**Mall för ITSS 2: IT-säkerhetsarkitektur**

FÖRSVARETS MATERIELVERK

**Så här används denna mall:**

* *Nedanstående mall ingår i metodstöd för att ta fram IT-säklerhetsarkitektur för system. I mallen benämns IT-säkerhetsarkitektur för ITSS 2.*
* *Denna mall ska användas för ITSS 2. För ITSS 1, 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 och med grå understrykning. 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, inklusive denna punktlista.*

**Innehållsförteckning**

1 Inledning 4

1.1 Syfte 4

1.2 Avgränsingar 4

1.3 Informationsklassning av dokumentet 4

1.4 Basfakta 4

2 Systemöversikt 5

2.1 Övergripande riktlinjer och designprinciper 5

3 Hot 6

4 Krav 6

4.1 IT-säkerhetskrav 6

4.2 Krav på omgivningen 7

5 IT-säkerhetsfunktioner 7

5.1 Intrångsskydd/Separation 7

5.2 Logghantering 11

5.3 Autentisering och behörigheter 12

5.4 Signalskydd 12

5.5 IDS-funktionalitet 13

5.6 Informationshantering och back up 13

5.7 Skydd mot RÖS 13

5.8 Integritetsskydd 14

5.9 Säkerhetsadministration 14

5.10 Skydd mot skadlig kod 15

5.11 Övrigt 15

6 IT-Säkerhetsfunktioner som kräver särskild assurans 16

6.1 Identifierade IT-säkerhetsfunktioner 16

6.2 Funktioner med behov av oberoende granskning 16

7 GFE-plan 16

# Inledning

## Syfte

*Här beskrivs ITSS 2 syfte och innehåll. Här beskrivs även ambition och motivation med avseende på vilken nivå FMV har valt att beskriva ITSS 2 till leverantör.*

## Avgränsingar

*Här beskrivs eventuella avgränsningar som har gjorts i arbetet med ITSS 2.*

## Informationsklassning av dokumentet

*Här beskrivs vilken informationsklassning dokumentet underställs, glöm inte att motivera informationsklassen.*

## Basfakta

### Referenser

*Här listas referenser som används i dokumentet.*

| Ref | Rubrik | Beteckning |
| --- | --- | --- |
| 1. |  |  |
|  |  |  |

### Giltighet och revision

*Det ska här framgå att dokumentets giltighet och vem som godkänner.*

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

### Granskning

*Det ska här framgå uppgifter kring gransknig av ITSS 2, vem som granskat, kompentensområde t.ex. SE samt vilken roll.*

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

### Begrepp och förkortningar

*Här listas begrepp och förkortningar som används i dokumentet.*

| Förkortning/Term | Förklaring |
| --- | --- |
|  |  |

# Systemöversikt

*I detta avsnitt beskrivs systemet med avseende på delsystem men även specifika aspekter som påverkar IT-säkerhetsarbetet såsom externa gränsytor. Denna beskrivning skall vara tillräckligt lätt att överblicka och på en nivå att den kan användas som input till ITSS 2. För att öka förståelsen kan det vara önskvärt att delar av beskrivningen består av bilder med förklarande text.*

## Övergripande riktlinjer och designprinciper

*I detta avsnitt beskrivs de övergripande riktlinjer och designprinciper som ska vara styrande för framtagning av ITSS 2. Exempel: Alla delar av kommunikationssystemet ska trafikskyddas, flerlagersäkerhet ska användas.*

# Hot

I detta avsnitt definieras de hotaktörer och de hot som är identifierade mot systemet. Hoten kan efter bedömning vara underlag för ytterligare IT-säkerhetskrav.

|  |  |  |
| --- | --- | --- |
| ID | Hotaktör | Beskrivning |
| *Hot001* | *Insider* | *Insider utnyttjar administrativ behörighet för att lösa information denne inte är behörig till.* |
| *Hot002* |  |  |
| *Hot003* |  |  |

# Krav

## IT-säkerhetskrav

*I detta avsnitt listas vilka IT-säkerhetskrav som fördelas och hanteras på vilken/vilka IT-säkerhetsfunktioner. IT-säkerhetskraven och den tekniska specifikationen kan behöva uppdateras kontinuerligt under arbetet med IT-säkerhetsarkitekturen.*

