utifrån hur personer vistas i systemets lokaler. Ett systems exponering uttrycks i fyra nivåer med E1 som lägsta och E4 som högsta exponeringsnivå, se exempel Figur 2. Ökade möjligheter för någon aktör att påverka systemet definieras som en högre exponeringsnivå, vilket i sin tur medför högre krav på systemets säkerhetsförmåga.*

*Initialt kommer exponeringsnivån baseras på verksamhetens perspektiv där man tar hänsyn till IT-systemets omgivning. För att ta fram en optimal exponeringsnivå kommer iterativ exponeringsanalys att genomföras vid framtagningen av ITSS 2. Resultatet av denna exponeringsanalys kan innebära att man behöver uppdatera ITSS 1.*

*Verksamhetens perspektiv kan innebära att tar hänsyn till hur många personer som ska använda systemet och systemets lokal ser ut. För mer information kring exponeringsnivå, se aktuellt KSF 3-dokument.*



Figur : Exponeringsnivå med tillhörande kriterier

### Kravnivå

*Det finns tre kravnivåer i KSF 3, Grund (G), Utökad (U) och Hög (H). Kravnivåerna bestäms utifrån konsekvensnivå, dvs. konsekvens av informationsförlust, och systemets exponeringsnivå, se Figur 3. Kravnivån avgör vilka säkerhetskrav som systemet måste uppfylla. Eftersom exponeringsnivån initialt baseras på verksamhetens perspektiv kommer iterativ exponeringsanalys att genomföras vid framtagningen av ITSS 2 för att ta fram en optimal kravnivå. Innebörden av tabellen nedan tydliggörs i exponeringsanalysen. Resultatet av denna exponeringsanalys kan innebära att man behöver uppdatera kravnivån i ITSS 1.*



Figur : Kravnivåer för funktionella säkerhetskrav och assuranskrav

## Exponering

*Här beskrivs systemets miljö i form av exponering. Med exponering avses fysiskt och organisatoriskt skydd samt externa gränsytor ur projektets perspektiv. Input till avsnittet kan exempelvis hämtas från säkerhetsmålsättningen och TTEM.*

### Antagande om fysiskt skydd

*Detta avsnitt ska beskriva antagande om fysiskt skydd som begränsar exponeringen. Nedan ges exempel.*

| ID | Beskrivning | Referens |
| --- | --- | --- |
|  | *Systemet installeras i apparatutrymmen godkänt för förvaring HEMLIG/RESTRICTED materiel.* |  |
|  |  |  |

### Antagande om organisatorisk skydd

*Detta avsnitt ska beskriva antagande om organisatoriskt skydd som begränsar exponeringen. Nedan ges exempel.*

| ID | Beskrivning | Referens |
| --- | --- | --- |
|  | *Behörig åtkomst till administration av it-säkerhetsfunktioner medges endast it-säkerhetsadministratören.* |  |
|  |  |  |

### Externa gränsytor

*Här beskrivs externa gränsytor och identifierade hotaktörer till den produkt som projektet ska leverera. Hotaktörer kan vara såväl insiders som externa angripare. Okunskap om anslutande systems säkerhetsmekanismer, användare, säkerhetsnivåer mm ger osäkerhet kring omfattningen av möjliga hot och därför behöver de externa gränsytorna beskrivas. Om det finns en illustration över systemet inklusive gränsytor är det också bra att presentera här. Här görs inga analyser utan mer en tolkning från FM-krav.*

| ID | Beskrivning | Referens |
| --- | --- | --- |
|  |  |  |
|  |  |  |

## Assurans

*Med assurans avses krav på verifieringsarbetet under hela utvecklingscykeln utifrån ett IT-säkerhetsperspektiv. Genom detta åstadkoms tillräcklig tillit till att säkerhetsfunktioner uppfyller ställda krav. I de fall assuransnivån är identifierad i Säkerhetsmålsättning och TTEM ska det beskrivas i detta avsnitt*

