<SYSTEM> <VERSION>IT-SÄKERHETSSPECIFIKATION DEFINIERA (ITSS-D)

Innehåll

[Mallinformation 4](#_Toc72305960)

[Versionshistorik för mallen 4](#_Toc72305961)

[Generell mallinstruktion 4](#_Toc72305962)

[Specifik mallinstruktion 4](#_Toc72305963)

[Dokumentstruktur Definiera-fasen 4](#_Toc72305964)

[Att tänka på i arbetet med framtagning av ITSS-D 5](#_Toc72305965)

[1 Basfakta 6](#_Toc72305966)

[1.1 Giltighet och version 6](#_Toc72305967)

[1.2 Terminologi 6](#_Toc72305968)

[1.3 Referenser 6](#_Toc72305969)

[1.4 Underbilagor 6](#_Toc72305970)

[2 Inledning 7](#_Toc72305971)

[2.1 Syfte 7](#_Toc72305972)

[2.2 ITSS referens 7](#_Toc72305973)

[2.3 IT-systemreferens 7](#_Toc72305974)

[2.4 Styrande dokument 7](#_Toc72305975)

[2.5 Systemöversikt 7](#_Toc72305976)

[2.6 KSF-kravnivå 8](#_Toc72305977)

[2.6.1 Konsekvensnivå 8](#_Toc72305978)

[2.6.2 Exponeringsnivå 9](#_Toc72305979)

[2.6.3 Fastställande av KSF-kravnivå 11](#_Toc72305980)

[3 Systembeskrivning 12](#_Toc72305981)

[3.1 Förutsättningar 12](#_Toc72305982)

[3.1.1 Avsedd användning av systemet 12](#_Toc72305983)

[3.1.2 Tänkta användare och deras rättigheter 12](#_Toc72305984)

[3.1.3 Informationssystemets driftmiljö 12](#_Toc72305985)

[3.1.4 Information 13](#_Toc72305986)

[3.1.5 Avgränsning av ackrediteringsobjektet 13](#_Toc72305987)

[3.2 Informationssystemets arkitektur 13](#_Toc72305988)

[3.3 Informationssystemets externa gränsytor 14](#_Toc72305989)

[3.3.1 Fysiska externa gränsytor 14](#_Toc72305990)

[3.3.2 Logiska externa gränsytor 14](#_Toc72305991)

[3.4 Säkerhetsförmågor 14](#_Toc72305992)

[4 Sammanställning av säkerhetskrav 15](#_Toc72305993)

[4.1 Krav från KSF 15](#_Toc72305994)

[4.1.1 Funktionella säkerhetskrav 15](#_Toc72305995)

[4.1.2 Assuranskrav 40](#_Toc72305996)

[4.2 Tillkommande säkerhetskrav 68](#_Toc72305997)

[4.2.1 Säkerhetskrav från verksamheten 68](#_Toc72305998)

[4.2.2 Säkerhetskrav från regelverk 68](#_Toc72305999)

[4.2.3 Säkerhetskrav från hot- och riskanalys 69](#_Toc72306000)

[4.2.4 Övriga säkerhetskrav 69](#_Toc72306001)

[5 Säkerhetskrav på omgivningen 70](#_Toc72306002)

[6 Tolkade säkerhetskrav 71](#_Toc72306003)

[7 Uppfyllande av säkerhetskrav 72](#_Toc72306004)

# Mallinformation

## Versionshistorik för mallen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Datum | Version | Beskrivning | Ansvarig | Fastställd  |
| 2021-05-19 | 1.0 | ISD 3.1 | Ulf Christensen |  |

## Generell mallinstruktion

* Detta kapitel innehåller information avsedd att hjälpa författaren till dokumentet. Kapitlet ska raderas i sin helhet innan dokumentet färdigställs.
* Röd text (som denna) är en vägledning till författaren och ska raderas innan dokumentet färdigställs.
* Text som befinner sig innanför ”<“ och ”>” uppdateras eller tas bort. T.ex. ska <system><version> ersättas med informationssystemets namn och version (d.v.s. det IT-system som ska ackrediteras).
* Övrig svart text kan användas i det färdigställda dokumentet.

## Specifik mallinstruktion

* Denna mall används för att skapa dokumentet ITSS-D i ISD-processens *Definiera*-fas.
* FMV Projektledare är ansvarig för ITSS-D.
* ITSS-D är en bilaga till ISD-D. ITSS-D godkänns i och med att huvuddokumentet godkänns.

## Dokumentstruktur Definiera-fasen

Dokumentstrukturen för ISD-processens *Definiera*-fas illustreras nedan. Här visas att ISD-planen styr ISD-arbetet som resulterar i dokument ISD-D med dess tre bilagor.



* ISD-planen styr ISD-arbetet i genomförandeprojektet. Planen klargör förutsättningar och utmaningar, aktiviteter och leveranser med tidplan, vilka kompetenser som behövs, och vilken projektsamverkan som behöver finnas.
* ISD-D deklarerar realiserbarheten av informationssystemet utifrån informationssäkerhetens perspektiv.
* AU-D innehåller bl.a. de analyser som genomförts, redovisning av kravspårning, hantering av inte tillämpbara krav, förteckning över krav som ska hanteras av evalueraren samt redovisning över hur designreglerna omhändertagits.
* ITSS-D bygger vidare på ITSS-I (eller på FM ITSS om ingen ITSS-I finns) med tolkade och allokerade informationssäkerhetskrav, på en detaljnivå att kraven kan användas för upphandling och verifiering.
* ITSA dokumenterar säkerhetsarkitekturen som dels uppfyller informationssäkerhetskraven och dels harmoniserar med System Engineering-arbetet i projektet.

## Att tänka på i arbetet med framtagning av ITSS-D

Lämplig kompetens för att utarbeta ITSS-D finns hos ISA, med stöd av ISM-rollen.

Arbetet med AU-D, ITSS-D och ITSA hänger samman och utförs med fördel parallellt.

Finns ITSS-I bör stora delar kunna återanvändas i ITSS-D. Mallarna skiljer sig dock något, så lämpligast kopieras innehållet avsnitt för avsnitt *istället* för att bara döpas om från ITSS-I till
ITSS-D.

Strukturen i denna mall är FMVs tolkning av KSF-kraven för ITSS som anges i SASS-klassen [2]. Genom att följa mallens struktur och anvisningar ökar chansen att dokumentet evalueras med godkänt resultat mot denna kravklass.

Kravhanteringen dokumenteras och utvecklas succesivt via IT-Säkerhetsspecifikationerna i *Identifiera*-fasen (ITSS-I), *Definiera*-fasen (ITSS-D) och *Realisera*-fasen (ITSS-R). Detta bidrar till spårbarheten i säkerhetslösningen och det är mot ITSS-R som evaluering av kravuppfyllnad genomförs. Denna ligger i sin tur till grund för FMVs Informationssäkerhetsdeklaration (ISD), som produceras i *Realisera*-fasen.

ITSS-I innehåller systembeskrivning och informationssäkerhetsrelaterade krav som ställs på informationssystemet och dess omgivning.

Bra underlag för att skapa ITSS-D kan vara t.ex.:

* ITSS-I.
* ISD-plan
* Särskild säkerhetsskyddsbedömning från Försvarsmakten
* ITSS från Försvarsmakten
* AU-I
* AU-D

# Basfakta

## Giltighet och version

Detta dokument är ITSS i ISD-processens *Definiera*-fas (ITSS-D) för <informationssystem><version> inför FMV VHL T2- och T3-beslut.

| Datum | Version | Beskrivning | Ansvarig |
| --- | --- | --- | --- |
| <datum> |  | Initial version |  |
|  |  |  |  |
|  |  |  |  |

Tabell 1 – Versionshistorik

## Terminologi

Se referens [1] för en generell förteckning över begrepp och förkortningar som används inom ISD-processen. Följande tabell innehåller specifika begrepp och förkortningar som används i *detta* dokument.

| Begrepp/förkortning | Definition/förklaring |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

Tabell 2 – Begrepp och förkortningar

## Referenser

Använd kommentarskolumnen i tabellen nedan för att ange t.ex. status, klassning, utgivande organisation, författare eller årtal.

| Referens | Beteckning  | Kommentar |
| --- | --- | --- |
| 1. ISD v3.1, Begrepp och förkortningar
 | 20FMV5903-1:1.1 |  |
| 1. Beslut om krav på godkända säkerhetsfunktioner version 3.1 (KSF v3.1)
 | FM2014-5302:1 |  |
| 1. AU-I <system>
 | <TBD> |  |
| 1. AU-D <system>
 | <TBD> |  |

Tabell 3 – Referenser

## Underbilagor

Om detta dokument har några underbilagor ska dessa förtecknas här. Annars radera nedanstående och skriv ”Inga underbilagor.”

Detta dokument har följande underbilagor:

* Underbilaga 1: <titel på underbilaga 1>
* ...

# Inledning

## Syfte

Syftet med ITSS-D är att specificera samtliga informationssäkerhetskrav på informationssystemet respektive på driftmiljön. Kraven på informationssystemet ska kunna ingå i kravställning vid upphandling av utveckling av informationssystemsystemet från en eller flera leverantörer. Kraven på driftmiljön ska kunna ingå som förutsättningar i *Informationssäkerhetsdeklarationen*.

## ITSS referens

Här ska en unik referens för detta dokument ges enligt KSF-krav SASS\_INL.C1-C2. Dokumentet kan ges en unik referens med diarienummer och är detta fallet så kan nedanstående text användas.

Diarienummer utgör en unik dokumentreferens och anges i sidhuvudet.

## IT-systemreferens

Här ska en unik referens ges för informationssystemet (ackrediteringsobjektet) i enlighet med KSF-krav SASS\_INL.C1 och C3.

En unik referens kan t.ex. vara i form av M-nummer. I denna version av ITSS (ITSS-D) finns normalt ingen unik referens uttagen ännu och i så fall kan följande text användas.

Informationssystemet som denna ITSS omfattar är enligt vad som är angivet som titel på detta dokument.

En unik referens kommer att tillföras under detta avsitt i senare version av dokumentet.

## Styrande dokument

Här ska, i enlighet med KSF-kraven SASS\_INL.C4 och C5, anges:

* Vilken version av KSF-krav som tillämpas.
* Vilka styrande dokument man tagit hänsyn till.
* Vilka ev. internationella standarder man baserat arbetet på.
* Övriga säkerhetsrelaterade styrningar ackrediteringsobjektet ska tillämpa.

Följande dokument är styrande för denna ITSS:

* KSF version 3.1, referens [2]
* <lista referenser till andra styrande säkerhetsrelaterade dokument>

## Systemöversikt

Detta avsnitt beskriver informationssystemets användning och säkerhetsmekanismer, samt dess övergripande systemarkitektur.

Systemöversikten ska kortfattat beskriva arkitekturen, användningen och säkerhetsmekanismerna för informationssystemet i enlighet med KSF-krav SASS\_INL.C7. Beskrivningen ska ge en översiktlig bild informationssystemets säkerhetsförmåga och dess tänkta användning. Lämplig ambitionsnivå är 1-2 sidor. En mer utförlig systembeskrivning ges i kapitel 3 *Systembeskrivning*.

## KSF-kravnivå

Detta avsnitt ska visa de fastställda kravnivåerna (i enlighet med KSF-krav SASS\_INL.C4) och motivera valet (i enlighet med SASS\_SYS.C2). Föregående avsnitt 2.5 ska vara tillräckligt omfattande för att förstå denna motivering.

KSF-kravnivå utgör ingångsvärde för fortsatt arbete med krav och kravkomponenter i KSF, referens [2].

KSF-kravnivån som informationssystemet (ackrediteringsobjektet) ska uppfylla är fastställd till <Grund/Utökad/Hög>.

Motivering av fastställd kravnivå görs i följande underavsnitt.

### Konsekvensnivå

Vid en informationsklassificering identifieras vilken skyddsvärd information som hanteras av informationssystemet. Med hjälp av säkerhetsskyddsklassificeringen kan sedan en konsekvensnivå identifieras. Konsekvensnivån för systemet identifieras enligt Tabell 4 utifrån vilken konsekvens som uppstår om ett informationssystems skyddsvärda tillgångar röjs, förvanskas eller förloras.

| Gradering | Generell konsekvensbeskrivning samt konsekvensbeskrivning vid informationsförlust av sekretessklassificerade uppgifter | Konsekvensbeskrivning avseende informationsförlust av hemliga eller utrikesklassificerade uppgifter |
| --- | --- | --- |
| K5  | Synnerligen allvarlig | Förväntade konsekvenser medför en synnerlig negativ effekt. Konsekvenserna innebär synnerligen allvarliga negativa effekter av stor omfattning, under lång tid och utgör ett direkt hot mot organisationen. Konsekvenserna är inte begränsade till enstaka förmågor eller funktioner inom organisationen. | Hemliga uppgifter vars röjande kan medföra synnerligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet (kvalificerat hemliga uppgifter). Hemlig handling som har åsatts beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |
| K4 | Allvarlig | Förväntade konsekvenser är betydande. Konsekvenserna är allvarliga, av stor omfattning eller av väsentlig art och innebär ett direkt hot, om än mot avgränsade förmågor eller funktioner inom organisationen. | Hemliga uppgifter vars röjande kan medföra betydande men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. Hemlig handling som har åsatts beteckningen SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |
| K3 | Kännbar | Förväntade konsekvenser är inte obetydliga och äventyrar, vållar skada, hindrar, underlättar, innebär större avbrott samt medför påtagliga negativa effekter om än i begränsad omfattning. | Hemliga uppgifter vars röjande kan medföra ett inte obetydligt men för totalförsvaret eller för- hållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. Hemlig handling som har åsatts beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |
| K2 | Lindrig | Förväntade konsekvenser är ringa och begränsas till att påverka, försvåra, hindra, undergräva, misskreditera eller störa verksamheten i mindre omfattning. | Hemliga uppgifter vars röjande kan medföra endast ringa men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. Hemlig handling som har åsatts beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation. |
| K1 | Försumbar | Konsekvenser för verksamheten är försumbara. | Uppgifter är inte hemliga eller utrikesklassificerade. |

Tabell 4 – Bedömning av konsekvensnivå enligt femgradig skala, referens [2]

Använd KSFs termer så att tolkningen av KSF-kraven kan baseras på dessa.

*Exempel: Identifierad konsekvensnivå för informationssystemet är K4, då systemet hanterar information med sekretess, säkerhetsskyddsklassificerad upp till och med Hemlig (H).*

Identifierad konsekvensnivå för informationssystemet är <K1/K2/K3/K4/K5>, eftersom det hanterar information med <motivering>.

### Exponeringsnivå

Exponeringsnivån är ett mått på hur informationssystemet exponeras gentemot annan aktörs möjlighet att påverka det. Möjligheten kan vara såväl fysisk, d.v.s. att någon kommer åt informationssystemets tekniska utrustning, som logisk via systemets olika gränssnitt.

*Tabell* *5* listar olika exponeringsnivåer med tillhörande kriterier, enligt referens [2]. Ökade möjligheter för aktör att påverka systemet definieras som en högre exponeringsnivå, vilket i sin tur medför högre krav på informationssystemets säkerhetsförmåga.

| Exponeringsnivå | Kriterier för exponeringsnivå |
| --- | --- |
| Tillgång till systemets fysiska och logiska gränsytor |  | Informationsutbyte |
| E4 | Alla fall som inte uppfyller kriterierna för någon av exponeringsnivå E1-E3 nedan. |  | Alla fall som inte uppfyller kriterierna för någon av exponeringsnivå E1-E3 nedan. |
| E3 | Alla personer med tillgång till någon av systemets gränsytor är säkerhetsprövade. | **och** | Samtliga system som systemet utbyter information med är ackrediterade till en högre konsekvensnivå**eller**Samtliga system som systemet utbyter information med är ackrediterade till samma konsekvensnivå med högst exponeringsnivå E3. |
| E2 | Alla personer med tillgång till någon av systemets gränsytor är behöriga till någon information inom den högsta konsekvensnivån som behandlas i systemet. | **och** | Samtliga system som systemet utbyter information med är ackrediterade till en högre konsekvensnivå**eller**Samtliga system som systemet utbyter information med är ackrediterade till samma konsekvensnivå med högst exponeringsnivå E2. |
| E1 | Alla personer med tillgång till systemets gränsytor är behöriga till all information som behandlas i systemet. | **och** | Systemet utbyter ingen information med andra system. |

Tabell 5 – Exponeringsnivåer med tillhörande kriterier, referens [2]

Använd KSFs termer så att tolkningen av KSF-kraven kan baseras på dessa.

Röd text nedan är exempel på motiveringar för att hitta rätt exponeringsnivå.

Tillgång till systemets fysiska och logiska gränsytor:

* *Ex: Alla personer med tillgång till någon av systemets gränsytor är behöriga till någon information inom den högsta konsekvensnivån K4.*

Informationsutbyte:

* *Ex: Ackrediteringsobjektet utbyter information med två andra system. Båda dessa är ackrediterade till K4 och har exponeringsnivå E2.*

Enligt Tabell 5 blir exponeringsnivån för informationssystemet: <E1/E2/E3/E4>.

### Fastställande av KSF-kravnivå

Enligt referens [2], ska *Tabell* *6* användas för att fastställa KSF-kravnivån på informationssystemet.

Röd tabell nedan är exempel på hur man kan illustrera identifierad kravnivå.

| Konsekvensnivå | Kriterier för exponeringsnivå |
| --- | --- |
| E1 | E2 | E3 | E4 |
| K5 | H | H | H | H |
| K4 | U | H | H | H |
| K3 | U | U | U | H |
| K2 | G | U | U | U |
| K1 | G | G | G | G |

| Konsekvensnivå | Kriterier för exponeringsnivå |
| --- | --- |
| E1 | E2 | E3 | E4 |
| K5 | H | H | H | H |
| K4 | U | H | H | H |
| K3 | U | U | U | H |
| K2 | G | U | U | U |
| K1 | G | G | G | G |

Tabell 6 – Kravnivåer för funktionella säkerhetskrav och assuranskrav, referens [2]. G = Grund, U = Utökad och H = Hög.

*Tabell 6* ger KSF-kravnivån <Grund/Utökad/Hög>.

# Systembeskrivning

Detta kapitel syftar till att uppfylla KSF-krav SASS\_SYS.D1, C1-C11.

Systembeskrivningen ska ge en utförlig beskrivning av informationssystemet. Beskrivningen ska ge de som ackrediterar systemet, användarna samt drift och förvaltning en djupare förståelse för säkerhetsförmågan i systemet än vad som ges i kapitlet *Inledning*.

Detta kapitel är en systembeskrivning där informationssystemets förutsättningar, arkitektur, gränsytor samt säkerhetsförmågor framgår.

I denna version av ITSS (ITSS-D) är inte alla nödvändiga detaljer utarbetade. ITSS-D används inför kravställning till leverantör. Leverantörens design- och implementeringsbeslut kan komma att påverka denna systembeskrivning, som då behöver anpassas i kommande ITSS-R.

Både ITSA och ITSS-D innehåller en systembeskrivning. Om dessa kan utformas som *en* *gemensam* systembeskrivning kan det vara lämpligt att dokumenteringen endast sker i ett av dokumenten, och det andra dokumentet refererar dit. Det kan också vara så att den ena systembeskrivningen behöver vara djupare eller ha ett annat fokus än den andra för att fylla sina syften. I så fall kan det vara aktuellt att skapa två separata systembeskrivningar, men att den ena hänvisar i delar till den andre för att minimera upprepningar.

## Förutsättningar

Detta avsnitt beskriver förutsättningarna som har styrt framtagning av säkerhetsarkitekturen, allokering av säkerhetskraven samt hur KSF har tolkats.

### Avsedd användning av systemet

Detta avsnitt avser att, tillsammans med avsnitt 3.1.2, uppfylla KSF-krav SASS\_SYS.C4

Beskriv verksamheten som informationssystemet ska stödja och hur detta stöd ska ske utifrån användarens perspektiv i termer av förmågor, användarroller, bearbetning, lagring och överföring av information.

<Beskriv avsedd användning av systemet>

### Tänkta användare och deras rättigheter

Detta avsnitt avser att, tillsammans med avsnitt 3.1.1, uppfylla KSF-krav SASS\_SYS.C4

Beskriv de tänkta användarrollerna i systemet och gruppera de gärna efter åtkomst till resurser och information. Exempelvis kan olika administratörer (Behörighets- , System- och Säkerhetsloggadministratör) placeras i olika grupper beroende på åtkomst.

<Beskriv tänkta användare och deras rättigheter>

### Informationssystemets driftmiljö

Beskriv informationssystemets placering i driftmiljön genom att beskriva fysiskt skydd, tillträdesbegränsning och andra förutsättningar som är säkerhetsrelevanta.

*T.ex:*

* *Hur mycket tid och resurser som kan läggas på administrativa rutiner.*
* *Förväntad kompetensnivå på de olika rollerna som ska hantera systemet.*
* *Hur kraft och reservkraft hanteras.*
* *Förutsättningar för röjande signaler (RÖS).*
* *Fysisk åtkomstmöjlighet.*

<Beskriv systemets driftmiljö>

### Information

Detta avsnitt avser uppfylla KSF-krav SASS\_SYS.C1

Beskriv typ av information, mängd, skyddsvärde, sekretessklassning och eventuella andra hanteringsregler (t.ex. från lagkrav) kring all data som hanteras av informationssystemet.

Använd termer från KSF vid beskrivning av information, konsekvens och exponering så att tolkningen av KSF-kraven kan baseras på dessa faktorer.

<Beskriv informationen i informationssystemet>

### Avgränsning av ackrediteringsobjektet

För att tydliggöra vad som omfattas av denna ITSS och vad som behöver hanteras av driftmiljön anges här avgränsning av informationssystemet (ackrediteringsobjektet).

Ett sätt att illustrera ackrediteringsobjektet är att beskriva tre zoner som ligger inuti varandra:

1. **Innersta zonen - ackrediteringsobjektet**

Innersta zonen innehåller det tekniska i informationssystemet som ska ackrediteras. Exempelvis programvara, operativsystem, datorhårdvara, nätverksutrustning, aktiva kort och brandväggar. Komponenter placerade i denna zon, som inte redan är godkända, kommer att kravställas och evalueras i ISD-arbetet.

1. **Omgivningen**

Zonen som omger ackrediteringsobjektet innehåller driftmiljön för informationssystemet. Exempelvis andra system med gränsytor till informationssystemet, entiteter som interagerar med informationssystemet, organisationer som äger/ansvarar/drift- och underhåller informationssystemet med alla dess instruktioner, manualer och rutinbeskrivningar. Ackrediteringsobjektet har ett beroende till denna driftmiljö tack vare att vissa informationssäkerhetskrav realiseras här eller på grund av interagerande system.