*Varje IT-säkerhetskrav erhåller en unik identitet. Kraven mappas till IT-säkerhetsfunktioner avsnitt 5.*

|  |  |  |
| --- | --- | --- |
| ID | IT-säkerhetskrav | IT-säkerhetsfunktion |
| *SäkKrav001:* | *Endast på förhand godkänd kod ska kunna exekvera i systemet* | *SäkFunk001* |
| *SäkKrav002:* | *Samtliga gränsytor mot andra system ska skyddas mot intrång med hjälp av Färist.* |  |
| *SäkKrav003* | *Alla centrala systemnoder och servrar ska kunna fjärradministreras via separat administratörsnätverk.* |  |
| *SäkKrav004* | *Stark autenticering ska användas för alla gränsytor förutom de som är åtkomliga inifrån serverrum.* |  |
| *SäkKrav005* |  |  |

## Krav på omgivningen

*I detta avsnitt listas vilka krav som IT-systemet ställer på omgivningen. Kraven på omgivningen kan behöva uppdateras kontinuerligt under arbetet med IT-säkerhetsarkitekturen.*

*Varje Krav på omgivningen erhåller en unik identitet. Kraven mappas till säkerhetsfunktioner avsnitt 4.*

|  |  |  |
| --- | --- | --- |
| ID | IT-säkerhetskrav | IT-säkerhetsfunktion |
| *OmgKrav001* | *Serverrum ska vara försett med inpasseringssystem som unikt identifierar behörig administratör.* | *SäkFunk001* |
| *OmgKrav002* | *Serverrum ska vara i säkerhetsklass 3* |  |
| *OmgKrav003* | *Loggar från inpasseringssystemet ska kunna korreleras med loggar från systemet.* |  |
| *OmgKrav004* |  |  |

# IT-säkerhetsfunktioner

*Detta avsnitt görs allokering av IT-säkerhetsfunktioner på systemet d.v.s var IT-säkerhetsfunktionerna finns på systemet (ex applikation, infrastruktur, kommunikation). IT-säkerhetsfunktionerna motsvarar grovt områdena i MUST KSF (Krav på SäkerhetsFunktioner) för att underlätta för verifiering. Är inte IT-säkerhetsfunktionerna applicerbara eller relevanta för det aktuella systemet skall det beskrivas varför.*

*Varje IT-säkerhetsfunktion beskrivs i tabellform nedan med unik identitet, kort beskrivning av funktion, vilka krav som den ska hantera samt hur den ska verifieras.*

*För att ytterligare vägleda projektet har det första området ”Intrångs- och separationsmekanismer illustrerats mha ett exempel på ett sätt att visualisera allokering av IT-säkerhetsfunktioner till systemet. I figuren finns IT-säkerhetsfunktionerna placerade i systemet, vilken IT-säkerhetsfunktion som är aktuell illusteras med dess unika identitet.*

## Intrångsskydd/Separation

*Här skrivs en sammanfattning av intrångs- och separationsfunktioner, på en övergripande nivå samt med fokus på hur dessa agerar tillsammans med det aktuella systemet. Det kan vara en fördel att beskriva dessa genom en övergripande vy. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

*Exempel*

*Allmän beskrivning av IT-säkerhetsfunktionen och den tänkta användningen.*

*Separation innebär att dela upp infrastrukturen i informationszoner vars syfte är att all kommunikation mellan olika zoner skall vara kontrollerad och att ingen information lämnar en zon utan att en komponent granskat den.*

*Att dela in ett system i informationszoner med kontrollerade övergångar följer tre principer för informationssäkerhet:*

 *Skottindelning, indelning i zoner gör så att ett intrång i en zon inte får effekter i en annan.*

* *Försvar på djupet, gör att en angripare måste ta sig förbi flera barriärer för att nå den mest hemliga informationen.*
* *Kontrollpunkt/flaskhals, vid åtkomst till information tvingas gå genom skyddsmekanismer så en angripare inte kan välja olika vägar som eventuellt kan ha mindre skydd.*

*Kommunikationen kan kontrolleras med hjälp av informationstrappor, datadioder och väggar. Informationstrappor är dubbelriktade och enbart definierade informationsmängder och informationstyper kan passera genom trappan. Datadioder ser till att kommunikationen är enkelriktad och att en lägre klassificerad zon inte når en högre klassificerad zon och vice versa. En vägg kan ytterligare separera en zon genom mjukvarufunktioner eller filter som begränsar kommunikationen inom zonen, de zonerna kallas segment.*

