KSF

Krav på IT-säkerhetsförmågor hos IT-system

v3.1

INNEHÅLLSFÖRTECKNING

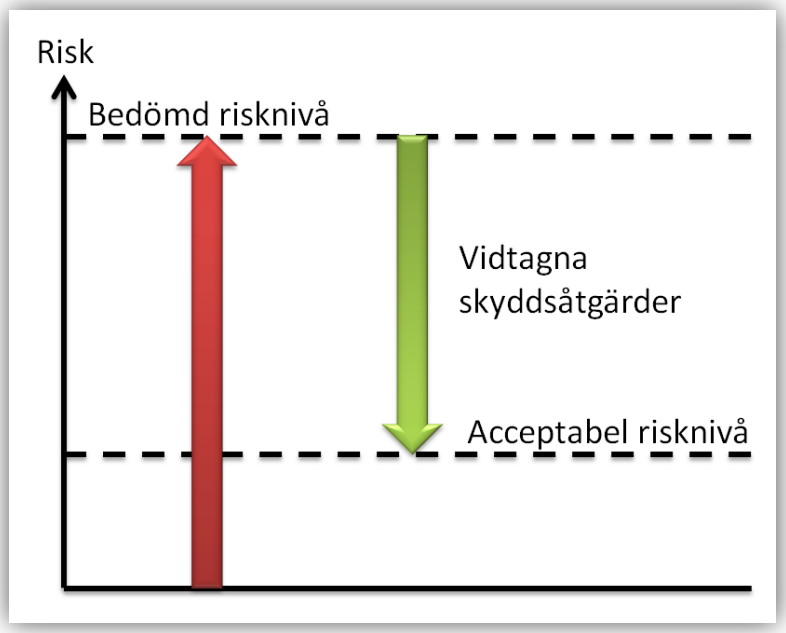
FIGURFÖRTECKNING

TABELLFÖRTECKNING

1 Introduktion

1.1 Inledning

KSF[1] är de krav på IT-säkerhetsförmågor som militära underrättelse- och säkerhetstjänsten (MUST) tagit fram och som, enligt C MUST beslut[2], alla IT-system[3] i Försvarsmakten måste uppfylla för att tillräckliga skyddsåtgärder ska anses föreligga. I detta perspektiv utgör KSF en del av MUST riskhantering avseende IT-säkerhetsförmågor för att reducera eller eliminera bedömda risker sett till IT-system.



Figur 1 Relation mellan bedömd risk och skyddsåtgärder i KSF

För ökad läsbarhet i detta dokument har prefixet ”IT-” lyfts bort från orden ”IT-säkerhetsförmågor” respektive ”IT-system”, dock är det samma innebörd som avses. I de fall annat avses så anges detta särskilt.

1.2 Syfte, målgrupper

KSF används i första hand när man definierar de IT-säkerhetskrav som ger systemet dess säkerhetsförmågor, inför upphandling samt då MUST bedömer IT-system ur säkerhetssynpunkt inför MUST yttrande inför ackreditering. Dessa krav utgör en del av Försvarsmaktens kravställning på IT-system inom IT-processen.

[1] Krav på säkerhetsfunktioner.
[2] KSF version 2.0 – Beslut om krav på godkända säkerhetsfunktioner, vers. 2.0, HKV skr. 2004-12-20 bet. 10 750:78976
[3] Med IT-system avses enligt 7 kap. 1 § 2 Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd system med teknik som hanterar och utbyter information med omgivningen.

Sett till ett systems livscykel fokuserar KSF på kravställning under utveckling av systemet, dvs. processen fram till ackreditering. Detta då IT-säkerhet och förtroendet för systemets säkerhetsförmåga måste byggas in i systemet från början och inte läggas till som avslutande åtgärder på ett redan utvecklat system.

KSF riktar sig i första hand till personal inom Försvarsmakten och externa organisationer som kravställer och anskaffar IT-system för Försvarsmaktens räkning.

KSF riktar sig inte direkt till de som utvecklar IT-system, då de istället är mottagare av den kompletta kravställning på IT-systemet som innehåller krav med ursprung i KSF. Det är kravställarens ansvar att se till att denna kravställning ger IT-systemet tillräckliga IT-säkerhetsförmågor enligt KSF.

Att systemet har tillräckliga säkerhetsförmågor innebär ingen garanti att systemet används på ett säkert sätt eftersom ansvaret för detta slutligen åligger nyttjaren. Uppföljning av säkert användande sker bland annat genom den kontrollverksamhet som bedrivs inom ramen för respektive definierad rolls ansvarsområde enligt livscykelmodellen och av Försvarsmaktens Chief Information Officer (CIO). Utöver detta genomför den militära säkerhetstjänsten säkerhetsskyddskontroller, där IT-säkerhet utgör en delmängd.