1. **Utanför omgivningen**

Yttersta zonen innehåller system, roller, organisation, rutiner m.m. som inte har någon påverkan eller interaktion med informationssystemet. Men det är lämpligt att förtydliga att dessa är avgränsade från ackrediteringsobjektet och dess omgivning.

<Beskriv avgränsning av ackrediteringsobjektet>

## Informationssystemets arkitektur

Detta avsnitt avser att uppfylla KSF-kraven SASS\_SYS.C7, C8 och C9.

För att kunna identifiera säkerhetskraven för informationssystemet är det nödvändigt att specificera dess övergripande arkitektur. Arkitekturbeskrivningen ska identifiera informationssystemets komponenter, beskriva hur de samverkar och visa vilka informationsflöden som finns.

Systemarkitekturen ska byggas på ett sådant sätt att den har förmåga att skydda informationssystemet för hot i och utanför systemet.

<Beskriv systemets arkitektur>

## Informationssystemets externa gränsytor

Detta avsnitt avser att uppfylla KSF-krav SASS\_SYS.C5, C6 och C9.

Detta avsnitt identifierar informationssystemets alla externa gränsytor, logiska och fysiska. Med externa avses gränsytor som är mellan ackrediteringsobjektet och driftmiljön.

*Beskrivningen ska t.ex. innehålla:*

* *Definition av gränssnitt och fysisk placering*
* *Syfte med gränsytan*
* *Identifiering av vilken information som är tänkt att utbytas vid gränsytan*
* *Beskrivning över hur informationsutbytet är tänkt att ske, med riktning*
* *Referens till komponenter i arkitekturbeskrivningen som utgör gränsytan*
* *Referens till eventuella komponenter som är avsedda att skydda gränsytan eller kontrollera informationsutbytet.*

Det är via gränsytorna som systemet exponeras från personer, både fysiskt och logiskt. Ange hur respektive gränsyta blir exponerad. Denna exponeringsanalys kan beskriva eller refereras tillsammans med kapitel 2.6.2.

Använd termer från KSF så att tolkningen av KSF-kraven kan baseras på dessa faktorer.

### Fysiska externa gränsytor

<Beskriv informationssystemets fysiska externa gränsytor>

### Logiska externa gränsytor

<Beskriv informationssystemets logiska externa gränsytor>

## Säkerhetsförmågor

Detta avsnitt ska uppfylla KSF-kravet SASS\_SYS.C10

Medan systemarkitekturen beskriver informationssystemets uppbyggnad och dess komponenter, beskrivs här systemets säkerhetsförmågor och -funktioner som systemet tillhandahåller. Säkerhetsförmågorna ska beskrivas på en detaljnivå som är tillräcklig för att ge läsaren en allmän förståelse.

<Beskriv systemets säkerhetsförmågor>

# Sammanställning av säkerhetskrav

Detta kapitel ska uppfylla KSF-kraven SASS\_KRV.D1, C1 till C4 och C6.

Detta kapitel identifierar de informationssäkerhetskrav som ställs på informationssystemets och dess omgivning. Informationssäkerhetskraven kommer hädanefter att benämnas säkerhetskrav; enligt språkbruk i KSF.

Säkerhetskraven delas in i två kategorier; *Krav från* *KSF* samt *Tillkommande Säkerhetskrav*.

## Krav från KSF

Krav från KSF definierar två typer av säkerhetskrav: *funktionella säkerhetskrav* och *assuranskrav*. Alla kravkomponenter från den fastställda kravnivån listas under detta kapitel.

I följande underavsnitt listas kraven utifrån den kravnivå som tidigare fastställts. Parentesen framför tabellerna identifierar vilken kravnivå som gäller (Grund, Utökad eller Hög). I vissa fall ser tabellen likadan ut i flera av kravnivåerna.

Spara endast de tabeller som gäller för informationssystemets kravnivå, ta bort övriga.

### Funktionella säkerhetskrav

#### Gemensamma krav (SFGK)

Vissa krav på säkerhetsfunktioners grundläggande funktionalitet är gemensamma och gäller alla komponenter i systemet som bidrar till att upprätthålla säkerheten. Dessa krav ska gälla för varje säkerhetsfunktion, men definieras i detta kapitel för att förenkla kravidentifikation.

##### Säkert tillstånd (SFGK\_FEL)

Säkerhetsfunktioner ska kunna upprätthålla ett säkert tillstånd vid fel. Fel i säkerhetsfunktioner eller dess styrande data ska upptäckas och systemet eller nödvändiga delar av systemet ska kunna försättas i ett definierat säkert tillstånd.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Ett definierat säkert tillstånd ska upprätthållas för de delar av systemet som berörs när hela eller delar av säkerhetsfunktionens konfiguration eller styrande data är korrupt eller oåtkomlig. Berörda delar av systemet innebär hela systemet eller, om så kan påvisas via analys, endast de delar av systemet som säkerhetsfunktionen skyddar. | SFGK\_FEL.1 |
| Ett definierat säkert tillstånd ska upprätthållas tills normal drift har återupptagits. | SFGK\_FEL.2 |

Tabell 7 – Funktionella krav – Gemensamma krav SFGK\_FEL

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Ett definierat säkert tillstånd ska upprätthållas för de delar av systemet som berörs när hela eller delar av säkerhetsfunktionens konfiguration eller styrande data är korrupt eller oåtkomlig. Berörda delar av systemet innebär hela systemet eller, om så kan påvisas via analys, endast de delar av systemet som säkerhetsfunktionen skyddar. | SFGK\_FEL.1 |
| Ett definierat säkert tillstånd ska upprätthållas tills normal drift har återupptagits. | SFGK\_FEL.2 |
| 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.3 |

Tabell 8 – Funktionella krav – Gemensamma krav SFGK\_FEL

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Ett definierat säkert tillstånd ska upprätthållas för de delar av systemet som berörs när hela eller delar av säkerhetsfunktionens konfiguration eller styrande data är korrupt eller oåtkomlig. Berörda delar av systemet innebär hela systemet eller, om så kan påvisas via analys, endast de delar av systemet som säkerhetsfunktionen skyddar. | SFGK\_FEL.1 |
| Ett definierat säkert tillstånd ska upprätthållas tills normal drift har återupptagits. | SFGK\_FEL.2 |
| 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.3 |
| Ingen användaraktivitet i systemet ska kunna ske om säkerhetsfunktionen är avstängd eller ur funktion. Nödvändig administration för att återställa systemet tillåts men verksamhetssystemets användare kan exempelvis bli utloggade. | SFGK\_FEL.4 |

Tabell 9 – Funktionella krav – Gemensamma krav SFGK\_FEL

##### Gemensam tid (SFGK\_TID)

Säkerhetsfunktionen ska använda systemets gemensamma tid. En gemensam och tillförlitlig tid är viktigt bland annat för:

* Autentisering som förlitar sig på tid för validering av säkerhetsattribut såsom certifikat eller genererade lösenord
* Behörighetskontroller med begränsningar baserade på tid
* Spårbarhet av händelser i systemet

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemgemensam tillförlitlig tid ska finnas tillgänglig. | SFGK\_TID.1 |
| Säkerhetsfunktioner ska använda den systemgemensamma tiden. | SFGK\_TID.2 |

Tabell 10 – Funktionella krav – Gemensamma krav SFGK\_TID

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemgemensam tillförlitlig tid ska finnas tillgänglig. | SFGK\_TID.1 |
| Säkerhetsfunktioner ska använda den systemgemensamma tiden. | SFGK\_TID.2 |
| Om säkerhetsfunktionen har externa beroenden eller helt eller delvis uppfylls av komponenter utanför systemet ska systemet ha en tid som är gemensam med de externa delarna, exempelvis genom att båda systemen tar tid från samma externa tidskälla. | SFGK\_TID.3 |

Tabell 11 – Funktionella krav – Gemensamma krav SFGK\_TID

#### Behörighetskontroll (SFBK)

Behörighetskontroll innebär att kunna avgöra vem eller vad som begär åtkomst till systemet eller informationen som behandlas i det och endast medge åtkomst om behörighet har tilldelats.

##### Unik identitet (SFBK\_UID)

Subjektet ska ha en unik identitet. För att möjliggöra spårning av aktivitet i systemet och en effektiv åtkomstkontroll måste alla subjekt i systemet representeras av en i systemet unik och otvetydig identitet.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla subjekt ska i systemet ha en unik identitet. | SFBK\_UID.1 |
| Ett subjekts unika identitet ska vara konstant över tid. En unik identitet får inte återanvändas. Ett subjekt får dock t.ex. byta namn så länge den unika identiteten bevaras och identifierar samma subjekt. | SFBK\_UID.2 |

Tabell 12 – Funktionella krav – Behörighetskontroll SFBK\_UID

##### Autentisering av subjekt (SFBK\_AUT)

Autentisering av subjektet ska ske. Subjekt måste autentiseras med tillräcklig grad av tillförlitlighet för att åtkomstkontroll och säkerhetsloggning av subjekts åtgärder i systemet ska ske med rätt identitet.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Subjekt ska autentiseras vid inloggning och upprättande av session. | SFBK\_AUT.1 |
| Subjekt ska autentiseras innan de ges åtkomst till objekt i systemet. Detta avser inte grundläggande systemfunktioner där session måste upprättas innan autentiseringsmekanismerna kan aktiveras. | SFBK\_AUT.2 |
| Det ska finnas möjlighet till tidsbegränsning av sessioner. | SFBK\_AUT.3 |
| Subjekt ska tvingas återautentisera sig när tiden för en tidsbegränsad session har gått ut. | SFBK\_AUT.4 |
| Säkerhetsattribut som används för autentisering ska ha en längsta giltighetstid. | SFBK\_AUT.5 |
| Säkerhetsfunktionen ska minst använda lösenord eller motsvarande som säkerhetsattribut för autentisering. | SFBK\_AUT.6 |
| Kvaliteten på säkerhetsattribut för autentisering ska kunna kontrolleras, exempelvis genom tvingande komplexitetskrav vid tilldelning och byte av lösenord. | SFBK\_AUT.7 |
| Systemet ska ha funktioner för att kunna revokera säkerhetsattribut. | SFBK\_AUT.8 |
| Säkerhetsattribut får inte överföras i klartext vid autentisering. | SFBK\_AUT.9 |
| Säkerhetsattribut ska ha skydd mot obehörig avläsning och modifikation när dessa lagras eller transporteras i systemet. | SFBK\_AUT.10 |
| Systemet ska ha möjlighet att reagera på upprepade felaktiga autentiseringsförsök, även sådana där den angivna identiteten förändras mellan försöken. | SFBK\_AUT.11 |
| Vid upprepade autentiseringsfel ska systemet automatiskt kunna införa en exponentiellt ökande fördröjning av nya autentiseringsförsök för subjektet alternativt kunna låsa berört subjekts säkerhetsattribut under en viss tid. | SFBK\_AUT.12 |
| Systemet ska inte uppge felorsak till subjekt vid autentiseringsfel. Syftar till att inte ge en attackerande part användbara upplysningar, t.ex. ”Angivet subjekt existerar inte” eller ”Felaktigt lösenord”. | SFBK\_AUT.13 |

Tabell 13 – Funktionella krav – Behörighetskontroll SFBK\_AUT

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Subjekt ska autentiseras vid inloggning och upprättande av session. | SFBK\_AUT.1 |
| Subjekt ska autentiseras innan de ges åtkomst till objekt i systemet. Detta avser inte grundläggande systemfunktioner där session måste upprättas innan autentiseringsmekanismerna kan aktiveras. | SFBK\_AUT.2 |
| Det ska finnas möjlighet till tidsbegränsning av sessioner. | SFBK\_AUT.3 |
| Subjekt ska tvingas återautentisera sig när tiden för en tidsbegränsad session har gått ut. | SFBK\_AUT.4 |
| Säkerhetsattribut som används för autentisering ska ha en längsta giltighetstid. | SFBK\_AUT.5 |
| Säkerhetsfunktionen ska minst använda lösenord eller motsvarande som säkerhetsattribut för autentisering. | SFBK\_AUT.6 |
| Kvaliteten på säkerhetsattribut för autentisering ska kunna kontrolleras, exempelvis genom tvingande komplexitetskrav vid tilldelning och byte av lösenord. | SFBK\_AUT.7 |
| Systemet ska ha funktioner för att kunna revokera säkerhetsattribut. | SFBK\_AUT.8 |
| Säkerhetsattribut får inte överföras i klartext vid autentisering. | SFBK\_AUT.9 |
| Säkerhetsattribut ska ha skydd mot obehörig avläsning och modifikation när dessa lagras eller transporteras i systemet. | SFBK\_AUT.10 |
| Systemet ska ha möjlighet att reagera på upprepade felaktiga autentiseringsförsök, även sådana där den angivna identiteten förändras mellan försöken. | SFBK\_AUT.11 |
| Vid upprepade autentiseringsfel ska systemet automatiskt kunna införa en exponentiellt ökande fördröjning av nya autentiseringsförsök för subjektet alternativt kunna låsa berört subjekts säkerhetsattribut under en viss tid. | SFBK\_AUT.12 |
| Systemet ska inte uppge felorsak till subjekt vid autentiseringsfel. Syftar till att inte ge en attackerande part användbara upplysningar, t.ex. ”Angivet subjekt existerar inte” eller ”Felaktigt lösenord”. | SFBK\_AUT.13 |
| Förstärkt inloggning ska tillämpas. Krav på förstärkt inloggning finns i HKV 2007-03-26 12 830:65517 Krav för signalskyddssystem. Nyttjande av lösning med av MUST godkänt aktivt kort ska eftersträvas. | SFBK\_AUT.14 |
| Systemet ska skydda en inloggad session så att den inte kan nyttjas av obehörig. | SFBK\_AUT.15 |
| Sessioner ska omfattas av tidsbegränsning. | SFBK\_AUT.16 |
| Systemet ska kunna notifiera om autentiseringsfel. Med notifiera menas att göra någon lämplig person (t.ex. operatör, administratör eller övervakningspersonal) uppmärksam på vad som skett. | SFBK\_AUT.17 |

Tabell 14 – Funktionella krav – Behörighetskontroll SFBK\_AUT

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Subjekt ska autentiseras vid inloggning och upprättande av session. | SFBK\_AUT.1 |
| Subjekt ska autentiseras innan de ges åtkomst till objekt i systemet. Detta avser inte grundläggande systemfunktioner där session måste upprättas innan autentiseringsmekanismerna kan aktiveras. | SFBK\_AUT.2 |
| Det ska finnas möjlighet till tidsbegränsning av sessioner. | SFBK\_AUT.3 |
| Subjekt ska tvingas återautentisera sig när tiden för en tidsbegränsad session har gått ut. | SFBK\_AUT.4 |
| Säkerhetsattribut som används för autentisering ska ha en längsta giltighetstid. | SFBK\_AUT.5 |
| Säkerhetsfunktionen ska minst använda lösenord eller motsvarande som säkerhetsattribut för autentisering. | SFBK\_AUT.6 |
| Kvaliteten på säkerhetsattribut för autentisering ska kunna kontrolleras, exempelvis genom tvingande komplexitetskrav vid tilldelning och byte av lösenord. | SFBK\_AUT.7 |
| Systemet ska ha funktioner för att kunna revokera säkerhetsattribut. | SFBK\_AUT.8 |
| Säkerhetsattribut får inte överföras i klartext vid autentisering. | SFBK\_AUT.9 |
| Säkerhetsattribut ska ha skydd mot obehörig avläsning och modifikation när dessa lagras eller transporteras i systemet. | SFBK\_AUT.10 |
| Systemet ska ha möjlighet att reagera på upprepade felaktiga autentiseringsförsök, även sådana där den angivna identiteten förändras mellan försöken. | SFBK\_AUT.11 |
| Vid upprepade autentiseringsfel ska systemet automatiskt kunna införa en exponentiellt ökande fördröjning av nya autentiseringsförsök för subjektet alternativt kunna låsa berört subjekts säkerhetsattribut under en viss tid. | SFBK\_AUT.12 |
| Systemet ska inte uppge felorsak till subjekt vid autentiseringsfel. Syftar till att inte ge en attackerande part användbara upplysningar, t.ex. ”Angivet subjekt existerar inte” eller ”Felaktigt lösenord”. | SFBK\_AUT.13 |
| Systemet ska skydda en inloggad session så att den inte kan nyttjas av obehörig. | SFBK\_AUT.15 |
| Sessioner ska omfattas av tidsbegränsning. | SFBK\_AUT.16 |
| Systemet ska kunna notifiera om autentiseringsfel. Med notifiera menas att göra någon lämplig person (t.ex. operatör, administratör eller övervakningspersonal) uppmärksam på vad som skett. | SFBK\_AUT.17 |
| Stark autentisering ska tillämpas. Krav på stark autentisering finns i skrivelsen HKV 2007-03-26 12 830:65517 Krav för signalskyddssystem. Nyttjande av lösning med av MUST godkänt aktivt kort ska eftersträvas. | SFBK\_AUT.18 |
| Vid låsning eller revokering av säkerhetsattribut ska pågående sessioner för berört subjekt avslutas. Låsningen kan vara orsakad av t.ex. misslyckade autentiseringsförsök, att giltighetstiden för säkerhetsattribut gått ut eller manuell revokering av säkerhetsattribut. | SFBK\_AUT.19 |
| All aktivitet som systemet genomför för en användares räkning ska knytas till den genom stark autentisering fastställda identiteten. | SFBK\_AUT.20 |

Tabell 15 – Funktionella krav – Behörighetskontroll SFBK\_AUT

##### Åtkomst (SFBK\_ÅTK)

Subjekt ska endast ges åtkomst till objekt som de är behöriga till. För att förhindra obehörig åtkomst till information måste systemet kunna styra subjekts tillgång till objekt och endast tillåta subjekt att utföra de åtgärder som de uttryckligen tilldelats behörighet till.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Subjekts unika och genom autentisering fastställda identitet ska alltid användas vid åtkomstkontroll till objekt. | SFBK\_ÅTK.1 |
| Endast subjekt med tilldelad åtkomsträttighet ska ges åtkomst till objekt. | SFBK\_ÅTK.2 |
| Funktioner för administration av säkerhetsfunktionalitet ska förses med behörighetskontroll. | SFBK\_ÅTK.3 |
| Det ska vara möjligt att använda rollbaserad åtkomstkontroll. Åtkomsträttigheter ska kunna tilldelas via roll eller grupptillhörighet för att minska risken för ackumulering av behörigheter via individuellt tilldelade åtkomsträttigheter. | SFBK\_ÅTK.4 |

Tabell 16 – Funktionella krav – Behörighetskontroll SFBK\_ÅTK

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Subjekts unika och genom autentisering fastställda identitet ska alltid användas vid åtkomstkontroll till objekt. | SFBK\_ÅTK.1 |
| Endast subjekt med tilldelad åtkomsträttighet ska ges åtkomst till objekt. | SFBK\_ÅTK.2 |
| Funktioner för administration av säkerhetsfunktionalitet ska förses med behörighetskontroll. | SFBK\_ÅTK.3 |
| Det ska vara möjligt att använda rollbaserad åtkomstkontroll. Åtkomsträttigheter ska kunna tilldelas via roll eller grupptillhörighet för att minska risken för ackumulering av behörigheter via individuellt tilldelade åtkomsträttigheter. | SFBK\_ÅTK.4 |
| Det ska finnas möjlighet till märkning av ett objekt med skyddsvärde för styrning av åtkomst. | SFBK\_ÅTK.5 |
| Märkningen av objekt med skyddsvärde ska ha minst lika starkt integritetsskydd som alla andra säkerhetsattribut som styr åtkomst till objektet. | SFBK\_ÅTK.6 |

Tabell 17 – Funktionella krav – Behörighetskontroll SFBK\_ÅTK

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Subjekts unika och genom autentisering fastställda identitet ska alltid användas vid åtkomstkontroll till objekt. | SFBK\_ÅTK.1 |
| Endast subjekt med tilldelad åtkomsträttighet ska ges åtkomst till objekt. | SFBK\_ÅTK.2 |
| Funktioner för administration av säkerhetsfunktionalitet ska förses med behörighetskontroll. | SFBK\_ÅTK.3 |
| Det ska vara möjligt att använda rollbaserad åtkomstkontroll. Åtkomsträttigheter ska kunna tilldelas via roll eller grupptillhörighet för att minska risken för ackumulering av behörigheter via individuellt tilldelade åtkomsträttigheter. | SFBK\_ÅTK.4 |
| Det ska finnas möjlighet till märkning av ett objekt med skyddsvärde för styrning av åtkomst. | SFBK\_ÅTK.5 |
| Märkningen av objekt med skyddsvärde ska ha minst lika starkt integritetsskydd som alla andra säkerhetsattribut som styr åtkomst till objektet. | SFBK\_ÅTK.6 |
| Märkning av objekt med skyddsvärde ska användas vid styrning av åtkomst. | SFBK\_ÅTK.7 |

Tabell 18 – Funktionella krav – Behörighetskontroll SFBK\_ÅTK

##### Administration av behörighetskontroll (SFBK\_ADM)

Administration av behörighetskontroll ska se på ett säkert sätt. Nödvändig administration av säkerhetsfunktionen måste ske men får inte skapa möjligheter att kringgå behörighetskontrollen eller ske på ett sätt som försvårar eller förhindrar spårandet av subjekts aktiviteter i systemet.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Det ska gå att lägga till, ta bort och förändra vilka åtkomsträttigheter som subjekt har till systemets objekt. | SFBK\_ADM.1 |

Tabell 19 – Funktionella krav – Behörighetskontroll SFBK\_ADM

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Det ska gå att lägga till, ta bort och förändra vilka åtkomsträttigheter som subjekt har till systemets objekt. | SFBK\_ADM.1 |
| Systemet ska kunna åtkomstkontrollerna administration av säkerhetslogg, daglig drift och tilldelning av åtkomsträttigheter separat så att rollseparation av dessa sysslor medges. | SFBK\_ADM.2 |
| Det ska inte finnas någon roll eller tillgängligt subjekt som har åtkomst till samtliga objekt i systemet. Möjligheten att som ”superuser” få “åtkomst till allt” eller kunna undantas behörighetskontroll får alltså inte finnas. Om sådant subjekt finns måste det göras ”otillgängligt” t.ex. genom konfiguration. | SFBK\_ADM.3 |

Tabell 20 – Funktionella krav – Behörighetskontroll SFBK\_ADM

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Det ska gå att lägga till, ta bort och förändra vilka åtkomsträttigheter som subjekt har till systemets objekt. | SFBK\_ADM.1 |
| Systemet ska kunna åtkomstkontrollerna administration av säkerhetslogg, daglig drift och tilldelning av åtkomsträttigheter separat så att rollseparation av dessa sysslor medges. | SFBK\_ADM.2 |
| Det ska inte finnas något subjekt i systemet som har åtkomst till samtliga objekt i systemet. En ”superuser”-roll eller liknande får alltså inte existera i systemet. | SFBK\_ADM.4 |
| Systemet ska kunna åtkomstkontrollera identitetsadministration respektive tilldelning av åtkomsträttigheter separat. Detta ska medge tilldelning av dessa rättigheter till olika personer så att exempelvis den som administrerar åtkomsträttigheter och rolltillhörigheter inte kan skapa en ny identitet i systemet. | SFBK\_ADM.5 |
| Rollerna för administration av behörighetskontroll och administration av säkerhetslogg ska inte kunna tilldelas samma person. | SFBK\_ADM.6 |

Tabell 21 – Funktionella krav – Behörighetskontroll SFBK\_ADM

#### Säkerhetsloggning (SFSL)

För att skydda ett system eller en domän behövs spårbarhet på alla säkerhetsrelaterade händelser i systemet. Detta behövs för att kunna spåra godkända och icke godkända händelser i systemet. I vissa fall behöver systemet även garantera oavvislighet för de åtgärder och händelser som genomförts i systemet.