*För att uppfylla separationskraven på det aktuella systemet har det delats upp i tre delar:*

* *informationszon A för servrar*
* *informationszon B för klienter med höga sekretesskrav*
* *samt informationszon C för vanliga klienter*

*Separeringen implementeras genom hårdvarubrandväggar, både mellan de olika zonerna men även för att separera klienterna inom informationszon B i olika segment.*

*Mellan nät av hög och låg informationsklass skall brandväggarna även ha stöd för nod funktionalitet.*

*Mellan informatioszon A och informationszon B skall en kontrollpunkt finnas som möjliggöra överföring av information på ett kontrollerat sätt via filterfunktion.*

*På samtliga klienter och servrar skall mjukvarubrandvägg och intrångsdetektionsprogramvara finnas.*

*Figur 1 nedan illustrerar separationen inom systemet, med dess olika IT-säkerhetsfunktioner utmarkerade med namn och identitet på säkerhetsfunktioner.*

*Figur 1 Separation med Informationszoner samt allokering av IT-säkerhetsfunktionerer*

### IT-Säkerhetsfunktion, intrång- och separation

*Här beskrivs de IT-säkerhetsfunktioner om är identifierade för systemet. IT-säkerhetsfunktionen mappas mot de nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *SäkFunk-001* |
| Beskrivning | En av Försvarsmakten ackrediterad Hårdvarubasserad, filtrerande OSI nivå3 brandvägg med proxy, IDS funktionalitet |
| Kravallokering från TS | SäkKrav01, SäkKrav02, SäkKrav03, SäkKrav04, SäkKrav05, SäkKrav06, SäkKrav07, HotKrav01 (kraven hämtade från avsnitt 3.1) |
| Verifierings-metod | Oberoende värdering, dokumentation och praktisk tekniska granskningar. |

|  |  |
| --- | --- |
| Funktion | *SäkFunk-002* |
| Beskrivning | Mjukvarubrandvägg av för Försvarsmakten godkänd typ |
| Kravallokering från TS | SäkKrav09, Hot 02 |
| Verifieringsmetod | Dokumentation |

|  |  |
| --- | --- |
| Funktion | *SäkFunk-003* |
| Beskrivning | Intrångsdetektionsprogramvara av för Försvarsmakten godkänd typ |
| Kravallokering från TS | SäkKrav10, Hot03 |
| Verifieringsmetod | Dokumenation |

|  |  |
| --- | --- |
| Funktion | *SäkFunk-004* |
| Beskrivning | Informationstrappa, Utöver övrig funktionalitet nod funktionalitet för nod kunna implementeras. |
| Kravallokering från TS | SäkKrav011, Hot 04 |
| Verifieringsmetod | Oberoende värdering, dokumentation samt penetrationstester |

|  |  |
| --- | --- |
| Funktion | *SäkFunk-005* |
| Beskrivning | Informationsfilter(informationstrappa)  |
| Kravallokering från TS | SäkKrav012, Hot 05 |
| Verifieringsmetod | Oberoende värdering, dokumentation samt penetrationstester |

## Logghantering

*Detta avsnitt innehåller en sammanfattning av hantering av säkerhetsloggar på en övergripande nivå samt med fokus på hur dessa agerar tillsammans.*

*Det kan vara en fördel att beskriva dessa genom en övergripande vy se exempel avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-Säkerhetsfunktioner, Logghantering, säkerhetsloggar

*Här beskrivs IT-säkerhetsfunktion för Logghantering som är identifierat för systemet, IT-säkerhetsfunktionen mappas även mot de nerbrutna IT-säkerhetssäkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion* |

## Autentisering och behörigheter

*Detta avsnitt ger en sammanfattning av autentiserings- och behörighetshantering, på en övergripande nivå. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se exempel i avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-säkerhetsfunktionen, Autentisering och behörighet

*Här beskrivs IT-säkerhetsfunktionen för autentisering och behörighet för systemet. IT-säkerhetsfunktionen mappas även mot de nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

## Signalskydd

*Här skrivs en sammanfattning av systemets signalskydd, på en övergripande nivå. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-säkerhetsfunktioner, signalskydd