1.3 Roller

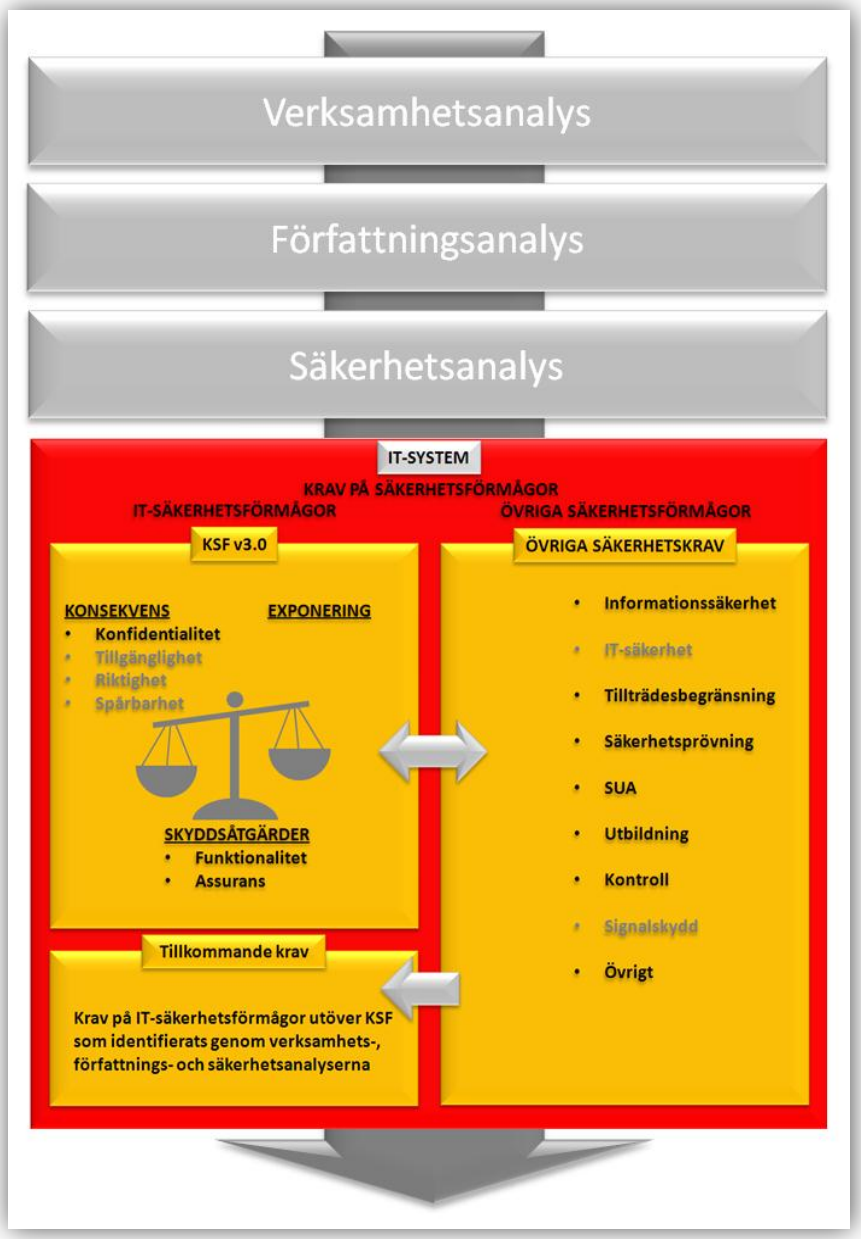
KSF följer av CIO framtagen IT-Styrmodell[4] vilket innebär att följande begrepp används:

- **Beställare** är de som beslutar, beställer och finansierar en IT-tjänst[5]. Beställaren är ansvarig för verksamhet eller sakområde enligt FM ArbO.
- **Koordinerare** ansvarar för att sammanställa och koordinera kravställningen på IT-tjänster. Koordineraren ansvarar också för att inrikta, beställa och följa upp produktionen av IT-tjänster. Ansvarig för sakområde IS/IT och informationsinfrastruktur är också ansvarig för koordineringen.
- **Utförare**[6] är de som producerar och tillhandahåller IT-tjänster. Ett annat sätt att uttrycka det är att de är leverantörer. I KSF används begreppen systemutvecklare och drift- och förvaltning för att precisera vilken typ av utförare som avses.
- **Nyttjare**, slutligen, är de som använder IT-tjänsterna i verksamheten.