Möjlighet till analyser av loggar är en grundläggande funktion för att kunna följa händelser och åtgärder genom systemets olika delar.

##### Registrering (SFSL\_REG)

Säkerhetsrelaterade händelser ska registreras. För att säkerhetsloggar ska kunna användas för spårning av intrång och överskridandet av befogenheter måste en komplett och otvetydig logg föras över alla säkerhetsrelaterade händelser i systemet.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla händelser som är av betydelse för säkerheten i systemet ska registreras i säkerhetsloggen. | SFSL\_REG.1 |
| Datum och tid ska registreras för varje loggad händelse. Se SFGK\_TID. | SFSL\_REG.2 |
| Subjektets unika identitet ska registreras för varje loggad händelse. Avser såväl användare som övriga subjekt. Se SFBK\_UID. | SFSL\_REG.3 |
| Registrerade händelser ska minst omfatta: * all autentisering och försök till autentisering
* skapande av nya identiteter och roller
* förändringar av subjekts säkerhetsattribut som används för autentisering
* nekande av åtkomst till objekt, förutom då händelsen uppenbart inte har betydelse för säkerheten i systemet
 | SFSL\_REG.4 |

Tabell 22 – Funktionella krav – Säkerhetsloggning SFSL\_REG

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla händelser som är av betydelse för säkerheten i systemet ska registreras i säkerhetsloggen. | SFSL\_REG.1 |
| Datum och tid ska registreras för varje loggad händelse. Se SFGK\_TID. | SFSL\_REG.2 |
| Subjektets unika identitet ska registreras för varje loggad händelse. Avser såväl användare som övriga subjekt. Se SFBK\_UID. | SFSL\_REG.3 |
| Registrerade händelser ska minst omfatta: * all autentisering och försök till autentisering
* skapande av nya identiteter och roller
* förändringar av subjekts säkerhetsattribut som används för autentisering
* nekande av åtkomst till objekt, förutom då händelsen uppenbart inte har betydelse för säkerheten i systemet
 | SFSL\_REG.4 |
| Registrerade händelser ska minst omfatta: * alla förändringar av subjekts åtkomsträttigheter till objekt och funktioner
* alla förändringar av objekts säkerhetsattribut som styr åtkomst
* skapande av nya skyddsvärda objekt, t.ex. registerposter och handlingar
* alla sekretessklassificeringsbeslut, t.ex. vid upprättande av handling
* all åtkomst till skyddsvärda objekt
* all förändring eller radering av skyddsvärda objekt
* alla sökningar i register, diarier och liknande
* all export av information från systemet, inklusive utskrifter på papper
* angiven identitet vid autentisering
* varje upprättande av session
* varje avslutande av session
 | SFSL\_REG.5 |

Tabell 23 – Funktionella krav – Säkerhetsloggning SFSL\_REG

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla händelser som är av betydelse för säkerheten i systemet ska registreras i säkerhetsloggen. | SFSL\_REG.1 |
| Datum och tid ska registreras för varje loggad händelse. Se SFGK\_TID. | SFSL\_REG.2 |
| Subjektets unika identitet ska registreras för varje loggad händelse. Avser såväl användare som övriga subjekt. Se SFBK\_UID. | SFSL\_REG.3 |
| Registrerade händelser ska minst omfatta: * all autentisering och försök till autentisering
* skapande av nya identiteter och roller
* förändringar av subjekts säkerhetsattribut som används för autentisering
* nekande av åtkomst till objekt, förutom då händelsen uppenbart inte har betydelse för säkerheten i systemet
 | SFSL\_REG.4 |
| Registrerade händelser ska minst omfatta: * alla förändringar av subjekts åtkomsträttigheter till objekt och funktioner
* alla förändringar av objekts säkerhetsattribut som styr åtkomst
* skapande av nya skyddsvärda objekt, t.ex. registerposter och handlingar
* alla sekretessklassificeringsbeslut, t.ex. vid upprättande av handling
* all åtkomst till skyddsvärda objekt
* all förändring eller radering av skyddsvärda objekt
* alla sökningar i register, diarier och liknande
* all export av information från systemet, inklusive utskrifter på papper
* angiven identitet vid autentisering
* varje upprättande av session
* varje avslutande av session
 | SFSL\_REG.5 |
| Registrerade händelser ska minst omfatta:* konfigurationsförändringar i systemet
 | SFSL\_REG.6 |

Tabell 24 – Funktionella krav – Säkerhetsloggning SFSL\_REG

##### Oavvislighet (SFSL\_OAV)

Användare ska kunna göras individuellt ansvariga för sina åtgärder. För att användares åtgärder i systemet inte ska kunna döljas eller förnekas måste viktiga funktioner i systemet förses med oavvislighetsmekanismer.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla förändringar till placering i informationssäkerhetsklass samt förändringar gällande märkning av objekt med skyddsvärde ska bindas till användaren med en oavvislighetsmekanism. | SFSL\_OAV.1 |

Tabell 25 – Funktionella krav – Säkerhetsloggning SFSL\_OAV

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla förändringar till placering i informationssäkerhetsklass samt förändringar gällande märkning av objekt med skyddsvärde ska bindas till användaren med en oavvislighetsmekanism. | SFSL\_OAV.1 |
| Förändringar till mjukvarufiler och relevanta konfigurationer som omfattas av riktighetskontroll enligt SFSK\_INT.4 ska bindas till användaren med en oavvislighetsmekanism. | SFSL\_OAV.2 |
| Export av skyddsvärd information från systemet, inklusive utskrifter på papper, ska bindas till användaren med en oavvislighetsmekanism. | SFSL\_OAV.3 |

Tabell 26 – Funktionella krav – Säkerhetsloggning SFSL\_OAV

##### Skydd av säkerhetsloggar (SFSL\_SKY)

Säkerhetsloggar ska inte kunna förvanskas eller förstöras. För att garantera möjligheten till spårning behöver säkerhetsloggar skyddas mot avsiktliga eller oavsiktliga förändringar, förluster eller raderingar.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Händelseposter som registrerats i säkerhetsloggar ska inte kunna förändras. | SFSL\_SKY.1 |
| Händelseposter som registrerats i säkerhetsloggar får inte skrivas över eller tas bort innan arkivering är genomförd. Tillräckligt diskutrymme ska finnas för lagring av säkerhetsloggar. | SFSL\_SKY.2 |
| Säkerhetsloggen ska kunna säkerhetskopieras. | SFSL\_SKY.3 |

Tabell 27 – Funktionella krav – Säkerhetsloggning SFSL\_SKY

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Händelseposter som registrerats i säkerhetsloggar ska inte kunna förändras. | SFSL\_SKY.1 |
| Händelseposter som registrerats i säkerhetsloggar får inte skrivas över eller tas bort innan arkivering är genomförd. Tillräckligt diskutrymme ska finnas för lagring av säkerhetsloggar. | SFSL\_SKY.2 |
| Säkerhetsloggen ska kunna säkerhetskopieras. | SFSL\_SKY.3 |
| Säkerhetsloggar ska lagras åtskilda från driftsloggar. | SFSL\_SKY.4 |
| En reserverad yta för lagring av säkerhetsloggar ska finnas i systemet. | SFSL\_SKY.5 |
| Registrerade händelser får inte raderas eller skrivas över som en följd av fel på säkerhetsfunktionen eller att säkerhetsloggen är full. | SFSL\_SKY.6 |
| Säkerhetsfunktionen ska meddela behörig administratör vid följande händelser:* fel på säkerhetsfunktionen eller delar därutav
* ledigt utrymme för säkerhetsloggen underskrider ett konfigurerat tröskelvärde
* när problem i kommunikation inom loggsystem uppstår
* vid övergång till säkert tillstånd, se SFGK\_FEL
* om säkerhetsloggen skrivs över
 | SFSL\_SKY.7 |

Tabell 28 – Funktionella krav – Säkerhetsloggning SFSL\_SKY

##### Analys av säkerhetsloggar (SFSL\_ANA)

Säkerhetsloggar ska analyseras för att upptäcka intrång och missbruk. För att möjliggöra analyser av och slutsatser ur säkerhetsloggarna, måste dessa kunna granskas. En åtgärd lämnar spår i olika loggar, varför det är viktigt att kunna korrelera loggar vid en analys. Analyser kan behöva göras i systemmiljön eller i en extern miljö, loggarna måste därför kunna exporteras, helt eller delvis.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemet ska tillhandahålla funktioner för verktygsbaserad analys av registrerade händelser i säkerhetsloggen. Dessa kan realiseras i ett externt system, t.ex. ett system som också analyserar händelser från ett flertal andra IT-system. | SFSL\_ANA.1 |
| Den information som registreras om en händelse i säkerhetsloggen ska vara tillräcklig för att kunna förstå vad som hänt utan att behöva åtkomst till systemet eller information som lagras däri. Till exempel måste referenser till information vara verksamhetsanknutna och inte radnummer i en databas eller någon annan systemintern referens. | SFSL\_ANA.2 |
| Det ska vara möjligt att överföra säkerhetsloggar till externt IT-system. Formatet på överförda loggar ska vara väl specificerat. | SFSL\_ANA.3 |
| Säkerhetsloggar från flera olika komponenter ska kunna sammanföras och analyseras i analysverktyget. | SFSL\_ANA.4 |
| Analysverktyget ska kunna upptäcka kända attackmönster. | SFSL\_ANA.5 |
| Analysverktyget ska medge tillägg och anpassningar av attackmönster. | SFSL\_ANA.6 |
| Analysverktyget ska kunna detektera avvikelser i frekvens av registrerade händelser och händelsetyper i systemet. Denna analys avser identifiera händelser som aldrig eller sällan setts tidigare samt händelsetyper vars frekvens överskriver vissa förutbestämda tröskelvärden. | SFSL\_ANA.7 |
| Analysverktyget ska kunna sortera samt söka på alla definierade attribut för registrerade händelser. | SFSL\_ANA.8 |

Tabell 29 – Funktionella krav – Säkerhetsloggning SFSL\_ANA

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemet ska tillhandahålla funktioner för verktygsbaserad analys av registrerade händelser i säkerhetsloggen. Dessa kan realiseras i ett externt system, t.ex. ett system som också analyserar händelser från ett flertal andra IT-system. | SFSL\_ANA.1 |
| Den information som registreras om en händelse i säkerhetsloggen ska vara tillräcklig för att kunna förstå vad som hänt utan att behöva åtkomst till systemet eller information som lagras däri. Till exempel måste referenser till information vara verksamhetsanknutna och inte radnummer i en databas eller någon annan systemintern referens. | SFSL\_ANA.2 |
| Det ska vara möjligt att överföra säkerhetsloggar till externt IT-system. Formatet på överförda loggar ska vara väl specificerat. | SFSL\_ANA.3 |
| Säkerhetsloggar från flera olika komponenter ska kunna sammanföras och analyseras i analysverktyget. | SFSL\_ANA.4 |
| Analysverktyget ska kunna upptäcka kända attackmönster. | SFSL\_ANA.5 |
| Analysverktyget ska medge tillägg och anpassningar av attackmönster. | SFSL\_ANA.6 |
| Analysverktyget ska kunna detektera avvikelser i frekvens av registrerade händelser och händelsetyper i systemet. Denna analys avser identifiera händelser som aldrig eller sällan setts tidigare samt händelsetyper vars frekvens överskriver vissa förutbestämda tröskelvärden. | SFSL\_ANA.7 |
| Analysverktyget ska kunna sortera samt söka på alla definierade attribut för registrerade händelser. | SFSL\_ANA.8 |
| Alla registrerade händelser i systemet ska sammanföras och normaliseras innan analys. | SFSL\_ANA.9 |
| Automatiska återkommande analyser ska vara möjliga att konfigurera i analysverktyget. | SFSL\_ANA.10 |
| Analysverktyget ska kunna detektera avvikelser från identifierade användningsmönster och händelsefrekvenser. Denna analys kräver att systemet profileras för att identifiera ”normala” mönster och gränsvärden (”baselining”) så att avvikelser från detta kan upptäckas. | SFSL\_ANA.11 |

Tabell 30 – Funktionella krav – Säkerhetsloggning SFSL\_ANA

#### Intrångsskydd (SFIS)

För att skydda ett system från intrång behövs säkerhetsfunktioner som kan tillåta behörig kommunikation och samtidigt avvärja icke behörig kommunikation. Detta skydd består av externt perimeterskydd, skydd av kommunikation inom systemet samt skydd av informationsflöden in i eller ut ur systemet.

Säkerhetsfunktioner mot intrång behövs både i perimetern och inne i systemet. De behövs också på olika nivåer i informationsflödet. Exempelvis behövs både kontroll av enskilda paket i ett kommunikationsflöde och kontroll av vilken information som skickas in i eller ut ur systemet.

##### Härdning (SFIS\_HRD)

Systemets komponenter ska härdas mot intrång. För att minska risken för att ett angrepp leder till fullbordat intrång måste systemets olika delar konfigureras så att den attackyta de exponerar minimeras och så att utnyttjandet av sårbarheter försvåras.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Samtliga funktioner som inte stöder systemets primära syfte ska vara avstängda. | SFIS\_HDR.1 |
| Ingående delar i systemet ska konfigureras enligt tillverkarens rekommendationer för säker konfiguration. Om sådana inte finns ska av IT-säkerhetsbranschen vedertagna rekommendationer för säker konfiguration av komponenttypen användas. | SFIS\_HDR.2 |

Tabell 31 – Funktionella krav – Intrångsskydd SFIS\_HRD

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Samtliga funktioner som inte stöder systemets primära syfte ska vara avstängda. | SFIS\_HDR.1 |
| Ingående delar i systemet ska konfigureras enligt tillverkarens rekommendationer för säker konfiguration. Om sådana inte finns ska av IT-säkerhetsbranschen vedertagna rekommendationer för säker konfiguration av komponenttypen användas. | SFIS\_HDR.2 |
| Mjukvarutjänster ska förhindras från att kunna påverka varandra eller övriga systemet med hjälp av existerande funktioner för behörighetskontroll. | SFIS\_HDR.3 |
| Säkerhetskänsliga funktioner som inte används, t.ex. sådana som utgör tillgänglig attackyta, ska tas bort ur systemet. | SFIS\_HDR.4 |

Tabell 32 – Funktionella krav – Intrångsskydd SFIS\_HRD

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Samtliga funktioner som inte stöder systemets primära syfte ska vara avstängda. | SFIS\_HDR.1 |
| Ingående delar i systemet ska konfigureras enligt tillverkarens rekommendationer för säker konfiguration. Om sådana inte finns ska av IT-säkerhetsbranschen vedertagna rekommendationer för säker konfiguration av komponenttypen användas. | SFIS\_HDR.2 |
| Mjukvarutjänster ska förhindras från att kunna påverka varandra eller övriga systemet med hjälp av existerande funktioner för behörighetskontroll. | SFIS\_HDR.3 |
| Säkerhetskänsliga funktioner som inte används, t.ex. sådana som utgör tillgänglig attackyta, ska tas bort ur systemet. | SFIS\_HDR.4 |
| Funktioner för att försvåra utnyttjandet av potentiella sårbarheter i mjukvara ska implementeras i systemet. | SFIS\_HDR.5 |
| Alla mjukvarutjänster ska vara isolerade från varandra och övriga systemet genom upprätthållandet av en restriktiv resursåtkomstpolicy. | SFIS\_HDR.6 |
| Alla funktioner som inte används ska tas bort ur systemet. Detta innebär avlägsnande av mjukvarufiler och dylikt, som inte krävs för korrekt operation, från alla systemets komponenter. | SFIS\_HDR.7 |

Tabell 33 – Funktionella krav – Intrångsskydd SFIS\_HRD

##### Otillbörlig åtkomst och manipulation (SFIS\_INT)

Kommunikation ska skyddas mot otillbörlig åtkomst och manipulation. För att försvåra för en angripare som finns inuti systemet måste kommunikation mellan systemets olika delar skyddas så att motparten verifieras och informationen som utbyts inte kan förändras av tredje part.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| All säkerhetsrelaterad eller skyddsvärd information ska skyddas mot manipulation vid kommunikation mellan distribuerade komponenter i systemet. | SFIS\_INT.1 |

Tabell 34 – Funktionella krav – Intrångsskydd SFIS\_INT

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| All överförd information ska skyddas mot manipulation vid kommunikation mellan distribuerade komponenter i systemet. Undantag kan medges för kommunikation som krävs för att upprätta skyddad trafik.  | SFIS\_INT.2 |
| Alla uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (SFS 2009:400) ska vid kommunikation mellan distribuerade komponenter inom ett system skyddas mot obehörig åtkomst. | SFIS\_INT.3 |
| Vid kommunikation mellan distribuerade komponenter i systemet ska motparten autentiseras. Undantag kan medges för kommunikation som krävs för att göra autentiseringsmekanismerna åtkomliga. | SFIS\_INT.4 |

Tabell 35 – Funktionella krav – Intrångsskydd SFIS\_INT

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (SFS 2009:400) ska vid kommunikation mellan distribuerade komponenter inom ett system skyddas mot obehörig åtkomst. | SFIS\_INT.3 |
| Vid kommunikation mellan distribuerade komponenter i systemet ska motparten autentiseras. Undantag kan medges för kommunikation som krävs för att göra autentiseringsmekanismerna åtkomliga. | SFIS\_INT.4 |
| All information ska vid kommunikation mellan distribuerade komponenter inom systemet skyddas mot obehörig åtkomst och manipulation. Undantag kan medges för kommunikation som krävs för att upprätta skyddad trafik. | SFIS\_INT.5 |

Tabell 36 – Funktionella krav – Intrångsskydd SFIS\_INT

##### Kontroll på information som flödar in genom systemet (SFIS\_KIN)

Information som passerar in genom systemets gränsytor ska kontrolleras. För att upprätthålla integriteten i systemets funktioner måste all data som passerar in genom systemets gränsytor kontrolleras av en säkerhetsfunktion så att endast korrekt data accepteras för användning i systemet.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemets indatakontroller ska minst omfatta:* Godkända tecken
* Rimligheten hos datastorlekar
* Att uppgifter ligger inom rimliga gränsvärden
* Kodning av teckensträngar
* Kodning av datastrukturer
 | SFIS\_KIN.1 |
| Information ska inte accepteras av systemet utan att säkerhetsfunktionens kontroller används. | SFIS\_KIN.2 |
| De kontroller som görs ska vara på applikationsprotokollnivå. | SFIS\_KIN.3 |
| Information som ett subjekt får som gensvar vid fel eller nekande av åtkomst ska begränsas. | SFIS\_KIN.4 |

Tabell 37 – Funktionella krav – Intrångsskydd SFIS\_KIN

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemets indatakontroller ska minst omfatta:* Godkända tecken
* Rimligheten hos datastorlekar
* Att uppgifter ligger inom rimliga gränsvärden
* Kodning av teckensträngar
* Kodning av datastrukturer
 | SFIS\_KIN.1 |
| Information ska inte accepteras av systemet utan att säkerhetsfunktionens kontroller används. | SFIS\_KIN.2 |
| De kontroller som görs ska vara på applikationsprotokollnivå. | SFIS\_KIN.3 |
| Information som ett subjekt får som gensvar vid fel eller nekande av åtkomst ska begränsas. | SFIS\_KIN.4 |
| Applikationsprotokollet ska begränsas så att endast den delmängd som krävs för korrekt operation tillåts. | SFIS\_KIN.5 |
| Säkerhetsfunktionen ska kontrollera att applikationsprotokollets syntax följer en väl definierad grammatik. | SFIS\_KIN.6 |

Tabell 38 – Funktionella krav – Intrångsskydd SFIS\_KIN

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemets indatakontroller ska minst omfatta:* Godkända tecken
* Rimligheten hos datastorlekar
* Att uppgifter ligger inom rimliga gränsvärden
* Kodning av teckensträngar
* Kodning av datastrukturer
 | SFIS\_KIN.1 |
| Information ska inte accepteras av systemet utan att säkerhetsfunktionens kontroller används. | SFIS\_KIN.2 |
| Information som ett subjekt får som gensvar vid fel eller nekande av åtkomst ska begränsas. | SFIS\_KIN.4 |
| Applikationsprotokollet ska begränsas så att endast den delmängd som krävs för korrekt operation tillåts. | SFIS\_KIN.5 |
| Säkerhetsfunktionen ska kontrollera att applikationsprotokollets syntax följer en väl definierad grammatik. | SFIS\_KIN.6 |
| Information som passerar in i systemet ska kunna märkas med skyddsvärde. | SFIS\_KIN.7 |
| All information som passerar kontrollen ska verifieras i minsta beståndsdel och endast kontrollerad data får passera in i systemet. Observera att t.ex. dokument- och bildformat kan vara för komplicerade för att automatiskt kunna verifieras med en tillräcklig tillförlitlighet och därför måste konverteras till ett enklare format innan kontroll. | SFIS\_KIN.8 |

Tabell 39 – Funktionella krav – Intrångsskydd SFIS\_KIN

##### Kontroll på information som flödar ut ur systemet (SFIS\_KUT)

Information som flödar ut ur systemet ska kontrolleras. För att förhindra sekretessförlust måste all data som passerar ut genom systemets gränsytor kontrolleras så att endast avsedd data ska kunna passera ut ur systemet.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| All informationsöverföring från systemet ska kontrolleras och vara möjlig att begränsa. | SFIS\_KUT.1 |
| Minst följande kontroller ska ske på datakommunikationens innehåll: * Att data inte uppenbart är av för högt skyddsvärde
* Att data ligger inom rimliga gränsvärden, t.ex. storlek och frekvens
* Att data är av avsedd typ, t.ex. vad gäller format
 | SFIS\_KUT.2 |

Tabell 40 – Funktionella krav – Intrångsskydd SFIS\_KUT

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| All informationsöverföring från systemet ska kontrolleras och vara möjlig att begränsa. | SFIS\_KUT.1 |
| Minst följande kontroller ska ske på datakommunikationens innehåll: * Att data inte uppenbart är av för högt skyddsvärde
* Att data ligger inom rimliga gränsvärden, t.ex. storlek och frekvens
* Att data är av avsedd typ, t.ex. vad gäller format
 | SFIS\_KUT.2 |
| Applikationsprotokollet ska begränsas så att endast den delmängd som krävs för korrekt operation tillåts. | SFIS\_KUT.3 |
| Säkerhetsfunktionen ska kontrollera att datakommunikationens användning av applikationsprotokollet följer en väl definierad grammatik. | SFIS\_KUT.4 |
| Säkerhetsfunktionen ska kontrollera rimligheten hos mängden utgående data över tid. | SFIS\_KUT.5 |
| Befintlig märkning av data med skyddsvärde ska upprätthållas och tas hänsyn till vid utförsel. | SFIS\_KUT.6 |
| Ett meddelande ska bara kunna överföras till system som tillåts hantera uppgifter med lägst samma skyddsvärde som meddelandet. | SFIS\_KUT.7 |

Tabell 41 – Funktionella krav – Intrångsskydd SFIS\_KUT

#### Intrångsdetektering (SFID)

För att skydda ett system från intrång behövs säkerhetsfunktioner som kan upptäcka och varna för icke behörig kommunikation och dataförändringar. Detta skydd består av externt perimeterskydd, skydd av data inom systemet, samt skydd av informationsflöden in eller ut ur systemet. Skyddsåtgärderna behövs både i perimetern och inne i systemet, där intrångsdetekteringen tillsammans med intrångsskyddet utgör en del, och integritetskontroller av applikationer och data utgör en annan del.