*Här beskrivs IT-säkerhetsfunktion för siganskydd som är identifierade för systemet, IT-säkerhetsfunktionen mappas även mot de nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

## IDS-funktionalitet

*Här skrivs en sammanfattning av IDS-funktionalitet, på en övergripande nivå. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-säkerhetsfunktioner, IDS

*Här listas IT-säkerhetsfunktioner för intrångsdetektering för systemet. IT-säkerhetsfunktionen mappas även mot de nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

## Informationshantering och back up

*Här skrivs en sammanfattning av funktioner för informationshantering och backup, på en övergripande nivå. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-säkerhetsfunktion, Informationshantering och backup

*Här listas IT-säkerhetsfunktioner för Informationshantering och backup som är identifierade för systemet. IT-säkerhetsfunktionen mappas även mot de nerbrutna säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

## Skydd mot RÖS

*Här skrivs en sammanfattning av skyddet mot RÖS, på en övergripande nivå samt med fokus på hur dessa agerar tillsammans. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-Säkerhetsfunktioner, skydd mot RÖS

*Här listas de IT-säkerhetsfunktioner för RÖS som är identifierade för systemet.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

## Integritetsskydd

*Här skrivs en sammanfattning av integritetsskyddet, på en övergripande nivå samt med fokus på hur dessa agerar tillsammans. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-Säkerhetsfunktioner, integritetsskydd

*Här listas de IT-säkerhetsfunktioner som är identifierade för systemet, IT-säkerhetsfunktionen mappas även mot de nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetid | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

## Säkerhetsadministration

*Här skrivs en sammanfattning av säkerhetsadministrationen, på en övergripande nivå. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-Säkerhetsfunktioner, säkerhetsadministration

*Här listas IT-säkerhetsfunktioner för säkerhetsadministration som är identifierade för systemet. IT-säkerhetsfunktionen mappas även mot nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

##  Skydd mot skadlig kod

*Här skrivs en sammanfattning av skyddet mot skadlig kod, på en övergripande nivå samt med fokus på hur dessa agerar tillsammans. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-Säkerhetsfunktioner, skydd mot skadlig kod

*Här listas de IT-säkerhetsfunktioner för skydd mot skadlig kod som är identifierade för systemet. IT-säkerhetsfunktionen mappas även mot de nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

## Övrigt

*Här skrivs en sammanfattning av övriga säkerhetsfunktioner på en övergripande nivå. Det kan vara en fördel att beskriva dessa genom en övergripande vy, se avsnitt 4.1. Förutom beskrivningen skall även ett resonemang föras avseende varför olika funktioner har valts.*

### IT-Säkerhetsfunktioner, övriga

*Här listas övriga IT-säkerhetsfunktioner som är identifierade för systemet. IT-säkerhetsfunktionen mappas även mot nerbrutna IT-säkerhetskraven.*

|  |  |
| --- | --- |
| Funktion | *Namn på säkerhetsfunktionen* |
| Beskrivning | *Beskrivning av funktionen* |
| Kravmappning | *De säkerhetskrav som denna funktion hjälper, helt eller delvis att lösa ut.* |
| Verifieringsmetod | *Vilken metod som ska användas för att verifieria IT-säkerhetskrav och IT-säkerhetsfunktion.* |

# IT-Säkerhetsfunktioner som kräver särskild assurans

*I detta avsnitt definieras de kritiska IT-säkerhetsfunktioner som har identifierats i samband med kravspecificering av* *systemet. Syftet är att framhäva de säkerhetsfunktioner som med största sannolikhet kommer kräva särskild hög assurans och oberoende värdering.*

## Identifierade IT-säkerhetsfunktioner

*Här beskrivs de komponenter som behöver hög assuransnivå, varför och vilka konsekvenser detta antas få.*

## Funktioner med behov av oberoende granskning

*Ett vanligt sätt att omhänderta de särskilda assuranskraven är att ställa krav på en oberoende granskning av dessa. Om IT-säkerhetsfunktioner där detta är lämpligt har identifierats så beskrivs de här.*

# GFE-plan

*En GFE-plan ska tas fram som beskriver identifierade GFE: er, när i tiden de ska levereras, hur många som krävs och om det krävs särskilda åtgärder t.ex. utbildning.*