[4] HKV 2011-10-31 09100:64970
[5] Kostnaderna för IT-infrastrukturen finansieras (kostnadsfördelas) också av beställarna.
[6] Intern organisationsenhet inom Försvarsmakten som erhåller uppdrag att leverera hel eller del av IT-tjänst benämns intern utförare, exempel är FMLOG eller FMTM. Andra myndigheter, företag och organisationer som via avtal förbinder sig att leverera hel eller del av IT-tjänst benämns extern leverantör, exempel är FMV eller industrin (HKV 2011-04-08 09100:56741).

1.4 Relationen till verksamhets-, författnings- och säkerhetsanalys

Figur 2 beskriver på en övergripande nivå sambandet mellan verksamhets-, författnings- och säkerhetsanalys samt KSF. Detta beskrivs kortfattat nedan.



Figur 2 Samband mellan verksamhets-, författnings- och säkerhetsanalys samt KSF

1.4.1 Verksamhetsanalys

En verksamhetsanalys beskriver i IT-säkerhetssammanhang den verksamhet som ett IT-system är tänkt att stödja, vilka slag av uppgifter som IT-systemet är avsett att behandla (t.ex. sekretessbedömning) samt verksamhetens krav på skydd (t.ex. i

fråga om tillgänglighet). En verksamhetsanalys utgör en utgångspunkt för författningsanalys och säkerhetsanalys.

1.4.2 Författningsanalys

En författningsanalys syftar till att beskriva vilka lagar, förordningar, föreskrifter och interna bestämmelser som är aktuella för ett IT-system och för de uppgifter som avses behandlas i IT-systemet

1.4.3 Säkerhetsanalys

I säkerhetsanalysen identifieras och prioriteras alla skyddsvärda tillgångar (personal, materiel, information, verksamhet och anläggningar) vilka kommer att bearbetas, lagras eller på annat sätt hanteras av systemet (inklusive systemet självt) och därefter görs en bedömning av vilken konsekvens som uppstår och omfattningen av denna om uppgifter rörande de identifierade tillgångarna utsätts för en oönskad händelse som påverkar sekretess, tillgänglighet, riktighet och spårbarhet.
Resultatet av säkerhetsanalysen utgör ingångsvärden till KSF genom att konsekvensnivån har beskrivits och bedömts enligt en fastställd skala. Säkerhetsanalysen resulterar även i ingångsvärden till *Övriga säkerhetskrav*. De övriga säkerhetskraven kan i vissa fall utgöra ingångsvärden till KSF säkerhetsmodell, t.ex. genom att påverka systemets exponering. De övriga säkerhetskraven kan även i vissa fall, då de är uppfyllda, ge driftmiljön egenskaper som bidrar till att uppfylla KSF. Detta representeras av den dubbelriktade pilen i Figur 2.

1.4.4 Krav på IT-säkerhetsförmågor (KSF)

Genom KSF anges vilka säkerhetsförmågor ett system minst ska ha samt vad MUST anser vara en acceptabel risknivå för system driftsatta i Försvarsmakten. Då risken kan variera mellan olika system bland annat genom verksamhetens art, driftmiljöns beskaffenhet och den typ av information som hanteras behöver säkerhetsförmågorna kunna anpassas efter dessa omständigheter. I KSF sker anpassningen med hjälp av en modell med tillhörande metodik för att identifiera och beskriva kraven. Det är till denna modell som verksamhets-, författnings- samt säkerhetsanalysen ger input, i termer av konsekvens och exponering, för att möjliggöra anpassning och fastställa krav på systemets IT-säkerhetsförmåga[7].

1.4.5 Tillkommande krav

Kraven KSF ställer på ett systems säkerhetsfunktioner utgör endast en för Försvarsmakten gemensam lägsta nivå. Det är därför mycket möjligt att det för ett specifikt system kan tillkomma säkerhetskrav som ett resultat av specifika behov (t.ex. hög tillgänglighet), från lagar och författningar (exempelvis PUL[8]) eller från

[7] I Figur 2 ovan är ingångsvärdena riktighet, tillgänglighet och spårbarhet gråmarkerade då dessa i KSF inte ingår i modellen och därmed inte heller hanteras genom specifika krav i KSF.
[8] *Personuppgiftslag (*1998:204)

den verksamhet som skall använda systemet. Dessa tillkommande säkerhetskrav identifieras genom verksamhets- och säkerhetsanalyserna.