Intrångsdetekteringen har också möjligheter att utnyttja delar av andra säkerhetsfunktioner, t.ex. säkerhetsfunktionen för säkerhetsloggning för att analysera händelser i systemet.

##### Datakällor ska vara tillgängliga för analys (SFID\_DAT)

Information från relevanta datakällor ska vara tillgängliga för analys. För att kunna upptäcka och varna för intrång och intrångsförsök behöver data om händelser i systemet kontinuerligt samlas in och göras tillgängliga för analys.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla säkerhetsloggar ska göras tillgängliga för analys. | SFID\_DAT.1 |
| Trafikdata från relevant kommunikation mellan komponenter i systemet ska göras tillgängligt för analys. | SFID\_DAT.2 |
| Trafikdata från all kommunikation över systemets gränsytor ska göras tillgängligt för analys. | SFID\_DAT.3 |
| Registrerade systemhändelser, t.ex. driftloggar, ska göras tillgängliga för analys. | SFID\_DAT.4 |
| Applikationshändelser ska göras tillgängliga för analys. | SFID\_DAT.5 |
| Alla händelseposter ska innehålla datum och tid. Se SFGK\_TID. | SFID\_DAT.6 |
| Alla händelseposter som kan härledas till ett subjekt ska innehålla detta subjekts unika identitet. | SFID\_DAT.7 |
| Information som gjorts tillgänglig för analys får inte skrivas över, ändras, eller förstöras innan analys genomförts. | SFID\_DAT.8 |

Tabell 42 – Funktionella krav – Intrångsdetektering SFID\_DAT

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Alla säkerhetsloggar ska göras tillgängliga för analys. | SFID\_DAT.1 |
| Trafikdata från relevant kommunikation mellan komponenter i systemet ska göras tillgängligt för analys. | SFID\_DAT.2 |
| Trafikdata från all kommunikation över systemets gränsytor ska göras tillgängligt för analys. | SFID\_DAT.3 |
| Registrerade systemhändelser, t.ex. driftloggar, ska göras tillgängliga för analys. | SFID\_DAT.4 |
| Applikationshändelser ska göras tillgängliga för analys. | SFID\_DAT.5 |
| Alla händelseposter ska innehålla datum och tid. Se SFGK\_TID. | SFID\_DAT.6 |
| Alla händelseposter som kan härledas till ett subjekt ska innehålla detta subjekts unika identitet. | SFID\_DAT.7 |
| Information som gjorts tillgänglig för analys ska överföras till en systemgemensam analys- och detekteringsfunktion. | SFID\_DAT.9 |
| Information som gjorts tillgänglig för analys får inte skrivas över, ändras, eller förstöras innan den överförts till analys- och detekteringsfunktionen. | SFID\_DAT.10 |

Tabell 43 – Funktionella krav – Intrångsdetektering SFID\_DAT

##### Intrång och missbruk ska upptäckas (SFID\_ANA)

Intrång och missbruk ska kunna upptäckas och spåras. För att kunna upptäcka pågående och redan genomförda intrång och intrångsförsök måste information om händelser i systemet kunna analyseras och slutsatser dras från korrelationer mellan olika datakällor.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Verktygsbaserad analys av allt tillgängliggjort data ska vara möjlig. | SFID\_ANA.1 |
| Analyserna ska kunna upptäcka kända attackmönster. | SFID\_ANA.2 |
| Analysfunktionen ska kunna kontinuerligt uppdatera signaturer för kända attackmönster. | SFID\_ANA.3 |
| Verktyget ska medge tillägg och anpassningar av attackmönster vid analys. | SFID\_ANA.4 |
| Analysfunktionen ska kunna detektera avvikelser i frekvens av händelser och händelsetyper i systemet. Denna analys avser identifiera händelser som aldrig eller sällan setts tidigare samt händelsetyper vars frekvens överskriver vissa förutbestämda tröskelvärden. | SFID\_ANA.5 |
| Händelsekedjor ska kunna skapas och följas i verktyget. Här avses att olika händelser ska kunna markeras som tillhörande samma ”incident” eller dylikt så att större händelseförlopp kan följas i verktyget. | SFID\_ANA.6 |
| Verktyget ska ge möjlighet att sortera och söka i händelser på alla definierade attribut. | SFID\_ANA.7 |
| All tillgängliggjort data ska i verktyget kunna presenteras i läsbar form. | SFID\_ANA.8 |

Tabell 44 – Funktionella krav – Intrångsdetektering SFID\_ANA

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Verktygsbaserad analys av allt tillgängliggjort data ska vara möjlig. | SFID\_ANA.1 |
| Analyserna ska kunna upptäcka kända attackmönster. | SFID\_ANA.2 |
| Analysfunktionen ska kunna kontinuerligt uppdatera signaturer för kända attackmönster. | SFID\_ANA.3 |
| Verktyget ska medge tillägg och anpassningar av attackmönster vid analys. | SFID\_ANA.4 |
| Analysfunktionen ska kunna detektera avvikelser i frekvens av händelser och händelsetyper i systemet. Denna analys avser identifiera händelser som aldrig eller sällan setts tidigare samt händelsetyper vars frekvens överskriver vissa förutbestämda tröskelvärden. | SFID\_ANA.5 |
| Händelsekedjor ska kunna skapas och följas i verktyget. Här avses att olika händelser ska kunna markeras som tillhörande samma ”incident” eller dylikt så att större händelseförlopp kan följas i verktyget. | SFID\_ANA.6 |
| Verktyget ska ge möjlighet att sortera och söka i händelser på alla definierade attribut. | SFID\_ANA.7 |
| All tillgängliggjort data ska i verktyget kunna presenteras i läsbar form. | SFID\_ANA.8 |
| All tillgängliggjort data ska sammanföras och analys ska göras på den samlade mängden. | SFID\_ANA.9 |
| Tillgängliggjort data ska normaliseras innan analys. | SFID\_ANA.10 |
| Automatiska analyser ska ske fortlöpande då nytt data tillgängliggörs. | SFID\_ANA.11 |
| Analyser som detekterar avvikelser från identifierade användningsmönster, dataflöden och händelsefrekvenser ska vara möjliga. Denna analys kräver att systemet profileras för att identifiera ”normala” mönster och gränsvärden (s.k. ”baselining”) så att avvikelser från detta kan upptäckas. | SFID\_ANA.12 |
| All tillgängliggjort data, analysresultat och åtgärder som vidtagits ska kunna överföras hel eller i delar till en extern miljö. | SFID\_ANA.13 |

Tabell 45 – Funktionella krav – Intrångsdetektering SFID\_ANA

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Verktygsbaserad analys av allt tillgängliggjort data ska vara möjlig. | SFID\_ANA.1 |
| Analyserna ska kunna upptäcka kända attackmönster. | SFID\_ANA.2 |
| Analysfunktionen ska kunna kontinuerligt uppdatera signaturer för kända attackmönster. | SFID\_ANA.3 |
| Verktyget ska medge tillägg och anpassningar av attackmönster vid analys. | SFID\_ANA.4 |
| Analysfunktionen ska kunna detektera avvikelser i frekvens av händelser och händelsetyper i systemet. Denna analys avser identifiera händelser som aldrig eller sällan setts tidigare samt händelsetyper vars frekvens överskriver vissa förutbestämda tröskelvärden. | SFID\_ANA.5 |
| Händelsekedjor ska kunna skapas och följas i verktyget. Här avses att olika händelser ska kunna markeras som tillhörande samma ”incident” eller dylikt så att större händelseförlopp kan följas i verktyget. | SFID\_ANA.6 |
| Verktyget ska ge möjlighet att sortera och söka i händelser på alla definierade attribut. | SFID\_ANA.7 |
| All tillgängliggjort data ska i verktyget kunna presenteras i läsbar form. | SFID\_ANA.8 |
| All tillgängliggjort data ska sammanföras och analys ska göras på den samlade mängden. | SFID\_ANA.9 |
| Tillgängliggjort data ska normaliseras innan analys. | SFID\_ANA.10 |
| Automatiska analyser ska ske fortlöpande då nytt data tillgängliggörs. | SFID\_ANA.11 |
| Analyser som detekterar avvikelser från identifierade användningsmönster, dataflöden och händelsefrekvenser ska vara möjliga. Denna analys kräver att systemet profileras för att identifiera ”normala” mönster och gränsvärden (s.k. ”baselining”) så att avvikelser från detta kan upptäckas. | SFID\_ANA.12 |
| All tillgängliggjort data, analysresultat och åtgärder som vidtagits ska kunna överföras hel eller i delar till en extern miljö. | SFID\_ANA.13 |
| Analyserna ska ske i annat system än det övervakade. Det andra systemet kan vara en avgränsad del av samma system som då i KSF-hänseende ska behandlas som ett eget system. | SFID\_ANA.14 |

Tabell 46 – Funktionella krav – Intrångsdetektering SFID\_ANA

#### Skydd mot skadlig kod (SFSK)

För att skydda ett system behövs säkerhetsfunktioner för att förhindra att systemet påverkas av skadlig kod, t.ex. virus, trojaner, maskar, logiska bomber och liknande. Skyddsåtgärderna behövs både i perimetern och inne i systemet, då hoten från skadlig kod varierar mellan olika typer av IT-system. Olika typer av skadlig kod attackerar också olika typer av gränsytor.

Varken försök att extrahera information eller angrepp avsedda att störa och förstöra den normala funktionen ska kunna genomföras.

##### Säkerhetsuppdateringar (SFSK\_UPD)

Funktioner för hantering av säkerhetsuppdateringar ska finnas. För att möjliggöra ett effektivt avhjälpande av kända säkerhetsbrister i systemet måste funktioner som informerar och stöder denna process finnas.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemet ska kunna rapportera exakt programvaruversion för alla i systemet ingående komponenter och dess mjukvarudelar. | SFSK\_UPD.1 |
| Systemet ska kunna uppdateras med säkerhetsuppdateringar. Införande av säkerhetsuppdateringar bör ske automatiskt så snart dessa finns tillgängliga. | SFSK\_UPD.2 |
| Systemet ska för alla uppdateringar kunna verifiera paketets integritet och säkerställa dess autenticitet innan de accepteras för införande. | SFSK\_UPD.3 |

Tabell 47 – Funktionella krav – Skydd mot skadlig kod SFSK\_UPD

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemet ska kunna rapportera exakt programvaruversion för alla i systemet ingående komponenter och dess mjukvarudelar. | SFSK\_UPD.1 |
| Systemet ska kunna uppdateras med säkerhetsuppdateringar. Införande av säkerhetsuppdateringar bör ske automatiskt så snart dessa finns tillgängliga. | SFSK\_UPD.2 |
| Systemet ska för alla uppdateringar kunna verifiera paketets integritet och säkerställa dess autenticitet innan de accepteras för införande. | SFSK\_UPD.3 |
| Systemet ska kunna kontrollera att installerad mjukvara överensstämmer med aktuella versioner från leverantören när behörig administratör påkallar. Detta för att följa upp utförda säkerhetsuppdateringar med kontroller av att rätt mjukvaruversion verkligen är driftsatt i systemet. | SFSK\_UPD.4 |

Tabell 48 – Funktionella krav – Skydd mot skadlig kod SFSK\_UPD

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemet ska kunna rapportera exakt programvaruversion för alla i systemet ingående komponenter och dess mjukvarudelar. | SFSK\_UPD.1 |
| Systemet ska kunna uppdateras med säkerhetsuppdateringar. Införande av säkerhetsuppdateringar bör ske automatiskt så snart dessa finns tillgängliga. | SFSK\_UPD.2 |
| Systemet ska för alla uppdateringar kunna verifiera paketets integritet och säkerställa dess autenticitet innan de accepteras för införande. | SFSK\_UPD.3 |
| Systemet ska innehålla funktioner för att automatiskt kontrollera att all installerad mjukvara överensstämmer med aktuella versioner från leverantören. Funktionen ska kunna göra återkommande kontroller av installerade mjukvarufiler för att kontrollera deras riktighet. | SFSK\_UPD.5 |

Tabell 49 – Funktionella krav – Skydd mot skadlig kod SFSK\_UPD

##### Riktighetskontroll av mjukvara och konfiguration (SFSK\_RIK)

Riktighetskontroll av mjukvara och konfigurationer ska vara möjlig. För att säkerställa systemets korrekthet och att dess funktioner arbetar som avsett måste kontroller kunna göras för att upptäcka icke godkända modifikationer av mjukvara eller konfiguration.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Integriteten hos alla mjukvarufiler och relevanta konfigurationer ska kunna verifieras med hjälp av en kryptografisk mekanism. Verifikation kan ske t.ex. mot installationsmedia. Med relevanta konfigurationer avses både säkerhetsrelaterade och systemrelaterade konfigurationer. | SFSK\_RIK.1 |
| Vid återställning av säkerhetskopior ska riktigheten hos kopiorna verifieras. | SFSK\_RIK.2 |

Tabell 50 – Funktionella krav – Skydd mot skadlig kod SFSK\_RIK

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Integriteten hos alla mjukvarufiler och relevanta konfigurationer ska kunna verifieras med hjälp av en kryptografisk mekanism. Verifikation kan ske t.ex. mot installationsmedia. Med relevanta konfigurationer avses både säkerhetsrelaterade och systemrelaterade konfigurationer. | SFSK\_RIK.1 |
| Vid återställning av säkerhetskopior ska riktigheten hos kopiorna verifieras. | SFSK\_RIK.2 |
| Riktigheten hos alla mjukvarufiler och relevanta konfigurationer ska verifieras automatiskt när behörig administratör påkallar. | SFSK\_RIK.3 |

Tabell 51 – Funktionella krav – Skydd mot skadlig kod SFSK\_RIK

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Integriteten hos alla mjukvarufiler och relevanta konfigurationer ska kunna verifieras med hjälp av en kryptografisk mekanism. Verifikation kan ske t.ex. mot installationsmedia. Med relevanta konfigurationer avses både säkerhetsrelaterade och systemrelaterade konfigurationer. | SFSK\_RIK.1 |
| Vid återställning av säkerhetskopior ska riktigheten hos kopiorna verifieras. | SFSK\_RIK.2 |
| Riktigheten hos alla mjukvarufiler och relevanta konfigurationer ska verifieras automatiskt när behörig administratör påkallar. | SFSK\_RIK.3 |
| Verifikationer av mjukvarufiler och konfigurationer ska ske löpande och endast sådana där riktigheten verifierats ska accepteras för användning. Med ”löpande” avses att verifikation bör ske vid varje nyttjande eller åtminstone varje gång objektet läses från lagringsmedium. | SFSK\_RIK.4 |

Tabell 52 – Funktionella krav – Skydd mot skadlig kod SFSK\_RIK

##### Exekvering av mjukvara (SFSK\_EXE)

Endast godkänd mjukvara ska kunna exekvera i systemet. För att förhindra manipulation av systemets mjukvarubaserade komponenter och deras funktion via införandet av skadlig kod måste kontroller av objekt med potentiellt exekverbart innehåll genomföras.

(GRUND/UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Kontroller ska finnas i alla systemets komponenter som kan påverkas av skadlig kod och ska omfatta alla typer av objekt med potentiellt exekverbart innehåll. | SFSK\_EXE.1 |
| Objekt ska kontrolleras innan de accepteras för användning. | SFSK\_EXE.2 |
| Vid detektering av potentiellt skadlig kod ska aktuell operation avbrytas och åtgärder automatiskt kunna vidtas. Att avbryta aktuell operation kan innebära att förhindra exekvering, lagring eller överföring av information. | SFSK\_EXE.3 |
| Vid detektering av potentiellt skadlig kod ska behörig administratör kunna notifieras. | SFSK\_EXE.4 |
| Säkerhetsfunktionen ska regelbundet kunna uppdatera kontrollmekanismerna för skyddet mot skadlig kod. | SFSK\_EXE.5 |
| System ska för alla uppdateringar av kontrollmekanismerna och dess styrande data verifiera paketets integritet och säkerställa att de kommer från betrodd utgivare. | SFSK\_EXE.6 |

Tabell 53 – Funktionella krav – Skydd mot skadlig kod SFSK\_EXE

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Kontroller ska finnas i alla systemets komponenter som kan påverkas av skadlig kod och ska omfatta alla typer av objekt med potentiellt exekverbart innehåll. | SFSK\_EXE.1 |
| Objekt ska kontrolleras innan de accepteras för användning. | SFSK\_EXE.2 |
| Vid detektering av potentiellt skadlig kod ska aktuell operation avbrytas och åtgärder automatiskt kunna vidtas. Att avbryta aktuell operation kan innebära att förhindra exekvering, lagring eller överföring av information. | SFSK\_EXE.3 |
| Vid detektering av potentiellt skadlig kod ska behörig administratör kunna notifieras. | SFSK\_EXE.4 |
| Säkerhetsfunktionen ska regelbundet kunna uppdatera kontrollmekanismerna för skyddet mot skadlig kod. | SFSK\_EXE.5 |
| System ska för alla uppdateringar av kontrollmekanismerna och dess styrande data verifiera paketets integritet och säkerställa att de kommer från betrodd utgivare. | SFSK\_EXE.6 |
| Endast sådan kod som tillhör systemet och vars riktighet verifierats ska accepteras för exekvering. Se SFSK\_RIK.4. | SFSK\_EXE.7 |

Tabell 54 – Funktionella krav – Skydd mot skadlig kod SFSK\_EXE

##### Spridning av skadlig kod (SFSK\_KUT)

Skadlig kod ska inte kunna spridas via systemet. För att inte systemet ska medverka till att sprida skadlig kod måste data som passerar ut genom systemets gränsytor kontrolleras.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| All information som förs ut ur systemet ska genomsökas efter potentiellt skadlig kod. | SFSK\_KUT.1 |
| Vid detektering av potentiellt skadlig kod ska aktuell överföring kunna avbrytas. | SFSK\_KUT.2 |

Tabell 55 – Funktionella krav – Skydd mot skadlig kod SFSK\_KUT

##### Införsel av skadlig kod (SFSK\_KIN)

Skadlig kod ska inte kunna föras in i systemet. För att systemet inte ska drabbas av skadlig kod måste all information som flödar in i systemet över systemets gränsytor kontrolleras.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| All information som förs in i systemet ska genomsökas efter potentiellt skadlig kod. Vid införsel av krypterat data ska kontrollen ske på dekrypterat data. Detta gäller såväl utbyte via nätverk som utbyte via flyttbara datamedia. | SFSK\_KIN.1 |
| Vid detektering av potentiellt skadlig kod ska aktuell överföring kunna avbrytas. | SFSK\_KIN.2 |

Tabell 56 – Funktionella krav – Skydd mot skadlig kod SFSK\_KIN

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| All information som förs in i systemet ska genomsökas efter potentiellt skadlig kod. Vid införsel av krypterat data ska kontrollen ske på dekrypterat data. Detta gäller såväl utbyte via nätverk som utbyte via flyttbara datamedia. | SFSK\_KIN.1 |
| Vid detektering av potentiellt skadlig kod ska aktuell överföring kunna avbrytas. | SFSK\_KIN.2 |
| Det ska gå att kontrollera och styra vilka objekttyper och dataformat som accepteras för införsel i systemet. | SFSK\_KIN.3 |
| Endast data i enkla och kontrollerbara format ska tillåtas passera in i systemet. Format på data som förs in i systemet behöver kunna kontrolleras, och i de fall där dataformatet är för komplext för att tekniskt kunna verifieras till en acceptabel nivå, måste data omvandlas till ett mindre komplext format. | SFSK\_KIN.4 |

Tabell 57 – Funktionella krav – Skydd mot skadlig kod SFSK\_KIN

#### Skydd mot röjande signaler, RÖS (SFRS)

För att skydda ett system från risken att röja information via de elektromagnetiska signaler som skapas i ett IT-system behöver systemet ha ett skydd mot dessa typer av läckage1. Skyddet kan realiseras av systemets komponenter, den lokal där systemet befinner sig eller båda i kombination.