*MUST ställer i KSF 3 nya krav på assuransnivåer för alla IT-system.*

| Krav ID | FM Kravbeskrivning/funktionella krav | FMV tolkning |
| --- | --- | --- |
| K1 |  |  |
| K2 |  |  |
| K3 |  |  |

## Kravtolkning av Försvarsmaktens krav

*Nedan visas exempel på kravfångst och kravtolkning med avseende på Försvarsmaktens krav.*

| Krav ID | FM Kravbeskrivning/funktionella krav | FMV tolkning | Ref |
| --- | --- | --- | --- |
| K1 | *IT-systemet ska vara försett med intrångsskydd.* | *Endast av Försvarsmakten godkända brandväggar ska användas.* | *SM1* |
| *Brandväggar ska användas på servrar och klienter.* |  |
| K2 | *All kommunikation till och från IT-systemet ska vara krypterad.* | *Endast av Försvarsmakten godkända krypton får användas.* | *SM2* |
| K3 | *Säkerhetsfunktionen för säkerhetsloggning skall säkerställa att alla registrerade händelser i säkerhetsloggen kan presenteras i läsbar form och att granskning av de registrerade händelserna kan genomföras.* | *IT-systemet ska vara försett med en central loggfunktion som samlar in samtliga säkerhetsrelevanta händelser till en plats för arkivering och analys.* | *SM3* |
| K4 | *Ett definierat säkert tillstånd ska upprätthållas för de delar av systemet som berörs när hela eller* *delar av säkerhetsfunktionens funktionalitet är korrupt eller oåtkomlig. Detta innebär att fel i* *funktionalitet måste kunna upptäckas, t.ex. via självtester.* |  | *SFGK\_FEL.4* |

# FMV:s interna krav

*Nedan visas exempel på kravfångst och kravtolkning med avseende på Försvarets materielverks krav.*

| Krav ID | FMV Kravbeskrivning |
| --- | --- |
| 1. | *Ex. Systemledningsarbetet ställer krav på leveranstid, ekonomi, funktionalitet för ingående komponenter/system till BMS*  |
| 2. | *AK Sjö plattform Ys ledningssystem ska utvecklas av AKLed där handlingsregler beskrivs i ref x.* |
| 3 | Beslut angående fullt införande av ISD-processen - 15FMV30-20:1  |
| 4 | Beslut angående FMVs införande och tillämpning av MUST Krav på Säkerhetsfunktioner - KSF 3.1/KSF 3.2 - 15FMV30-55:1 |

## Övergång till ITSS 2 i ISD-processen

I övergången mellan ITSS 1 och ITSS 2 ska kravreduktion och utveckling av krav ske för att i ITSS 2 endast ange de krav som ska införas i TS och SoW/VÅS. Dessa ska beskrivas och relateras till de delar av systemet där dessa krav är relevanta. Kravdefinitionens innehåll kan påverkas av den kravnedbrytning och arkitektur som identifieras och fastställs i ITSS 2. Kravet kan såväl öka som minska efter tex genomförd exponeringsanalys i ITSS 2. Krav som tas bort i ITSS 1 ska vara förklarade för att som del ingå i granskning av den slutliga kravmängdens riktighet och spårbarhet till SM krav på säkerhetsfunktioner för denna kravnivå (G, U eller H).

Design av *SYSTEM A* ska bygga på plattformen *SYSTEM B*. Villkor och förutsättningar för denna ska finnas tillgängliga för att kunna utforma ITSS 2 och TS/SoW som underlag för offertförfrågan.

TS och SoW/VÅS ska granskas och godkännas av FM som en del av Beslut om anskaffning.

FMV kommer att granska och verifiera leverantörens uppfyllnad av säkerhetskraven i TS och SoW/VÅS med stöd av leverantörens underlag samt tillsammans med övriga krav i ITSS 1 skapa en ITSS 4 där alla krav redovisas som uppfyllda eller med förslag på hur dessa ska hanteras av FM.