##### Skydd mot RÖS (SFRS\_REG)

RÖS krav från gällande regelverk ska uppfyllas. IT-system som hanterar sekretessbelagda uppgifter som rör rikets säkerhet ska uppfylla Försvarsmaktens krav på skydd mot röjande signaler. IT-system som utbyter hemlig information med andra nationer eller mellanfolkliga organisationer, eller som på annat sätt omfattas av ytterligare hanteringskrav gällande RÖS, ska uppfylla de krav som följer av sådan hantering.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Försvarsmaktens krav på skydd mot röjande signaler ska gälla. Dessa återfinns i skrivelsen HKV 2006-03-24 10:755.65114 Beslut om krav på skydd mot röjande signaler (RÖS). | SFRS\_REG.1 |
| IT-system som hanterar hemlig information under avtal med annan nation eller mellanfolklig organisation, eller som på motsvarande sätt påförs säkerhetsskyddskrav, ska uppfylla motpartens krav på skydd mot röjande signaler. | SFRS\_REG.2 |

Tabell 58 – Funktionella krav – Skydd mot röjande signaler SFRS\_REG

#### Skydd mot obehörig avlyssning (SFOA)

Skyddsvärd information som sänds i elektroniska kommunikationsnät måste skyddas mot obehörig avlyssning, detta sker normalt genom nyttjande av godkända signalskyddssystem.

I elektroniska kommunikationsnät där godkänt signalskydd inte används för all kommunikation måste dess kablar förläggas på ett sätt som inte exponerar dem för inkoppling av utrustning för obehörig avlyssning.

##### Elektroniska kommunikationsnät (SFOA\_KBL)

Hemliga uppgifter i elektroniska kommunikationsnät ska skyddas. För att skydda mot avlyssning av hemliga uppgifter som sänds i kablar till elektroniska kommunikationsnät måste antingen godkänt signalskydd användas eller kablarna förläggas så att åtkomst försvåras och manipulation kan upptäckas.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/RESTRICTED eller högre sänds utan godkänt signalskydd ska förläggas inom inhägnat och bevakat område. | SFOA\_KBL.1 |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/RESTRICTED eller högre sänds utan godkänt signalskydd, ska * utgöras av optisk fiberkabel eller skärmad kopparkabel som förläggs inom sektionerat område

eller * utgöras av obruten optisk fiberkabel övervakad av godkänd säkerhetslarmad ändutrustning

Med sektionerat område menas område inom en tillträdesbegränsad byggnad avgränsat med särskilt system för passerkontroll dit endast behörig personal har tillträde. | SFOA\_KBL.2 |

Tabell 59 – Funktionella krav – Skydd mot obehörig avlyssning SFOA\_KBL

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/RESTRICTED eller högre sänds utan godkänt signalskydd ska förläggas inom inhägnat och bevakat område. | SFOA\_KBL.1 |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/RESTRICTED eller högre sänds utan godkänt signalskydd, ska * utgöras av optisk fiberkabel eller skärmad kopparkabel som förläggs inom sektionerat område

eller * utgöras av obruten optisk fiberkabel övervakad av godkänd säkerhetslarmad ändutrustning

Med sektionerat område menas område inom en tillträdesbegränsad byggnad avgränsat med särskilt system för passerkontroll dit endast behörig personal har tillträde. | SFOA\_KBL.2 |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre sänds utan godkänt signalskydd ska vara inspekterbara i hela sin sträckning alternativt övervakas av godkänd säkerhetslarmad ändutrustning. Med inspekterbar menas att kabeln är synlig och identifierbar, undantag kan medges om kabeln förlagts i eget pansarrör under kortare sträcka. | SFOA\_KBL.3 |

Tabell 60 – Funktionella krav – Skydd mot obehörig avlyssning SFOA\_KBL

 (HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/RESTRICTED eller högre sänds utan godkänt signalskydd ska förläggas inom inhägnat och bevakat område. | SFOA\_KBL.1 |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/RESTRICTED eller högre sänds utan godkänt signalskydd, ska * utgöras av optisk fiberkabel eller skärmad kopparkabel som förläggs inom sektionerat område

eller * utgöras av obruten optisk fiberkabel övervakad av godkänd säkerhetslarmad ändutrustning

Med sektionerat område menas område inom en tillträdesbegränsad byggnad avgränsat med särskilt system för passerkontroll dit endast behörig personal har tillträde. | SFOA\_KBL.2 |
| Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre sänds utan godkänt signalskydd ska utgöras av optisk fiberkabel, förläggas inom sektionerat område och vara inspekterbara i hela sin sträckning. | SFOA\_KBL.4 |

Tabell 61 – Funktionella krav – Skydd mot obehörig avlyssning SFOA\_KBL

### Assuranskrav

#### Systemets IT-säkerhetsspecifikation (SASS)

Syftet med denna klass är att få förtroende för att systemets IT-säkerhetsspecifikation (ITSS) är lämplig som specifikation för en systemevaluering. Detta sker genom att man granskar om ITSS på ett korrekt sätt tillämpat KSF säkerhetsmodell för att bestämma nivån på säkerhetskraven, att ITSS är tekniskt sund, icke motsägelsefull och har gjort en riktig tolkning av säkerhetskraven. Huruvida systemet kan uppfylla dessa säkerhetskrav tas om hand av alla andra systemassuranskrav.

##### ITSS Inledning (SASS\_INL)

Kravet omfattar att Inledning i ITSS ger en övergripande och korrekt beskrivning av systemet som omfattar följande:

* En referens som identifierar ITSS.
* En referens som identifierar systemet och som visar att ITSS på ett acceptabelt sätt representerar KSF-krav och andra kravdokument som systemet uppfyller.
* En systemöversikt som kortfattat beskriver systemets användning, arkitektur och säkerhetsfunktioner.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Utvecklaren ska tillhandahålla en *Inledning*. | SASS\_INL.D1 |
| Inledningen ska bestå av ITSS-referens, systemreferens och systemöversikt. | SASS\_INL.C1 |
| ITSS referensen ska entydigt identifiera ITSS. | SASS\_INL.C2 |
| IT-systemreferens ska entydigt identifiera systemet. | SASS\_INL.C3 |
| IT-systemreferens ska identifiera versionen på KSF-krav, samt vilken kravnivå, som ITSS anger att systemet ska uppfylla. | SASS\_INL.C4 |
| IT-systemreferens ska identifiera styrande dokument, internationella standarder samt andra säkerhetsrelaterade dokument som ITSS anger att systemet ska uppfylla. | SASS\_INL.C5 |
| IT-systemreferens ska visa vilka säkerhetskrav i den aktuella kravsamlingen systemet och dess komponenter ska uppfylla. | SASS\_INL.C6 |
| Systemöversikt ska beskriva systemets användning och säkerhetsmekanismer i systemet på en hög nivå. | SASS\_INL.C7 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SASS\_INL.E1 |

Tabell 62 – Assuranskrav – Systemets IT-säkerhetsspecifikation SASS\_INL

##### Systembeskrivning (SASS\_SYS)

Kravet gäller beskrivningen av systemet i ITSS. Den måste beskriva systemet på ett sådant sätt att man ur systembeskrivningen kan identifiera vilka KSF-krav som gäller, men också att man förstår hur systemet ska användas och hur det ska samverka med sin omgivning. Därmed måste förutsättningar för systemet, dess arkitektur, gränsytor och säkerhetsförmågor beskrivas.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en *Systembeskrivning*. | SASS\_SYS.D1 |
| Systembeskrivningen ska beskriva vilken information som hanteras i systemet samt konsekvenserna som skulle uppstå vid förlust av denna information. | SASS\_SYS.C1 |
| Systembeskrivningen ska beskriva systemets exponering. | SASS\_SYS.C2 |
| Beskrivning av information, konsekvens och systemets exponering ska ske med termer som KSF använder och som möjliggör att KSF-kraven kan baseras på dessa faktorer. | SASS\_SYS.C3 |
| Systembeskrivningen ska beskriva systemets tänkta användning, användare av systemet och information som ska lagras, bearbetas, överförs i eller utförs ut ur systemet. | SASS\_SYS.C4 |
| Systembeskrivningen ska beskriva systemets fysiska avgränsning, och alla externt åtkomliga gränsytor. | SASS\_SYS.C5 |
| Systembeskrivningen ska beskriva syfte och användningssätt för alla externt åtkomliga gränsytor. | SASS\_SYS.C6 |
| Systembeskrivningen ska beskriva systemets arkitektur och design och ska identifiera de komponenter som systemet består av. | SASS\_SYS.C7 |
| Systembeskrivningen ska tydligt identifiera de komponenter som är Säkerhetsrelevanta. | SASS\_SYS.C8 |
| Systembeskrivningen ska för alla externt åtkomliga gränsytor innehålla en beskrivning av vilka individuella komponenter som utgör gränsytan. | SASS\_SYS.C9 |
| Systembeskrivningen ska beskriva systemets säkerhetsförmågor och de säkerhetsfunktioner som systemet tillhandahåller. | SASS\_SYS.C10 |
| Beskrivningen av systemets förmågor ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS. | SASS\_SYS.C11 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SASS\_SYS.E1 |

Tabell 63 – Assuranskrav – Systemets IT-säkerhetsspecifikation SASS\_SYS

##### Sammanställning av säkerhetskrav (SASS\_KRV)

Detta krav omfattar sammanställningen av alla systemets säkerhetskrav som dokumenteras i ITSS sammanställning av säkerhetskrav. Dessa säkerhetskrav på systemet identifieras utifrån KSF säkerhetsmodell och andra analyser som måste genomföras. Den ska visa att KSF säkerhetsmodell tillämpats i enlighet med kapitlet Systembeskrivning och att alla funktionella säkerhetskrav och assuranskrav identifierats och dokumenterats. Den ska även visa inte bara att alla säkerhetskrav identifierats, utan även att all säkerhetskrav antingen grundas i KSF-modellen eller har identifierats genom andra analyser och kravställningar.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en *Sammanställning av säkerhetskrav*. | SASS\_KRV.D1 |
| Sammanställningen av säkerhetskrav ska identifiera de krav som kommer från KSF och de krav som är tillkommande säkerhetskrav. | SASS\_KRV.C1 |
| Sammanställningen av KSF-krav ska beskriva kravnivån för alla krav, alla därav gällande kravkomponenter, både de som uppfylls av systemet och de som ska uppfyllas av systemets omgivning. | SASS\_KRV.C2 |
| Sammanställningen av KSF-krav ska beskriva kravnivå för assuranskrav och alla gällande kravkomponenter. | SASS\_KRV.C3 |
| Tillkommande säkerhetskrav ska identifiera alla säkerhetsmål som identifierades under andra analyser som genomförts (så som obligatoriska verksamhetsanalys, säkerhetsanalys, hot-, risk- och sårbarhetsanalys, och författningsanalys). | SASS\_KRV.C4 |
| Beskrivningen av KSF-krav och tillkommande säkerhetskrav ska identifiera vilka krav som ska uppfyllas av systemet och vilka som ska uppfyllas av systemets omgivning. | SASS\_KRV.C5 |
| Beskrivningen av KSF-krav och tillkommande funktionella krav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS. | SASS\_KRV.C6 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SASS\_KRV.E1 |

Tabell 64 – Assuranskrav – Systemets IT-säkerhetsspecifikation SASS\_KRV

##### Säkerhetskrav på omgivningen (SASS\_OMG)

Detta krav ska visa att förutsättningarna för systemets miljö och de säkerhetskrav som ställs på systemets miljö dokumenterats. Vissa säkerhetskrav för systemet är tänkt att vara helt eller delvis uppfyllda genom att utnyttja systemets miljö. Dessa säkerhetskrav måste dokumenteras hur och till vilken grad de är tänkt att uppfyllas med hjälp av säkerhetskrav på omgivningen, med en detaljnivå motsvarande säkerhetskravens kravkomponenter.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla *Säkerhetskrav på omgivningen*. | SASS\_OMG.D1 |
| Säkerhetskraven på omgivningen ska identifiera och beskriva alla förutsättningar på systemets miljö som är nödvändiga för att systemet ska kunna uppfylla sina säkerhetskrav. | SASS\_OMG.C1 |
| Säkerhetskraven på omgivningen ska beskriva fysiska, administrativa samt organisatoriska åtgärder i systemets miljö som helt eller delvis uppfyller säkerhetskraven för systemets miljö. | SASS\_OMG.C2 |
| Säkerhetskraven på omgivningen ska identifiera säkerhetskrav och de funktionella säkerhetskrav för systemet som härrör från KSF och som helt eller delvis omhändertas av systemets miljö. | SASS\_OMG.C3 |
| Beskrivningen av säkerhetskraven för systemets miljö ska tydligt visa vilka krav som uppfylls av systemet och vilka som uppfylls av systemets miljö. | SASS\_OMG.C4 |
| Beskrivningen av säkerhetskraven för systemets miljö ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS. | SASS\_OMG.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SASS\_OMG.E1 |

Tabell 65 – Assuranskrav – Systemets IT-säkerhetsspecifikation SASS\_OMG

##### Tolkning av säkerhetskrav (SASS\_TOL)

Detta krav innebär att säkerhetskraven för systemet måste tolkas (nedbrytas) på ett systemspecifikt sätt så att de konkret kan omsätts av systemet. Då de funktionella säkerhetskraven i KSF är formulerade på en allmän nivå som gör dem generellt användbara, måste man precisera dessa säkerhetskrav för varje system för att kunna beskriva en sammanställd kravbild för systemet. Tolkningen av säkerhetskraven ska vara så entydig att den kan användas som grund för en systemdesign. Tolkningen av säkerhetskrav innebär att visa att KSF-kraven preciseras. Detta innebär att evalueraren måste verifiera om det preciserade KSF-kravet är mer strikt än det ursprungliga KSF-kravet.

Det kan vara så att vissa funktionella krav uppfylls till viss del av systemet och till viss del av dess omgivning, eventuell i samverkan mellan systemet och dess omgivning. De tolkade kraven måste vara så att de entydigt identifierar vilka krav som gäller för systemet och vilka krav som gäller dess omgivning.

Notera: Även assuranskraven måste tolkas, men denna tolkning påverkar inte systemets design och implementation, utan tolkningen sker fortlöpande under utvecklingsarbetet

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en *Tolkning av säkerhetskrav*. | SASS\_TOL.D1 |
| Tolkningen av säkerhetskrav ska beskriva tolkningen av alla säkerhetskrav för Systemet. | SASS\_TOL.C1 |
| Tolkningen av säkerhetskrav ska precisera funktionella säkerhetskrav så att de tolkade kraven är testbara och att en design kan verifieras mot tolkningen av kravet. | SASS\_TOL.C2 |
| Tolkningen av säkerhetskraven måste vara lika strikt eller mer strikt än de ursprungliga kraven, oavsett om kraven kommer från KSF eller är tillkommande säkerhetskrav. | SASS\_TOL.C3 |
| Beskrivningen av tolkningen av KSF-krav och tillkommande säkerhetskrav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS. | SASS\_TOL.C4 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SASS\_TOL.E1 |

Tabell 66 – Assuranskrav – Systemets IT-säkerhetsspecifikation SASS\_TOL

##### Uppfyllande av säkerhetskrav (SASS\_UPF)

Detta krav innebär att Uppfyllande av säkerhetskraven ska visa att alla tolkade krav som finns för systemet ska uppfyllas av identifierad säkerhetsfunktionalitet hos systemet. Alla krav måste vara uppfyllda och endast säkerhetsfunktionalitet som uppfyller kraven ska beskrivas. Säkerhetsfunktionalitet som uppfyller av säkerhetskraven måste överensstämma med Systembeskrivningen.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla *Uppfyllande av säkerhetskrav*. | SASS\_UPF.D1 |
| Uppfyllande av säkerhetskrav ska visa hur alla säkerhetskrav i kapitlet Tolkning av säkerhetskrav har uppfyllts av systemets säkerhetsfunktioner. | SASS\_UPF.C1 |
| Uppfyllande av säkerhetskrav ska visa att alla krav fullständigt uppfylls av Systemet. | SASS\_UPF.C2 |
| Uppfyllande av säkerhetskrav ska för varje krav visa att hela kravet har uppfyllts av systemet. | SASS\_UPF.C3 |
| Beskrivningen av uppfyllandet av säkerhetskrav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS. | SASS\_UPF.C4 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SASS\_UPF.E1 |

Tabell 67 – Assuranskrav – Systemets IT-säkerhetsspecifikation SASS\_UPF

#### Systemutvecklingens livscykel (SALC)

Syftet med denna klass är att få förtroende för systemutvecklarens hantering av systemet från design, via systemutveckling och integration till leverans. Den första förutsättning är att få förtroende för ursprunget hos systemet och dess komponenter, för att försäkra sig om att systemutvecklaren hanterar systemet och dess komponenter på ett sätt som gör att förändringar i dessa endast sker under kontrollerade former.

SALC skiljer på om systemet är under komponentutvecklarens, systemutvecklarens eller drift- och förvaltningsorganisationens kontroll.

Ansvaret och kontrollen av systemet anses följa nedanstående steg:

1. Under utvecklingen av systemet, dvs. innan systemet är klart och har levererats, är systemet under systemutvecklarens kontroll.
2. När systemet blivit klart och har levererats samt accepterats övergår ansvaret och därmed kontrollen till drift- och förvaltning.
3. Förvaltningen av systemet påbörjas, vilket normalt involverar både systemutvecklaren och drift- och förvaltning. Åtgärdade säkerhetsrelaterade brister (t.ex. systemuppdateringar) utvecklas och distribueras till drift- och förvaltning som måste ha processer för att kunna hantera systemuppdateringarna så som att verifiera och installera dem. SALC omfattar bara systemutvecklarens del av detta; kraven på drift och förvaltning av systemet beskrivs i klassen SAOP.

SALC omfattar inte utvecklingen av de komponenter som igår i systemet. I SALC ingår bara krav på hanteringen av komponenterna i systemets livscykel, då de lämnat komponentutvecklarens kontroll och är under systemutvecklarens kontroll, fram till dess systemet levererats till drift- och förvaltning.

Kraven på komponenternas utveckling ingår i komponentassuranskraven och verifieras genom godkännandeprocessen för komponenter. Detta gäller även i de fall då systemutvecklaren själv utvecklar en del av komponenterna.

##### Utvecklingssäkerhet (SALC\_UTV)

Detta krav behandlar säkerheten i utvecklings och integrationsmiljön. Kravet fokuserar på var komponenter och system kommer ifrån, säkerheten i utvecklingsmiljön, personell och fysisk säkerhet men också åtkomst till kritisk information som kan påverka förtroendet för systemet.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemutvecklingsdokumentation. | SALC\_UTV.D1 |
| Systemutvecklaren ska tillämpa systemutvecklingsdokumentationen. | SALC\_UTV.D2 |
| Systemutvecklaren ska tillhandahålla integrationsdokumentation. | SALC\_UTV.D3 |
| Systemutvecklaren ska tillhandahålla acceptanskriterier för komponenter som ska ingå i systemet. | SALC\_UTV.D4 |
| Systemutvecklingsdokumentationen ska beskriva fysiska, logiska, administrativa, personella och andra säkerhetsåtgärder som behövs för att säkerställa sekretess och riktighet hos design och implementation av systemet i utvecklingsmiljön. | SALC\_UTV.C1 |
| Systemutvecklingsdokumentationen ska visa att säkerhetsåtgärderna erbjuder ett riktighetsskydd av utvecklingsmiljön som minst är i paritet med det skydd som systemet ska erbjuda. | SALC\_UTV.C2 |
| Acceptanskriterierna ska beskriva tillräckliga kriterier för acceptans och verifiering av säkerhetsrelaterade komponenter som ingår i systemet. | SALC\_UTV.C3 |
| Integrationsdokumentationen ska identifiera ursprunget hos alla ingående säkerhetsrelaterade komponenter och dokumentera hur ursprunget identifierades och hur acceptanskontrollen skett. | SALC\_UTV.C4 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_UTV.E1 |
| Evalueraren ska verifiera att systemutvecklingsdokumentationens säkerhetsåtgärder tillämpas | SALC\_UTV.E2 |

Tabell 68 – Assuranskrav – Systemutvecklingens livscykel SALC\_UTV

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemutvecklingsdokumentation. | SALC\_UTV.D1 |
| Systemutvecklaren ska tillämpa systemutvecklingsdokumentationen. | SALC\_UTV.D2 |
| Systemutvecklaren ska tillhandahålla integrationsdokumentation. | SALC\_UTV.D3 |
| Systemutvecklaren ska tillhandahålla acceptanskriterier för komponenter som ska ingå i systemet. | SALC\_UTV.D4 |
| Systemutvecklingsdokumentationen ska beskriva fysiska, logiska, administrativa, personella och andra säkerhetsåtgärder som behövs för att säkerställa sekretess och riktighet hos design och implementation av systemet i utvecklingsmiljön. | SALC\_UTV.C1 |
| Systemutvecklingsdokumentationen ska visa att säkerhetsåtgärderna erbjuder ett riktighetsskydd av utvecklingsmiljön som minst är i paritet med det skydd som systemet ska erbjuda. | SALC\_UTV.C2 |
| Acceptanskriterierna ska beskriva tillräckliga kriterier för acceptans och verifiering av alla IT- komponenter som ingår i systemet. | SALC\_UTV.C5 |
| Integrationsdokumentationen ska identifiera ursprunget hos alla ingående komponenter och dokumentera hur ursprunget identifierades och hur acceptanskontrollen skett. | SALC\_UTV.C6 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_UTV.E1 |
| Evalueraren ska verifiera att systemutvecklingsdokumentationens säkerhetsåtgärder tillämpas | SALC\_UTV.E2 |

Tabell 69 – Assuranskrav – Systemutvecklingens livscykel SALC\_UTV

##### Konfigurationsledning (SALC\_KFG)

Detta krav omfattar rutiner för versions- och konfigurationshantering i syfte att undvika obehörig eller oavsiktlig ändring av konfigurationsstyrda komponenter.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet och en unik systemreferens. | SALC\_KFG.D1 |
| Systemutvecklaren ska använda ett konfigurationsledningssystem. | SALC\_KFG.D2 |
| Systemutvecklaren ska tillhandahålla dokumentation som beskriver konfigurationsledningssystemet. | SALC\_KFG.D3 |
| IT-systemet och de ingående komponenterna ska märkas med en unik referens. | SALC\_KFG.C1 |
| Dokumentationen som beskriver konfigurationsledning ska visa metoder för unik identifiering av konfigurationsstyrda IT- komponenter. | SALC\_KFG.C2 |
| Dokumentationen som beskriver konfigurationsledning ska visa hur konfigurationsledningen används i systemutvecklingen och systemutvecklarens förvaltning av systemet. | SALC\_KFG.C3 |
| Alla konfigurationsobjekt som ingår i systemet ska ligga under konfigurationsledningen. | SALC\_KFG.C4 |
| Dokumentationen som beskriver konfigurationsledning ska beskriva acceptansprocedurer för nya och uppdaterade konfigurationsobjekt. | SALC\_KFG.C5 |
| Dokumentationen som beskriver konfigurationsledning ska påvisa att de acceptansprocedurer som används tillhandahåller tillräcklig ändringshantering för alla konfigurationsobjekt. | SALC\_KFG.C6 |
| Underlag ska påvisa att systemet för konfigurationsledning bedrivs i enligheten med dokumentationen som beskriver konfigurationsledning. | SALC\_KFG.C7 |
| Underlag ska påvisa att alla ingående komponenter och dess delar, alla assuransunderlag, rapporter om eventuella säkerhetsbrister och annan dokumentation som beskriver leverantörens förvaltning av systemet är under kontroll av konfigurationsledningen. | SALC\_KFG.C8 |
| Konfigurationsledningssystemet ska tillhandahålla säkerhetsåtgärder för ändringshanteringar som säkerställer att alla ändringar genomförs på ett kontrollerat sätt och av behörig personal. | SALC\_KFG.C9 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_KFG.E1 |
| Evalueraren ska verifiera att konfigurationsledningssystemets säkerhetsåtgärder tillämpas. | SALC\_KFG.E2 |

Tabell 70 – Assuranskrav – Systemutvecklingens livscykel SALC\_KFG

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet och en unik systemreferens. | SALC\_KFG.D1 |
| Systemutvecklaren ska använda ett konfigurationsledningssystem. | SALC\_KFG.D2 |
| Systemutvecklaren ska tillhandahålla dokumentation som beskriver konfigurationsledningssystemet. | SALC\_KFG.D3 |
| IT-systemet och de ingående komponenterna ska märkas med en unik referens. | SALC\_KFG.C1 |
| Dokumentationen som beskriver konfigurationsledning ska visa metoder för unik identifiering av konfigurationsstyrda IT- komponenter. | SALC\_KFG.C2 |
| Dokumentationen som beskriver konfigurationsledning ska visa hur konfigurationsledningen används i systemutvecklingen och systemutvecklarens förvaltning av systemet. | SALC\_KFG.C3 |
| Alla konfigurationsobjekt som ingår i systemet ska ligga under konfigurationsledningen. | SALC\_KFG.C4 |
| Dokumentationen som beskriver konfigurationsledning ska beskriva acceptansprocedurer för nya och uppdaterade konfigurationsobjekt. | SALC\_KFG.C5 |
| Dokumentationen som beskriver konfigurationsledning ska påvisa att de acceptansprocedurer som används tillhandahåller tillräcklig ändringshantering för alla konfigurationsobjekt. | SALC\_KFG.C6 |
| Underlag ska påvisa att systemet för konfigurationsledning bedrivs i enligheten med dokumentationen som beskriver konfigurationsledning. | SALC\_KFG.C7 |
| Underlag ska påvisa att alla ingående komponenter och dess delar, alla assuransunderlag, rapporter om eventuella säkerhetsbrister och annan dokumentation som beskriver leverantörens förvaltning av systemet är under kontroll av konfigurationsledningen. | SALC\_KFG.C8 |
| Konfigurationsledningssystemet ska tillhandahålla säkerhetsåtgärder för ändringshanteringar som säkerställer att alla ändringar genomförs på ett kontrollerat sätt och av behörig personal. | SALC\_KFG.C9 |
| Konfigurationsledningssystemet ska innehålla tekniska funktioner för spårbarhet som säkerställer att alla ändringar entydigt går att spåra till den enskilda person som genomförde dem. | SALC\_KFG.C10 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_KFG.E1 |
| Evalueraren ska verifiera att konfigurationsledningssystemets säkerhetsåtgärder tillämpas. | SALC\_KFG.E2 |

Tabell 71 – Assuranskrav – Systemutvecklingens livscykel SALC\_KFG

##### Systemleverans (SALC\_LEV)

Detta krav omfattar rutiner för leveransprocessen för att undvika och upptäcka manipulation, sekretessförlust eller annan åverkan som kan leda till att systemets säkerhetsförmåga inte kan upprätthållas.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumentation som beskriver rutiner och mekanismer för IT system- och komponentleveranser. | SALC\_LEV.D1 |
| Systemutvecklaren ska använda leveransrutinerna. | SALC\_LEV.D2 |
| Leveransdokumentationen ska beskriva alla rutiner som är nödvändiga för att upprätthålla säkerheten för systemet under dess leverans till drift- och förvaltningsorganisationen. | SALC\_LEV.C1 |
| Leveransdokumentationen ska beskriva hur systemets riktighet skyddas under leveransen. | SALC\_LEV.C2 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_LEV.E1 |

Tabell 72 – Assuranskrav – Systemutvecklingens livscykel SALC\_LEV

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumentation som beskriver rutiner och mekanismer för IT system- och komponentleveranser. | SALC\_LEV.D1 |
| Systemutvecklaren ska använda leveransrutinerna. | SALC\_LEV.D2 |
| Leveransdokumentationen ska beskriva alla rutiner som är nödvändiga för att upprätthålla säkerheten för systemet under dess leverans till drift- och förvaltningsorganisationen. | SALC\_LEV.C1 |
| Leveransdokumentationen ska beskriva hur systemets riktighet skyddas under leveransen. | SALC\_LEV.C2 |
| Leveransdokumentationen ska beskriva hur systemets riktighet kan verifieras av mottagaren vid leverans samt vid godtycklig tidpunkt efter leverans. | SALC\_LEV.C3 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_LEV.E1 |

Tabell 73 – Assuranskrav – Systemutvecklingens livscykel SALC\_LEV

##### Livscykelmodell (SALC\_LCM)

Detta krav omfattar livscykelmodellen för systemutveckling. Grundläggande delar av en livscykelmodell är test och acceptansprocedurer i design, utveckling och leveransfaserna av ett system.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska upprätta en livscykelmodell som ska användas vid utveckling av systemet och systemutvecklarens förvaltning av systemet. | SALC\_LCM.D1 |
| Systemutvecklaren ska tillhandahålla dokumentation som beskriver livscykelmodellen. | SALC\_LCM.D2 |
| Livscykelmodellen ska omfatta systemutveckling och systemutvecklarens förvaltning av systemet. | SALC\_LCM.C1 |
| Livscykelmodellen ska tillhandahålla kontroll över systemutveckling och systemutvecklarens förvaltning av systemet. | SALC\_LCM.C2 |
| Livscykelmodellen ska beskriva det som behövs för att kunna bedöma säkerhetspåverkan av ändringar i systemet under systemets livscykel. | SALC\_LCM.C3 |
| Livscykelmodellen ska beskriva det som behövs för att kunna upprätthålla säkerhet i systemet under dess livscykel och systemutvecklarens förvaltning av systemet. | SALC\_LCM.C4 |
| Livscykelmodellen ska beskriva de delar av design-, drift- och förvaltningsdokumentationen som behövs för att upprätthålla säkerhet under systemets livscykel. | SALC\_LCM.C5 |
| Livscykelmodellen ska beskriva rutiner för verifiering av komponenternas lämplighet för användning i systemet. | SALC\_LCM.C6 |
| Livscykelmodellen ska beskriva acceptans- och releaseprocedurer för systemdesign och de ingående komponenterna. | SALC\_LCM.C7 |
| Livscykelmodellen ska beskriva hur kvalitetssäkring är integrerad i systemets livscykel. | SALC\_LCM.C8 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_LCM.E1 |
| Evalueraren ska verifiera att livscykelmodellen tillämpas. | SALC\_LCM.E2 |

Tabell 74 – Assuranskrav – Systemutvecklingens livscykel SALC\_LCM

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska upprätta en livscykelmodell som ska användas vid utveckling av systemet och systemutvecklarens förvaltning av systemet. | SALC\_LCM.D1 |
| Systemutvecklaren ska tillhandahålla dokumentation som beskriver livscykelmodellen. | SALC\_LCM.D2 |
| Livscykelmodellen ska omfatta systemutveckling och systemutvecklarens förvaltning av systemet. | SALC\_LCM.C1 |
| Livscykelmodellen ska tillhandahålla kontroll över systemutveckling och systemutvecklarens förvaltning av systemet. | SALC\_LCM.C2 |
| Livscykelmodellen ska beskriva det som behövs för att kunna bedöma säkerhetspåverkan av ändringar i systemet under systemets livscykel. | SALC\_LCM.C3 |
| Livscykelmodellen ska beskriva det som behövs för att kunna upprätthålla säkerhet i systemet under dess livscykel och systemutvecklarens förvaltning av systemet. | SALC\_LCM.C4 |
| Livscykelmodellen ska beskriva de delar av design-, drift- och förvaltningsdokumentationen som behövs för att upprätthålla säkerhet under systemets livscykel. | SALC\_LCM.C5 |
| Livscykelmodellen ska beskriva rutiner för verifiering av komponenternas lämplighet för användning i systemet. | SALC\_LCM.C6 |
| Livscykelmodellen ska beskriva acceptans- och releaseprocedurer för systemdesign och de ingående komponenterna. | SALC\_LCM.C7 |
| Livscykelmodellen ska beskriva hur kvalitetssäkring är integrerad i systemets livscykel. | SALC\_LCM.C8 |
| Livscykelmodellen ska beskriva hur processen för kvalitetssäkring möter liknande krav som ställs i standarden ISO 9001. | SALC\_LCM.C9 |
| Rutinerna för verifiering av komponenternas lämplighet för användning i systemet skall omfatta bedömmande av varje komponents säkerhetspåverkan på systemet. | SALC\_LCM.C10 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_LCM.E1 |
| Evalueraren ska verifiera att livscykelmodellen tillämpas. | SALC\_LCM.E2 |

Tabell 75 – Assuranskrav – Systemutvecklingens livscykel SALC\_LCM

##### Bristkorrigering (SALC\_BRK)

Detta krav omfattar hur upptäckta säkerhetsrelevanta brister i ett levererat system hanteras. Kraven omfattar hela livscykeln för en säkerhetsrelevant brist, hur och vart den rapporteras, vilken information som delges drift- och förvaltning, processen för hur bristen åtgärdas och hur systemet uppdateras.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet. | SALC\_BRK.D1 |
| Systemutvecklaren ska ha erforderliga avtal och processer för att få information kring säkerhetsrelevanta brister i systemet och ingående komponenter. | SALC\_BRK.D2 |
| Systemutvecklaren ska tillhandahålla drift- och förvaltningsdokumentation kring säkerhetsrelevanta brister i systemet. | SALC\_BRK.D3 |
| Systemutvecklaren ska etablera en process för rapportering av säkerhetsrelevanta brister i systemet. | SALC\_BRK.D4 |
| Drift- och förvaltningsdokumentation ska beskriva hur drift- och förvaltningsorganisationen kan rapportera misstänkta säkerhetsrelevanta brister i systemet. | SALC\_BRK.C1 |
| Drift- och förvaltningsdokumentation ska identifiera specifik kontaktyta för alla rapporter och förfrågningar angående säkerhetsrelevanta brister i systemet. | SALC\_BRK.C2 |
| Dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet ska beskriva metoder för säker leverans av information om brister och bristkorrigering samt säkerhetsuppdateringar till drift- och förvaltningsorganisationen. | SALC\_BRK.C3 |
| Dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet ska säkerställa att korrigerande åtgärder identifieras för alla kända säkerhetsrelevanta brister. | SALC\_BRK.C4 |
| Dokumentationen som beskriver hantering av säkerhetsrelevanta brister ska beskriva hur information kring brister och instruktioner om korrigerande åtgärder tillhandahålls drift- och förvaltningsorganisationen. | SALC\_BRK.C5 |
| Dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet ska säkerställa att alla kända säkerhetsrelevanta brister är åtgärdade och att säkerhetsuppdateringar är utfärdade till drift- och förvaltningsorganisationen. | SALC\_BRK.C6 |
| Dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet ska säkerställa att säkerhetsuppdateringar inte inför några nya säkerhetsrelaterade brister eller brister i funktionalitet. | SALC\_BRK.C7 |
| Dokumentationen som beskriver hantering av säkerhetsrelevanta brister ska beskriva procedurer som används för att spåra alla rapporterade säkerhetsrelevanta brister i systemet i varje release. | SALC\_BRK.C8 |
| Dokumentationen som beskriver hantering av säkerhetsrelevanta brister ska beskriva hur drift- och förvaltningsdokumentationen kategoriserar arten och effekten av varje säkerhetsrelevant brist samt statusen på korrigerande åtgärder. | SALC\_BRK.C9 |
| Dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet ska säkerställa att alla ingående komponenter är integrerade i processen för hantering av säkerhetsrelevanta brister i systemet. | SALC\_BRK.C10 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SALC\_BRK.E1 |

Tabell 76 – Assuranskrav – Systemutvecklingens livscykel SALC\_BRK

#### Arkitektur och design (SADE)

Syftet med denna klass är att uppnå förtroende för att systemets arkitektur och design är välbeskriven och icke motsägelsefull. Det ska även påvisas att arkitekturen och de enskilda komponenterna ger den säkerhetsfunktionalitet och assurans som anges i ITSS.

När säkerhetsarkitektur och design dokumenteras är det framförallt två egenskaper som är viktiga:

* Säkerhetsfunktionaliteten ska vara tydligt identifierad i arkitekturen och säkerhetsfunktioner ska vara specificerade.
* IT-systemet ska inte kunna användas på ett sådant sätt att säkerhetsfunktionalitet kan manipuleras eller kringgås.

##### Gränsytebeskrivning (SADE\_GRÄ)

Detta krav omfattar identifiering och beskrivning av systemets externa gränsytor för att förstå hur externa entiteter, så som användare eller andra system, interagerar med systemet samt vilka risker detta medför.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en beskrivning av systemets gränsytor. | SADE\_GRÄ.D1 |
| Beskrivningen av systemets gränsytor ska innehålla en analys av vilka externt åtkomliga gränsytor som är säkerhetsrelevanta och vilka som ej är säkerhetsrelevanta. | SADE\_GRÄ.C1 |
| Beskrivningen av systemets gränsytor ska innehållande en beskrivning av de ur säkerhetssynpunkt relevanta åtgärder som är associerade med varje säkerhetsrelevant gränsyta. | SADE\_GRÄ.C2 |
| Beskrivningen av systemets gränsytor ska innehålla en sammanfattning av de säkerhetsfunktioner som är associerade med respektive gränsyta. | SADE\_GRÄ.C3 |
| Beskrivningen av systemets gränsytor ska innehålla fullständig beskrivning för de interaktioner systemets alla externt åtkomliga gränsytor medger. | SADE\_GRÄ.C4 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SADE\_GRÄ.E1 |

Tabell 77 – Assuranskrav – Arkitektur och Design SADE\_GRÄ

##### Säkerhetsarkitektur (SADE\_ARK)

Detta krav innebär att systemutvecklaren måste tillhandahålla en beskrivning av systemets säkerhetsarkitektur som ska visa dels hur komponenter bidrar till systemets säkerhet och dels säkerhetskritiska beroenden mellan komponenter.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en beskrivning av systemets säkerhetsarkitektur. | SADE\_ARK.D1 |
| Systemutvecklaren ska designa och implementera systemet så att säkerhetsfunktioner ej kan kringgås. | SADE\_ARK.D2 |
| Beskrivningen av säkerhetsarkitekturen ska påvisa hur komponenterna tillsammans och deras interaktioner resulterar i systemets säkerhetsfunktionalitet. | SADE\_ARK.C1 |
| Säkerhetsarkitekturen ska för varje säkerhetsrelevant komponent identifiera vilka andra komponenter som den är beroende av och på vilket sätt den är beroende av de andra komponenterna. | SADE\_ARK.C2 |
| Beskrivningen av säkerhetsarkitekturen ska påvisa att systemarkitekturen förhindrar att säkerhetsfunktionalitet kan kringgås. | SADE\_ARK.C3 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SADE\_ARK.E1 |
| Evalueraren ska analysera underlaget och verifiera att det inte går att kringgå systemets säkerhetsfunktioner. | SADE\_ARK.E2 |

Tabell 78 – Assuranskrav – Arkitektur och Design SADE\_ARK

##### Dataflödesanalys (SADE\_DFA)

Dataflödesanalys behandlar identifieringen av de komponenter som lagrar och bearbetar kritiska data. Ett system har olika komponenter som hanterar en rad olika data, dock är all data inte är kritisk.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en dataflödesanalys för kritiska data i systemet. | SADE\_DFA.D1 |
| Dataflödesanalysen ska identifiera all kritisk data som lagras och bearbetas av systemet. | SADE\_DFA.C1 |
| Dataflödesanalysen ska innehålla en konsekvensnivåbedömning av det kritiska data som lagras eller bearbetas av komponenterna i systemet. | SADE\_DFA.C2 |
| Dataflödesanalysen ska dokumentera vilka komponenter som lagrar eller bearbetar kritiska data samt de komponenter som inte bearbetar eller lagrar kritiska data. | SADE\_DFA.C3 |
| Dataflödesanalysen ska dokumentera hur kritiska data överförs mellan komponenter i systemet. | SADE\_DFA.C4 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SADE\_DFA.E1 |

Tabell 79 – Assuranskrav – Arkitektur och Design SADE\_DFA

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en dataflödesanalys för kritiska data i systemet. | SADE\_DFA.D1 |
| Dataflödesanalysen ska identifiera all kritisk data som lagras och bearbetas av systemet. | SADE\_DFA.C1 |
| Dataflödesanalysen ska innehålla en konsekvensnivåbedömning av det kritiska data som lagras eller bearbetas av komponenterna i systemet. | SADE\_DFA.C2 |
| Dataflödesanalysen ska dokumentera vilka komponenter som lagrar eller bearbetar kritiska data samt de komponenter som inte bearbetar eller lagrar kritiska data. | SADE\_DFA.C3 |
| Dataflödesanalysen ska dokumentera hur kritiska data överförs mellan komponenter i systemet. | SADE\_DFA.C4 |
| Dataflödesanalysen ska betrakta all data som kritisk och därför fullständigt beskriva systemets samtliga dataflöden. | SADE\_DFA.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SADE\_DFA.E1 |

Tabell 80 – Assuranskrav – Arkitektur och Design SADE\_DFA

##### Designdokumentation (SADE\_DES)

Detta krav behandlar hur varje komponent bidrar med säkerhetsfunktionalitet till systemet samt hur komponenterna integreras i systemet.

(GRUND)

Inga krav på KSF-kravnivå Grund.

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla designdokumentation för systemet. | SADE\_DES.D1 |
| Designen ska beskriva systemets struktur i termer av dess ingående komponenter. | SADE\_DES.C1 |
| Designen ska identifiera alla komponenter som bidrar med säkerhetsfunktionalitet i systemet. | SADE\_DES.C2 |
| Designen ska beskriva varje komponents beteende i tillräcklig grad för att avgöra vilka komponenter som är säkerhetsrelevanta. | SADE\_DES.C3 |
| Designen ska innehålla en beskrivning av interaktionen mellan säkerhetsrelevanta komponenter samt mellan säkerhetsrelevanta och icke säkerhetsrelevanta komponenter. | SADE\_DES.C4 |
| Designdokumentationen ska påvisa att varje externt åtkomlig gränsyta som identifierats i gränsytebeskrivningen är associerad med minst en säkerhetsrelevant komponent. | SADE\_DES.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SADE\_DES.E1 |

Tabell 81 – Assuranskrav – Arkitektur och Design SADE\_DES

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla designdokumentation för systemet. | SADE\_DES.D1 |
| Designen ska beskriva systemets struktur i termer av dess ingående komponenter. | SADE\_DES.C1 |
| Designen ska identifiera alla komponenter som bidrar med säkerhetsfunktionalitet i systemet. | SADE\_DES.C2 |
| Designen ska beskriva varje komponents beteende i tillräcklig grad för att avgöra vilka komponenter som är säkerhetsrelevanta. | SADE\_DES.C3 |
| Designen ska innehålla en beskrivning av interaktionen mellan säkerhetsrelevanta komponenter samt mellan säkerhetsrelevanta och icke säkerhetsrelevanta komponenter. | SADE\_DES.C4 |
| Designdokumentationen ska påvisa att varje externt åtkomlig gränsyta som identifierats i gränsytebeskrivningen är associerad med minst en säkerhetsrelevant komponent. | SADE\_DES.C5 |
| Designdokumentationen skall visa fullständigt hur systemets komponenter och deras konfiguration ger systemet dess avsedda IT-säkerhetsförmågor. | SADE\_DES.C6 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SADE\_DES.E1 |

Tabell 82 – Assuranskrav – Arkitektur och Design SADE\_DES

#### Installation och drift (SOAP)

Syftet med denna klass är se till att systemet kan installeras, driftsättas, administreras och underhållas på ett säkert sätt.

Systemutvecklaren ansvarar för att tillhandahålla fullständig, tydlig och icke motsägelsefull drift- och förvaltningsdokumentation för systemet. Detta kan innebära att särskild drift- och förvaltningsdokumentation behöver tas fram för specifika konfigurationer eller miljöer. För att säkerställa att systemets säkerhet upprätthålls under systemets hela livscykel måste medföljande drift- och förvaltningsdokumentation innehålla tillräcklig information som krävs för att drift- och förvaltningspersonal ska kunna tillämpa sin del av felhanteringsprocessen då systemet är under drift- och förvaltningsorganisationens kontroll.

##### Installation och förberedelser (SAOP\_INS)

Detta krav ska säkerställa att systemet blir mottaget och installerat i sin driftmiljö på ett säkert sätt och som systemutvecklaren avsett.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet med dokumentation som beskriver förberedande åtgärder. | SAOP\_INS.D1 |
| De förberedande åtgärderna ska beskriva alla nödvändiga steg för att säkert kunna acceptera det levererade systemet i enlighet med systemutvecklarens leveransförfarande (SALC\_LEV). | SAOP\_INS.C1 |
| De förberedande åtgärderna ska beskriva alla nödvändiga steg för säker installation av systemet. | SAOP\_INS.C2 |
| De förberedande åtgärderna ska innehålla steg för att säkerställa att den driftmiljön stämmer med kraven på den driftmiljön som dokumenterats i ITSS (SASS\_OMG). | SAOP\_INS.C3 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SAOP\_INS.E1 |

Tabell 83 – Assuranskrav – Installation och Drift SAOP\_INS

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet med dokumentation som beskriver förberedande åtgärder. | SAOP\_INS.D1 |
| De förberedande åtgärderna ska beskriva alla nödvändiga steg för att säkert kunna acceptera det levererade systemet i enlighet med systemutvecklarens leveransförfarande (SALC\_LEV). | SAOP\_INS.C1 |
| De förberedande åtgärderna ska beskriva alla nödvändiga steg för säker installation av systemet. | SAOP\_INS.C2 |
| De förberedande åtgärderna ska innehålla steg för att säkerställa att den driftmiljön stämmer med kraven på den driftmiljön som dokumenterats i ITSS (SASS\_OMG). | SAOP\_INS.C3 |
| De förberedande åtgärderna ska innehålla steg för verifikation av korrekt installation. | SAOP\_INS.C4 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SAOP\_INS.E1 |
| Evalueraren ska tillämpa åtgärderna för att verifiera att systemet kan mottagas och installeras på ett säkert sätt genom att följa beskrivningen av dem. | SAOP\_INS.E2 |

Tabell 84 – Assuranskrav – Installation och Drift SAOP\_INS

##### Drift- och förvaltningsdokumentation (SAOP\_DOK)

Detta krav innebär att drift- och förvaltningsdokumentationen måste innehålla nödvändig information för att systemet ska kunna fungera på ett säkert sätt, i enlighet med systemutvecklarens intentioner.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla drift- och förvaltningsdokumentation. | SAOP\_DOK.D1 |
| Drift- och förvaltningsdokumentation ska för varje användarroll beskriva de användargränssnitt och säkerhetsfunktioner som är tillgängliga för användaren. | SAOP\_DOK.C1 |
| Drift- och förvaltningsdokumentation ska för varje användarroll beskriva hur tillgängliga användargränssnitt tillhandahållna av systemet ska användas på ett säkert sätt. Detta innefattar även samtliga säkerhetsparametrar som användaren kan förändra och med vilka värden de kan anses vara säkra. | SAOP\_DOK.C2 |
| Drift- och förvaltningsdokumentation ska för varje användarroll tydligt beskriva varje typ av säkerhetsrelevant aktivitet kopplat till de för användaren tillgängliga åtgärder som måste utföras omfattande drift och underhåll av säkerhetsfunktioner. | SAOP\_DOK.C3 |
| Drift- och förvaltningsdokumentation ska identifiera alla tänkbara driftsformer i systemet, inklusive drift efter inträffade fel om systemet hamnar i ett osäkert läge, dess konsekvenser och innebörd för fortsatt säker drift av systemet. | SAOP\_DOK.C4 |
| Drift- och förvaltningsdokumentation ska beskriva alla säkerhetskrav som systemet och dess komponenter har på miljön och andra komponenter som hanteras av den driftmiljön av respektive användarroll. | SAOP\_DOK.C5 |
| Drift- och förvaltningsdokumentation ska för respektive användarroll dokumentera alla tillåtna systemkonfigurationers kritiska beroenden mellan de olika komponenterna konfigurationer. | SAOP\_DOK.C6 |
| Drift- och förvaltningsdokumentation ska beskriva processer för rapportering av säkerhetsrelaterade händelser, t.ex. förlust av utrustning eller röjda säkerhetsattribut. | SAOP\_DOK.C7 |
| Drift- och förvaltningsdokumentation ska vara tydlig och rimlig för de tänkta användarna. | SAOP\_DOK.C8 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SAOP\_DOK.E1 |

Tabell 85 – Assuranskrav – Installation och Drift SAOP\_DOK

##### Bristkorrigering (SAOP\_BRK)

Detta krav ska säkerställa att drift- och förvaltningsorganisationen har förutsättningar att ta emot och implementera åtgärder för att hantera säkerhetsrelevanta brister i systemet.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla instruktioner som möjliggör för drift- och förvaltningsorganisationen att utföra bevakning av brister samt bristkorrigering. | SAOP\_BRK.D1 |
| Systemutvecklaren ska tillhandahålla nödvändiga kontakter till drift- och förvaltningsorganisationen för att bristkorrigeringsinformation för systemets komponenter ska kunna bevakas. | SAOP\_BRK.D2 |
| Instruktionerna ska innehålla processer för bevakning av källor till information om säkerhetsrelevanta brister i systemet och dess ingående komponenter. | SAOP\_BRK.C1 |
| Instruktionerna ska innehålla processer för hur säkerhetsrelevanta brister följs upp och korrigeras. | SAOP\_BRK.C2 |
| Instruktionerna ska beskriva hur uppföljning av säkerhetsrelevanta brister ska dokumenteras och visa att dokumentationen ska innehålla källor, analys, slutsats och rekommenderade åtgärder. | SAOP\_BRK.C3 |
| Instruktionerna ska innehålla processer för integrering av säkerhetsuppdateringar i systemet, inklusive avinstallering. | SAOP\_BRK.C4 |
| Instruktionerna ska innehålla metoder för säkert mottagande av bristinformation och bristkorrigering för systemet och dess ingående komponenter. | SAOP\_BRK.C5 |
| Instruktionerna ska innehålla rutiner för verifiering av riktighet och ursprung hos säkerhetuppdateringar innan de införs i systemet. | SAOP\_BRK.C6 |
| Livscykelmodellen ska innehålla rutiner för att bedöma om en åtgärdad brist i en komponent är säkerhetsrelevant och ska införas och hur den ska accepteras. | SAOP\_BRK.C7 |
| Instruktionerna ska innehålla rutiner för att testa säkerhetsuppdateringar för att säkerställa att säkerhetsfunktionaliteten fortfarande är intakt efter införandet. | SAOP\_BRK.C8 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SAOP\_BRK.E1 |

Tabell 86 – Assuranskrav – Installation och Drift SAOP\_BRK

#### Administrativa rutiner (SARU)

Syftet med denna klass är att verifiera att den dokumentation som systemutvecklaren producerat innehåller alla de administrativa rutiner som behövs för att systemets säkerhetsfunktioner ska kunna administreras på ett korrekt sätt. Detta behövs för att säkerställa att systemet används på det sätt som avsågs då systemutvecklaren designade och implementerade säkerhetsfunktionerna så att rätt IT-säkerhetsförmågor för systemet erhålls.

##### Åtkomsträttigheter (SARU\_ÅTK)

Detta krav skall se till att de administrativa rutinerna beskriver all nödvändig information som behövs för administrationen av användares rättigheter.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för tilldelning och återkallning av åtkomsträttigheter. | SARU\_ÅTK.D1 |
| Rutinerna ska beskriva hur åtkomsträttigheter tilldelas och återkallas. | SARU\_ÅTK.C1 |
| Rutinerna ska visa att åtkomsträttigheter som huvudregel tilldelas via roller (eller grupper) och beskriva de fall där särskilda åtkomsträttigheter kan behöva tilldelas direkt till subjekt. | SARU\_ÅTK.C2 |
| Rutinerna ska visa att användare eller subjekt endast tilldelas de roller (och grupper) som de är behöriga till och som är nödvändiga för deras tjänst. | SARU\_ÅTK.C3 |
| Rutinerna ska beskriva hur uppföljning av tilldelning sker för att säkerställa att systemets användare och subjekt har korrekt tilldelade roller och åtkomsträttigheter. | SARU\_ÅTK.C4 |
| Rutinerna ska beskriva att endast behörig driftspersonal ska tilldelas åtkomsträttigheter till administrativa funktioner för säkerhetsfunktioner, deras konfiguration och styrande data. | SARU\_ÅTK.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_ÅTK.E1 |

Tabell 87 – Assuranskrav – Administrativa rutiner SARU\_ÅTK

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för tilldelning och återkallning av åtkomsträttigheter. | SARU\_ÅTK.D1 |
| Rutinerna ska beskriva hur åtkomsträttigheter tilldelas och återkallas. | SARU\_ÅTK.C1 |
| Rutinerna ska visa att åtkomsträttigheter som huvudregel tilldelas via roller (eller grupper) och beskriva de fall där särskilda åtkomsträttigheter kan behöva tilldelas direkt till subjekt. | SARU\_ÅTK.C2 |
| Rutinerna ska visa att användare eller subjekt endast tilldelas de roller (och grupper) som de är behöriga till och som är nödvändiga för deras tjänst. | SARU\_ÅTK.C3 |
| Rutinerna ska beskriva hur uppföljning av tilldelning sker för att säkerställa att systemets användare och subjekt har korrekt tilldelade roller och åtkomsträttigheter. | SARU\_ÅTK.C4 |
| Rutinerna ska beskriva att endast behörig driftspersonal ska tilldelas åtkomsträttigheter till administrativa funktioner för säkerhetsfunktioner, deras konfiguration och styrande data. | SARU\_ÅTK.C5 |
| Rutinerna ska beskriva att en person inte får tilldelas åtkomsträttigheter till fler än en av följande funktioner eller roller: * administration av behörighetskontroll
* administration av säkerhetslogg
* övrig driftsadministration
 | SARU\_ÅTK.C6 |
| Rutinerna ska beskriva att en person som tilldelas åtkomsträttigheter till funktioner för administration av intrångsskydd inte samtidigt får ha tilldelad åtkomsträttighet att initiera informationsöverföringar som kontrolleras av intrångsskyddet. | SARU\_ÅTK.C7 |
| Rutinerna ska beskriva att endast den person som ansvarar för administration av säkerhetslogg får tilldelas åtkomsträttigheter till systemets säkerhetsloggar. | SARU\_ÅTK.C9 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_ÅTK.E1 |

Tabell 88 – Assuranskrav – Administrativa rutiner SARU\_ÅTK

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för tilldelning och återkallning av åtkomsträttigheter. | SARU\_ÅTK.D1 |
| Rutinerna ska beskriva hur åtkomsträttigheter tilldelas och återkallas. | SARU\_ÅTK.C1 |
| Rutinerna ska visa att åtkomsträttigheter som huvudregel tilldelas via roller (eller grupper) och beskriva de fall där särskilda åtkomsträttigheter kan behöva tilldelas direkt till subjekt. | SARU\_ÅTK.C2 |
| Rutinerna ska visa att användare eller subjekt endast tilldelas de roller (och grupper) som de är behöriga till och som är nödvändiga för deras tjänst. | SARU\_ÅTK.C3 |
| Rutinerna ska beskriva hur uppföljning av tilldelning sker för att säkerställa att systemets användare och subjekt har korrekt tilldelade roller och åtkomsträttigheter. | SARU\_ÅTK.C4 |
| Rutinerna ska beskriva att endast behörig driftspersonal ska tilldelas åtkomsträttigheter till administrativa funktioner för säkerhetsfunktioner, deras konfiguration och styrande data. | SARU\_ÅTK.C5 |
| Rutinerna ska beskriva att en person inte får tilldelas åtkomsträttigheter till fler än en av följande funktioner eller roller: * administration av behörighetskontroll
* administration av säkerhetslogg
* övrig driftsadministration
 | SARU\_ÅTK.C6 |
| Rutinerna ska beskriva att en person som tilldelas åtkomsträttigheter till funktioner för administration av intrångsskydd inte samtidigt får ha tilldelad åtkomsträttighet att initiera informationsöverföringar som kontrolleras av intrångsskyddet. | SARU\_ÅTK.C7 |
| Rutinerna ska beskriva att en person inte får tilldelas åtkomsträttigheter till fler än en av följande funktioner eller roller: * administration av identiteter och säkerhetsattribut för autentisering
* tilldelande av roller eller åtkomsträttigheter till användare eller subjekt
 | SARU\_ÅTK.C8 |
| Rutinerna ska beskriva att endast den person som ansvarar för administration av säkerhetslogg får tilldelas åtkomsträttigheter till systemets säkerhetsloggar. | SARU\_ÅTK.C9 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_ÅTK.E1 |

Tabell 89 – Assuranskrav – Administrativa rutiner SARU\_ÅTK

##### Säkerhetsattribut för autentisering (SARU\_ATT)

Detta krav skall se till att de administrativa rutinerna beskriver hur kvaliteten på säkerhetsattribut för autentisering ska kontrolleras.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för kontroll av kvaliteten på säkerhetsattribut som används för autentisering. | SARU\_ATT.D1 |
| Rutinerna ska beskriva en lägsta acceptabel kvalitetsnivå för lösenord som väljs av användare. | SARU\_ATT.C1 |
| Rutinerna ska beskriva att alla tilldelade lösenord genereras slumpmässigt och hur detta sker. | SARU\_ATT.C2 |
| Rutinerna ska visa att slumpmässigt genererade lösenord alltid består av minst 12 tecken. | SARU\_ATT.C3 |
| Rutinerna ska visa att lösenord byts vid driftsättning av systemet samt löpande med en bestämd intervall. | SARU\_ATT.C4 |
| Rutinerna ska beskriva att regelbunden uppdatering av revokeringslistor för certifikat ska ske. | SARU\_ATT.C5 |
| Rutinerna ska visa att varje användaridentitet i systemet kan bindas till en specifik person. | SARU\_ATT.C6 |
| Rutinerna ska beskriva hur uppföljning av systemets subjekt ska ske för att säkerställa att endast behöriga användares subjekt har giltiga säkerhetsattribut för autentisering. | SARU\_ATT.C7 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_ATT.E1 |

Tabell 90 – Assuranskrav – Administrativa rutiner SARU\_ATT

##### Upptäcka och spåra intrång och missbruk (SARU\_INT)

Detta krav skall se till att de administrativa rutinerna beskriver all nödvändig information som behövs för att upptäcka och spåra intrång och missbruk i systemet.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att upptäcka och spåra intrång och missbruk i systemet. | SARU\_INT.D1 |
| Rutinerna ska beskriva hur länge säkerhetsloggar ska sparas och visa att de överensstämmer med minst den tid som de gällande föreskrifterna påbjuder. | SARU\_INT.C1 |
| Rutinerna ska beskriva hur och med vilken regelbundenhet som verktygsbaserad analys av registrerade händelser i säkerhetsloggen ska ske. | SARU\_INT.C2 |
| Rutinerna ska beskriva hur analys av driftsrelaterade felhändelser i systemet ska ske och hur de ska dokumenteras. | SARU\_INT.C3 |
| Rutinerna ska beskriva hur analysresultat klassificeras och visa hur klassificeringsbeslutet samt beslut om åtgärd dokumenteras. | SARU\_INT.C4 |
| Rutinerna ska beskriva att analys och klassificering av analysresultat endast utförs av utbildad operatör. | SARU\_INT.C5 |
| Rutinerna ska beskriva hur rapporter om säkerhetsrelaterade händelser, t.ex. förlust av utrustning eller röjda säkerhetsattribut, ska hanteras och vilka åtgärder som ska vidtas. | SARU\_INT.C6 |
| Rutinerna ska beskriva hur alla identifierade incidenter ska utredas och rapporteras. | SARU\_INT.C7 |
| Rutinerna ska beskriva att analysresultat fortlöpande ska hanteras i enlighet med organisationens fastställda IT-säkerhetsplan. | SARU\_INT.C10 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_INT.E1 |

Tabell 91 – Assuranskrav – Administrativa rutiner SARU\_INT

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att upptäcka och spåra intrång och missbruk i systemet. | SARU\_INT.D1 |
| Rutinerna ska beskriva hur länge säkerhetsloggar ska sparas och visa att de överensstämmer med minst den tid som de gällande föreskrifterna påbjuder. | SARU\_INT.C1 |
| Rutinerna ska beskriva hur och med vilken regelbundenhet som verktygsbaserad analys av registrerade händelser i säkerhetsloggen ska ske. | SARU\_INT.C2 |
| Rutinerna ska beskriva hur analys av driftsrelaterade felhändelser i systemet ska ske och hur de ska dokumenteras. | SARU\_INT.C3 |
| Rutinerna ska beskriva hur analysresultat klassificeras och visa hur klassificeringsbeslutet samt beslut om åtgärd dokumenteras. | SARU\_INT.C4 |
| Rutinerna ska beskriva att analys och klassificering av analysresultat endast utförs av utbildad operatör. | SARU\_INT.C5 |
| Rutinerna ska beskriva hur rapporter om säkerhetsrelaterade händelser, t.ex. förlust av utrustning eller röjda säkerhetsattribut, ska hanteras och vilka åtgärder som ska vidtas. | SARU\_INT.C6 |
| Rutinerna ska beskriva hur alla identifierade incidenter ska utredas och rapporteras. | SARU\_INT.C7 |
| Rutinerna ska beskriva hur säkerhetskopiering av säkerhetsloggen ska ske regelbundet till annat lagringsmedium. | SARU\_INT.C8 |
| Rutinerna ska beskriva hur säkerhetskopian av säkerhetsloggen ska förvaras och visa att den ska förvaras fysiskt separerat från säkerhetsloggen. | SARU\_INT.C9 |
| Rutinerna ska beskriva att analysresultat fortlöpande ska hanteras i enlighet med organisationens fastställda IT-säkerhetsplan. | SARU\_INT.C10 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_INT.E1 |

Tabell 92 – Assuranskrav – Administrativa rutiner SARU\_INT

##### Säkerhetsuppdateringar (SARU\_UPD)

Detta krav skall se till att rutinerna beskriver all nödvändig information som behövs för att driftspersonal ska kunna utföra regelbundna säkerhetsuppdateringar av systemet.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att utföra regelbundna säkerhetsuppdateringar av systemet. | SARU\_UPD.D1 |
| Rutinerna ska innehålla detaljerade instruktioner för hantering av säkerhetsuppdateringar för samtlig mjukvara i systemet. | SARU\_UPD.C1 |
| Rutinerna ska beskriva processer för säker uppdatering av de säkerhetsfunktioner som är beroende av extern tillförsel av säkerhetsmekanismer eller styrande data. | SARU\_UPD.C2 |
| Rutinerna ska beskriva att uppdateringar av säkerhetsfunktioners kontrollmekanismer och deras styrande data ska verifieras med avseende på riktighet och ursprung innan de införs i systemet. | SARU\_UPD.C3 |
| Rutinerna ska visa att alla säkerhetsrelaterade brister i systemet ska korrigeras inom ett dokumenterat tidsintervall ifrån kännedomstillfället. | SARU\_UPD.C4 |
| Rutinerna ska beskriva att säkerhetsuppdateringar till någon av systemets komponenter ska införas så snart det är möjligt efter att dessa gjorts tillgängliga. | SARU\_UPD.C5 |
| Rutinerna ska beskriva att säkerhetsuppdateringars riktighet och ursprung ska verifieras innan de införs i systemet. | SARU\_UPD.C6 |
| Rutinerna ska beskriva hur efterlevnad av rutiner för bristhantering och säkerhetsuppdatering dokumenteras på sådant sätt att kontroller enkelt kan genomföras. | SARU\_UPD.C7 |
| Rutinerna ska beskriva hur riskminimerande åtgärder ska vidtas omedelbart efter att en säkerhetsrelaterad brist i systemet konstaterats. | SARU\_UPD.C8 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_UPD.E1 |

Tabell 93 – Assuranskrav – Administrativa rutiner SARU\_UPD

##### Konfigurationsstyrning (SARU\_KFG)

Detta krav skall se till att de administrativa rutinerna beskriver all nödvändig information som behövs för att driftspersonal ska kunna genomföra konfigurationsstyrning av systemet.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att genomföra konfigurationsstyrning av systemet. | SARU\_KFG.D1 |
| Rutinerna ska beskriva hur aktuell version och uppdateringsnivå för all mjukvara i systemet ska dokumenteras. | SARU\_KFG.C1 |
| Rutinerna ska beskriva hur aktuell konfiguration av alla komponenter i systemet ska vara dokumenterad. | SARU\_KFG.C2 |
| Rutinerna ska beskriva hur återkommande kontroller av att dokumentationen stämmer överens med systemet ska genomföras av driftspersonal. | SARU\_KFG.C3 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_KFG.E1 |

Tabell 94 – Assuranskrav – Administrativa rutiner SARU\_KFG

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att genomföra konfigurationsstyrning av systemet. | SARU\_KFG.D1 |
| Rutinerna ska beskriva hur aktuell version och uppdateringsnivå för all mjukvara i systemet ska dokumenteras. | SARU\_KFG.C1 |
| Rutinerna ska beskriva hur aktuell konfiguration av alla komponenter i systemet ska vara dokumenterad. | SARU\_KFG.C2 |
| Rutinerna ska beskriva hur återkommande kontroller av att dokumentationen stämmer överens med systemet ska genomföras av driftspersonal. | SARU\_KFG.C3 |
| Rutinerna ska beskriva hur alla förändringar till systemets mjukvara och konfiguration ska beslutas och dokumenteras innan de genomförs. | SARU\_KFG.C4 |
| Rutinerna ska beskriva hur ändringsbeslut dokumenteras och visa att de ska innehålla anledning, syfte och dokumentera exakt vilka förändringar som ska genomföras. | SARU\_KFG.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_KFG.E1 |

Tabell 95 – Assuranskrav – Administrativa rutiner SARU\_KFG

##### Säkerhetsutbildning av användare (SARU\_UTB)

Detta krav skall se till att systemutvecklare tillhandahåller utbildningsunderlag för alla olika användare av systemet.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla underlag för utbildning. | SARU\_UTB.D1 |
| Systemutvecklaren ska tillhandahålla rutiner för utbildning av användare. | SARU\_UTB.D2 |
| Utbildningsunderlag ska finnas för alla typer av användare av systemet. | SARU\_UTB.C1 |
| Utbildningsunderlag ska innefatta beskrivningar av hur användare ska rapportera säkerhetsrelaterade incidenter och vilka typer av incidenter som ska rapporteras. | SARU\_UTB.C2 |
| Utbildningsunderlag ska för varje typ av användare ange förutsättningar såsom förkunskaper. | SARU\_UTB.C3 |
| Rutinerna för utbildning ska ange hur utbildning genomförs och hur genomförd utbildning innebär att användare förstår användningen och sin roll i upprätthållandet av systemets säkerhet. | SARU\_UTB.C4 |
| Rutinerna för utbildning ska visa att användare ska ha genomgått utbildning med godkänt resultat innan de ges behörighet att använda systemet. | SARU\_UTB.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARU\_UTB.E1 |

Tabell 96 – Assuranskrav – Administrativa rutiner SARU\_UTB

#### Systemintegrationstest (SATS)

Syftet med denna klass är att verifiera att systemets säkerhetsfunktionalitet fungerar så som det är beskrivet i ITSS och att säkerhetsfunktioner inte kan kringgås. Verifiering sker genom systemutvecklarens funktionstest av säkerhetsfunktionaliteten (SATS\_FUN) samt av systemutvecklarens angripartester (SATS\_ANG). Hur ingående testerna måste vara ges av kravet på testtäckning (SATS\_TTK). Evaluerarens testning (SATS\_EVL) ger förtroende att systemet beter sig som specificerats och möter systemets funktionella säkerhetskrav genom kvalitetssäkring av systemutvecklarens testning samt kompletterande egna tester.

##### Testtäckning (SATS\_TTK)

Detta krav ska visa att det finns testfall som täcker systemets alla funktionella säkerhetskrav och ska därmed omfatta alla komponenter som bidrar till den totala säkerhetsfunktionaliteten.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en analys av testtäckningen för funktionella- och angripartester. | SATS\_TTK.D1 |
| Analysen skall innehålla en motivering till varför de genomförda funktionella testerna och angripartesterna anses tillräckliga och omfattar alla systemets säkerhetsfunktioner. | SATS\_TTK.C1 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_TTK.E1 |

Tabell 97 – Assuranskrav – Systemintegrationstest SATS\_TTK

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en analys av testtäckningen för funktionella- och angripartester. | SATS\_TTK.D1 |
| Analysen skall innehålla en motivering till varför de genomförda funktionella testerna och angripartesterna anses tillräckliga och omfattar alla systemets säkerhetsfunktioner. | SATS\_TTK.C1 |
| Analysen ska visa hur testfallen i testdokumentationen överensstämmer med de säkerhetsfunktionella kraven, säkerhetsfunktionerna och komponenterna så som de beskrivs i designdokumentationen. | SATS\_TTK.C2 |
| Analysen ska visa att alla kravkomponenter i alla funktionella säkerhetskrav testats. | SATS\_TTK.C3 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_TTK.E1 |

Tabell 98 – Assuranskrav – Systemintegrationstest SATS\_TTK

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en analys av testtäckningen för funktionella- och angripartester. | SATS\_TTK.D1 |
| Analysen skall innehålla en motivering till varför de genomförda funktionella testerna och angripartesterna anses tillräckliga och omfattar alla systemets säkerhetsfunktioner. | SATS\_TTK.C1 |
| Analysen ska visa hur testfallen i testdokumentationen överensstämmer med de säkerhetsfunktionella kraven, säkerhetsfunktionerna och komponenterna så som de beskrivs i designdokumentationen. | SATS\_TTK.C2 |
| Analysen ska visa att alla kravkomponenter i alla funktionella säkerhetskrav testats. | SATS\_TTK.C3 |
| Analysen ska visa att alla systemets säkerhetsfunktioner testats i alla de säkerhetsrelevanta komponenter som implementerar dem. | SATS\_TTK.C4 |
| Analysen ska visa att alla säkerhetsrelevanta komponenters säkerhetsfunktionalitet för systemet testats för komponentens alla gränsytor. | SATS\_TTK.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_TTK.E1 |

Tabell 99 – Assuranskrav – Systemintegrationstest SATS\_TTK

##### Funktionstester (SATS\_FUN)

Detta krav innebär att funktionstester av säkerhetsfunktionalitet ska genomföras av systemutvecklaren för att säkerställa att säkerhetsfunktionaliteten fungerar enligt specifikationen.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska testa systemet och producera testdokumentation. | SATS\_FUN.D1 |
| Systemutvecklaren ska tillhandahålla en testrapport. | SATS\_FUN.D2 |
| Testrapporten ska bestå av beskrivning av hur testerna genomförts, testernas övergripande resultat samt eventuella anmärkningar avseende utfallet av testerna. | SATS\_FUN.C1 |
| Testdokumentationen ska bestå av testplaner, förväntat resultat och faktiskt resultat. | SATS\_FUN.C2 |
| Testplanerna ska beskriva de tester som ska genomföras och scenariot för varje test. Beskrivningarna ska vara så detaljerade att testerna kan reproduceras. | SATS\_FUN.C3 |
| Det förväntade resultatet ska beskriva hur ett framgångsrikt testresultat kan identifieras och skiljas från ett icke framgångsrikt testresultat. Detta ska ske för varje testfall. | SATS\_FUN.C4 |
| Det faktiska testresultatet ska överensstämma med det förväntade testresultatet. | SATS\_FUN.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_FUN.E1 |

Tabell 100 – Assuranskrav – Systemintegrationstest SATS\_FUN

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska testa systemet och producera testdokumentation. | SATS\_FUN.D1 |
| Systemutvecklaren ska tillhandahålla en testrapport. | SATS\_FUN.D2 |
| Systemutvecklaren ska tillhandahålla testdokumentation. | SATS\_FUN.D3 |
| Testrapporten ska bestå av beskrivning av hur testerna genomförts, testernas övergripande resultat samt eventuella anmärkningar avseende utfallet av testerna. | SATS\_FUN.C1 |
| Testdokumentationen ska bestå av testplaner, förväntat resultat och faktiskt resultat. | SATS\_FUN.C2 |
| Testplanerna ska beskriva de tester som ska genomföras och scenariot för varje test. Beskrivningarna ska vara så detaljerade att testerna kan reproduceras. | SATS\_FUN.C3 |
| Det förväntade resultatet ska beskriva hur ett framgångsrikt testresultat kan identifieras och skiljas från ett icke framgångsrikt testresultat. Detta ska ske för varje testfall. | SATS\_FUN.C4 |
| Det faktiska testresultatet ska överensstämma med det förväntade testresultatet. | SATS\_FUN.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_FUN.E1 |

Tabell 101 – Assuranskrav – Systemintegrationstest SATS\_FUN

##### Angripartester (SATS\_ANG)

Detta krav innebär att tester av säkerhetsfunktionalitet ska genomföras av systemutvecklaren för att säkerställa att säkerhetsfunktionaliteten i systemet inte går att otillbörligt påverka eller kringgå.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska testa systemet och producera testdokumentation. | SATS\_ANG.D1 |
| Systemutvecklaren ska tillhandahålla en testrapport. | SATS\_ANG.D2 |
| Testrapporten ska bestå av beskrivning av hur testerna genomförts, testernas övergripande resultat samt eventuella anmärkningar avseende utfallet av testerna. | SATS\_ANG.C1 |
| Testdokumentationen ska bestå av testplaner, förväntat resultat och faktiskt resultat. | SATS\_ANG.C2 |
| Testplanerna ska beskriva de tester som ska genomföras och scenariot för varje test. Beskrivningarna ska vara så detaljerade att testerna kan reproduceras. | SATS\_ANG.C3 |
| Det förväntade resultatet ska beskriva hur ett framgångsrikt testresultat kan identifieras och skiljas från ett icke framgångsrikt testresultat. Detta ska ske för varje testfall. | SATS\_ANG.C4 |
| Det faktiska testresultatet ska överensstämma med det förväntade testresultatet. | SATS\_ANG.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_ANG.E1 |

Tabell 102 – Assuranskrav – Systemintegrationstest SATS\_ANG

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska testa systemet och producera testdokumentation. | SATS\_ANG.D1 |
| Systemutvecklaren ska tillhandahålla en testrapport. | SATS\_ANG.D2 |
| Systemutvecklaren ska tillhandahålla testdokumentation. | SATS\_ANG.D3 |
| Testrapporten ska bestå av beskrivning av hur testerna genomförts, testernas övergripande resultat samt eventuella anmärkningar avseende utfallet av testerna. | SATS\_ANG.C1 |
| Testdokumentationen ska bestå av testplaner, förväntat resultat och faktiskt resultat. | SATS\_ANG.C2 |
| Testplanerna ska beskriva de tester som ska genomföras och scenariot för varje test. Beskrivningarna ska vara så detaljerade att testerna kan reproduceras. | SATS\_ANG.C3 |
| Det förväntade resultatet ska beskriva hur ett framgångsrikt testresultat kan identifieras och skiljas från ett icke framgångsrikt testresultat. Detta ska ske för varje testfall. | SATS\_ANG.C4 |
| Det faktiska testresultatet ska överensstämma med det förväntade testresultatet. | SATS\_ANG.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_ANG.E1 |

Tabell 103 – Assuranskrav – Systemintegrationstest SATS\_ANG

##### Evaluerarens testning (SATS\_EVL)

Detta krav omfattar den testning som evalueraren ska genomföra för ett system.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet för testning. | SATS\_EVL.D1 |
| Systemutvecklaren ska tillhandahålla motsvarande uppsättning testresurser som de som systemutvecklaren använde vid den funktionella testningen. | SATS\_EVL.D2 |
| IT-systemet ska vara i testbart skick. | SATS\_EVL.C1 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_EVL.E1 |
| Evalueraren ska, om denne finner det nödvändigt, upprepa ett representativt antal av systemutvecklarens tester och bekräfta att systemutvecklarens testresultat för dessa testfall. | SATS\_EVL.E2 |

Tabell 104 – Assuranskrav – Systemintegrationstest SATS\_EVL

(UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet för testning. | SATS\_EVL.D1 |
| Systemutvecklaren ska tillhandahålla motsvarande uppsättning testresurser som de som systemutvecklaren använde vid den funktionella testningen. | SATS\_EVL.D2 |
| IT-systemet ska vara i testbart skick. | SATS\_EVL.C1 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SATS\_EVL.E1 |
| Evalueraren ska, om denne finner det nödvändigt, upprepa ett representativt antal av systemutvecklarens tester och bekräfta att systemutvecklarens testresultat för dessa testfall. | SATS\_EVL.E2 |
| Evalueraren ska analysera systemutvecklarens testfall och komplettera dessa testfall med egna testfall. | SATS\_EVL.E3 |
| Evalueraren ska genomföra de egna testfallen, dokumentera resultatet och bekräfta att systemet fungerar enligt specifikation. | SATS\_EVL.E4 |

Tabell 105 – Assuranskrav – Systemintegrationstest SATS\_EVL

#### Riskanalys och sårbarhetsanalys (SARA)

Syftet med denna klass är att identifiera och värdera eventuella avvikelser, sårbarheter och kvarstående risker för att kunna avdöma och hantera, alternativt acceptera dem. Systemutvecklaren ska identifiera alla avvikelser som därefter ska verifieras och analyseras av evalueraren. Evalueraren ska dessutom identifiera och värdera sårbarheter som kan finnas i den faktiska användningen av systemet.

Ett system kan innehålla sårbarheter antingen genom sin konstruktion (design och arkitektur) eller genom sin användning (t.ex. genom risk för felaktig konfigurering). Det kan även finnas assuransbrister som måste identifieras vilka skulle kunna leda till ökad risk för sårbarheter. Exempel på assuransbrister är om vissa komponenter förlitar sig på andra komponenter vars säkerhet inte är verifierad eller där en viss godkänd komponent används i annan konfiguration än den som verifierats.

##### Avvikelseanalys (SARA\_AVV)

Kravet innebär att säkerhetsrelevanta avvikelser från godkänd användning av komponenter identifieras och beskrivs på ett sådant sätt att systemutvecklaren kan kompensera bristen med egna åtgärder som t.ex. analys av skillnaden mellan certifierad konfiguration och faktisk konfiguration.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla en avvikelseanalys. | SARA\_AVV.D1 |
| Avvikelseanalysen ska omfatta alla avvikelser från den godkända konfigurationen för alla systemets säkerhetsrelevanta komponenter. | SARA\_AVV.C1 |
| Avvikelseanalysen ska omfatta alla avvikelser från den i godkännandet avsedda användningen av alla systemets säkerhetsrelevanta komponenter. | SARA\_AVV.C2 |
| Avvikelseanalysen ska omfatta alla avvikelser från de i godkännandet beskrivna antaganden om systemets utformning för alla systemets säkerhetsrelevanta komponenter. | SARA\_AVV.C3 |
| Avvikelseanalysen ska för varje avvikelse visa vilken inverkan den har och hur den har hanterats. | SARA\_AVV.C4 |
| Avvikelseanalysen ska visa att åtgärderna som vidtagits för att hantera avvikelserna är effektiva. | SARA\_AVV.C5 |
| Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation. | SARA\_AVV.E1 |

Tabell 106 – Assuranskrav – Riskanalys och Sårbarhetsanalys SARA\_AVV

##### Sårbarhetsanalys (SARA\_SBH)

Kravet innebär att en sårbarhetsanalys ska genomföras för att identifiera eventuella sårbarheter i systemet som skulle kunna utnyttjas i systemets driftmiljö.

(GRUND)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet för testning. | SARA\_SBH.D1 |
| IT-systemet ska vara i testbart skick. | SARA\_SBH.C1 |
| Evalueraren ska verifiera att informationen i leverantörens dokumentation är tillräcklig för att utföra en grundlig sårbarhetsanalys av hela systemet. | SARA\_SBH.E1 |
| Evalueraren ska använda tillgängliga källor för att komplettera leverantörens dokumentation, t.ex. publik sårbarhetsinformation. | SARA\_SBH.E2 |
| Evalueraren 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. | SARA\_SBH.E3 |
| Evalueraren ska genomföra en oberoende sårbarhetsanalys av systemet baserad på arkitektur- och designinformationen, drift- och förvaltningsdokumentation och avvikelseanalysen för att identifiera potentiella sårbarheter i systemet. | SARA\_SBH.E4 |

Tabell 107 – Assuranskrav – Riskanalys och Sårbarhetsanalys SARA\_SBH

(UTÖKAD)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet för testning. | SARA\_SBH.D1 |
| IT-systemet ska vara i testbart skick. | SARA\_SBH.C1 |
| Evalueraren ska verifiera att informationen i leverantörens dokumentation är tillräcklig för att utföra en grundlig sårbarhetsanalys av hela systemet. | SARA\_SBH.E1 |
| Evalueraren ska använda tillgängliga källor för att komplettera leverantörens dokumentation, t.ex. publik sårbarhetsinformation. | SARA\_SBH.E2 |
| Evalueraren 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. | SARA\_SBH.E3 |
| Evalueraren ska genomföra en oberoende och metodisk sårbarhetsanalys av systemet baserad på all tillgänglig information och erfarenhet för att identifiera potentiella sårbarheter i systemet. | SARA\_SBH.E5 |
| Evalueraren ska genomföra praktiska tester av systemet för att avgöra om de potentiella sårbarheterna kan utnyttjas i den tänkta användningen av systemet. | SARA\_SBH.E7 |

Tabell 108 – Assuranskrav – Riskanalys och Sårbarhetsanalys SARA\_SBH

(HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Systemutvecklaren ska tillhandahålla systemet för testning. | SARA\_SBH.D1 |
| IT-systemet ska vara i testbart skick. | SARA\_SBH.C1 |
| Evalueraren ska verifiera att informationen i leverantörens dokumentation är tillräcklig för att utföra en grundlig sårbarhetsanalys av hela systemet. | SARA\_SBH.E1 |
| Evalueraren ska använda tillgängliga källor för att komplettera leverantörens dokumentation, t.ex. publik sårbarhetsinformation. | SARA\_SBH.E2 |
| Evalueraren 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. | SARA\_SBH.E3 |
| Evalueraren ska genomföra en oberoende, metodisk och semiformell sårbarhetsanalys av systemet baserad på all tillgänglig information och erfarenhet för att identifiera potentiella sårbarheter i systemet. | SARA\_SBH.E6 |
| Evalueraren ska genomföra praktiska tester av systemet för att avgöra om de potentiella sårbarheterna kan utnyttjas i den tänkta användningen av systemet. | SARA\_SBH.E7 |

Tabell 109 – Assuranskrav – Riskanalys och Sårbarhetsanalys SARA\_SBH

##### Restriskanalys (SARA\_RRA)

Kravet syftar till att identifiera sårbarheter och osäkerheter för systemets säkerhetsförmågor.

(GRUND/UTÖKAD/HÖG)

| KSF kravtext | Källa [2] |
| --- | --- |
| Evalueraren ska verifiera att alla andra evalueringsaktiviteter är genomförda med godkänt resultat. | SARA\_RRA.E1 |
| Evalueraren ska genomföra restriskanalys för att identifiera kvarvarande osäkerheter kring systemets IT-säkerhetsförmågor. | SARA\_RRA.E2 |
| Evalueraren 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. | SARA\_RRA.E3 |

Tabell 110 – Assuranskrav – Riskanalys och Sårbarhetsanalys SARA\_RRA

## Tillkommande säkerhetskrav

I följande underavsnitt finns samtliga tillkommande säkerhetskrav förtecknade.

De säkerhetskrav som inte härstammar från KSF definieras som ”tillkommande krav”. Dessa ska hanteras på motsvarande sätt som KSF-kraven i det fortsatta design- och kravarbetet.

De tillkommande kraven hämtas från andra kravkällor, dokument. De har då redan en kravidentitet (Krav-ID). Om modifiering sker behöver en ny unik Krav ID tas fram. Modifieringar görs normalt i efterföljande kapitel då kraven allokeras och tolkas. Där kommer kraven att behöva nya Krav ID enligt en fastlagd konvention.

### Säkerhetskrav från verksamheten

Detta avsnitt innehåller verksamhetens tillkommande krav på informationssäkerhet.

Dessa krav hämtas från verksamhetsanalysen ur *Särskild säkerhetsskyddsbedömning*, från FM ITSS, AU-I eller från AU-D. Ange i kolumnen *Källa* både vilket dokument kravet är hämtat från och den kravidentitet som använts i källan.

| Kravtext | Kravkommentar | Källa |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Tabell 111 – Verksamhetens tillkommande säkerhetskrav. Formulering oförändrad från källan.

### Säkerhetskrav från regelverk

Detta avsnitt innehåller tillkommande krav på informationssäkerhet för uppfyllnad av tillämpliga regelverk.

Dessa krav hämtas från regelverksanalysen ur *Särskild säkerhetsskyddsbedömning*, från FM ITSS, AU-I eller från AU-D. Ange i kolumnen Källa både från vilket dokument kravet är hämtat och den kravidentitet som använts i källan.

| Kravtext | Kravkommentar | Källa |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Tabell 112 – Säkerhetskrav från regelverk. Formulering oförändrad från källan.

### Säkerhetskrav från hot- och riskanalys

Detta avsnitt innehåller tillkommande krav för riskreducering.

Dessa krav hämtas från hot- risk- och sårbarhetsanalys i *Särskild säkerhetsskyddsbedömning*, från FM ITSS, AU-I eller från AU-D. Ange i kolumnen *Källa* både från vilket dokument kravet är hämtat och den kravidentitet som använts i källan.

| Kravtext | Kravkommentar | Källa |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Tabell 113 – Tillkommande riskreducerande krav. Formulering oförändrad från källan.

### Övriga säkerhetskrav

Detta avsnitt innehåller tillkommande krav från övriga kravkällor.

Om det finns krav från övriga källor används detta avsnitt (annars radera avsnittet). Ange i kolumnen *Källa* både från vilket dokument kravet är hämtat och den kravidentitet som använts i källan.

Exempel på krav som ställs här är sådana som gäller leverantörens kompetens avseende informationssäkerhet, samt vad som förväntas av leverantören vid respektive avstämningspunkt.

| Kravtext | Kravkommentar | Källa |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Tabell 114 – Tillkommande krav från övriga kravkällor. Formulering oförändrad från källan.

# Säkerhetskrav på omgivningen

Detta kapitel avser uppfylla KSF-kraven SASS\_OMG.D1, C1 till C5.

I detta kapitel specificeras de informationssäkerhetskrav som ställs på informationssystemets driftmiljö.

Detta kapitel specificerar de informationssäkerhetskrav som inte uppfylls av ackrediteringsobjektet men som måste hanteras av driftmiljön eller omgivningen, för att informationssystemet ska vara säkert att använda. Hur dessa krav hanteras anges i *Informationssäkerhetsdeklaration* för informationssystem (t.ex. krav som ska uppfyllas av Försvarsmakten eller av andra informationssystem). Kraven kan vara antingen tekniska, administrativa, organisatoriska eller fysiska. Kraven måste formuleras så mottagaren enkelt kan verifiera och begripa dem. Se anvisningstexten i nästa kapitel för mer stöd om lämpliga egenskaper för krav.

*Tabell 115* nedan är ett förslag till hur kraven kan förtecknas. Ange i kolumnen *Källa* vart kravet, är hämtat och vilken kravidentitet som använts.

| Nytt krav ID | Ny kravtext | Ny kravkommentar | Källa |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabell 115 – Tolkade säkerhetskrav på omgivningen

# Tolkade säkerhetskrav

Detta kapitel avser uppfylla KSF-kraven SASS\_TOL.D1, C1 till C4.

I detta kapitel specificeras de informationssäkerhetskrav som ställs på ackrediteringsobjektet och dess utveckling (leverantörer).

Med en specificerad säkerhetsarkitektur kan kraven från kapitel 4 och andra kravkällor (se ISD-plan, AU-D och ITSA) tolkas för varje komponent i informationssystemet. Kraven kan i detta skede också allokeras till omgivningen (se *kapitel 5*) respektive på ackrediteringsobjektet (detta kapitel).

Syftet med kraven som redovisas i detta kapitel är att de ska kunna lyftas ut (kopieras) till en eller flera *Tekniska Specifikationer* (TS)/*Verksamhetsåtagandespecifikationer* (VÅS) såsom formulerade här. När dessa är färdigställda innehåller de den totala kravbilden som respektive leverantör ska uppfylla.

Härifrån kan kravtexten och kommentarer kopieras från till TS/VÅS. Krav ID blir troligen nytt för att passa strukturen i kravdokumenten. Spårningsinformation som inte tillför leverantören något raderas. Men terminologin i TS/VÅS behöver synkroniseras för att tydliggöra kravbilden för leverantören.

I de fall kraven ska fördelas på flera leverantörer kan behov finnas att dela upp dem och/eller ge samma krav till mer än en leverantör. Detta görs vid kravallokeringen på de komponenter som ska utvecklas av olika leverantörer. Detta gör att kraven som finns specificerade och allokerade i detta kapitel kan kopieras som de är till respektive leverantörs TS/VÅS.

Ett välformulerat krav behöver uppfylla en rad egenskaper bl.a. ska det vara:

* Specifikt – det ska inte finnas några tolkningsmöjligheter av kravet.
* Mätbart – det ska gå att mäta om ett krav uppfyllts eller ej.
* Realiserbart – det ska vara möjligt att uppfylla kravet inom ställda ramar.
* Allokerat – det ska framgå vilket delsystem/komponent som ska uppfylla kravet.
* Spårbart – det ska motiveras och framgå vilka källkrav som uppfylls av detta krav, med motivering.

Kravarbetet görs lämpligen i ett externt verktyg och resultatet redovisas i detta kapitel. Hur strukturen på redovisningen sker är valfritt.

*T.ex. Samtliga krav kan redovisas i en enda lång tabell eller gruppvis av sammanhörande krav (per säkerhetsfunktion och per komponent).*

Nedanstående tabell är ett förslag till hur kraven kan förtecknas. Ange i kolumnen *Källa* vart kravet är hämtat från och vilken kravidentitet som använts.

| Nytt krav ID | Ny kravtext | Ny kravkommentar | Källa |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabell 116 – Tolkade säkerhetskrav

# Uppfyllande av säkerhetskrav

Detta kapitel lämnas tomt men kommer att kompletteras i en senare fas av ISD-arbetet.