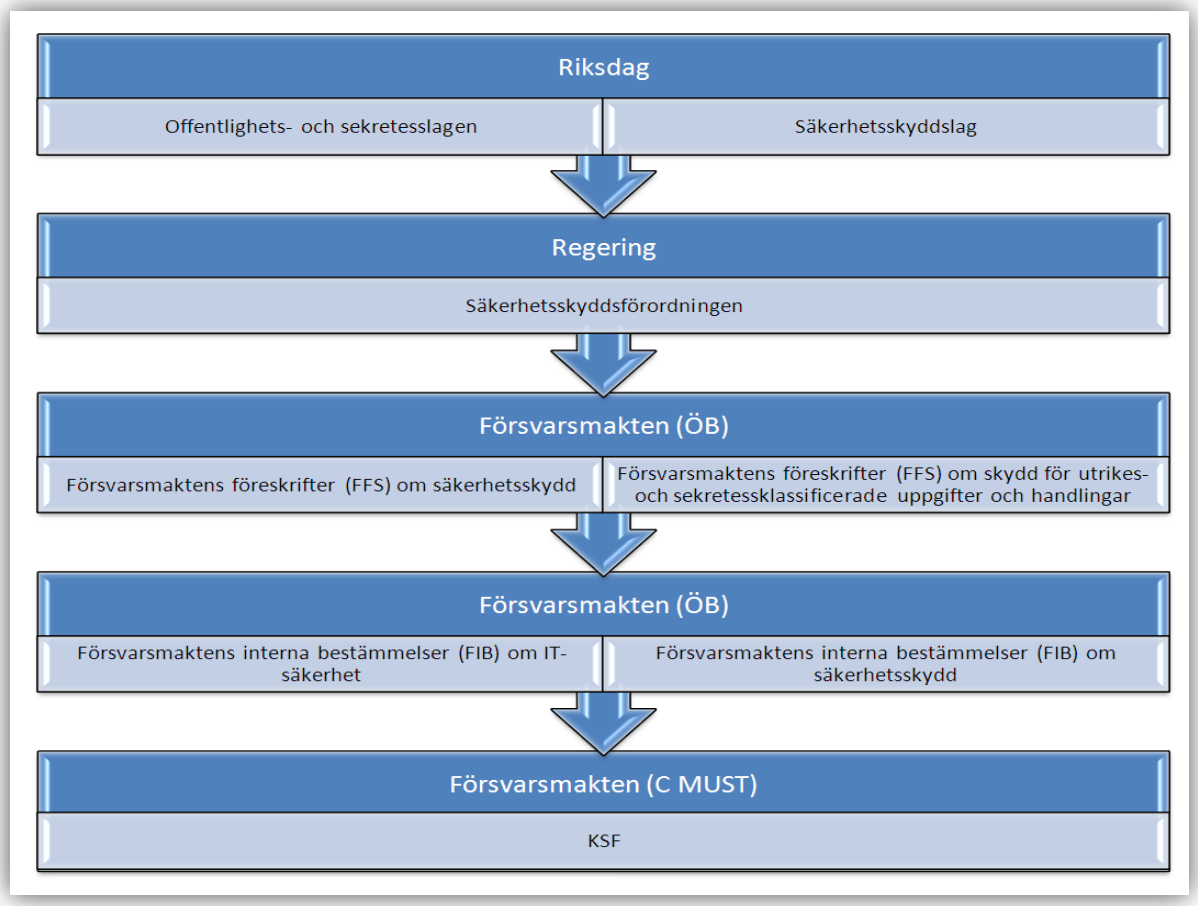
1.5 Dispositionen av KSF

KSF har följande disposition:

- Beslutsskrivelse
- Bilaga 1 med följande innehåll:
    - Kapitel 1 (detta kapitel) är en inledande beskrivning för att ge läsaren en översikt av KSF och kan läsas som en sammanfattning och introduktion till KSF modell.
    - Kapitel 2 beskriver grundläggande principer och den säkerhetsmodell som används för att identifiera gällande säkerhetskrav. Kapitel 2 lägger grunden för en djupare förståelse av modellen
    - Kapitel 3 beskriver de funktionella säkerhetskraven som definierar vilka säkerhetsförmågor ett system måste ha.
    - Kapitel 4 beskriver hur man identifierar assuranskrav på system samt vilken nivå av godkännande som krävs av IT-säkerhetskomponenter.
- Underbilaga 1 innehåller ordlista med begrepp och akronymer.
- Underbilaga 2 definierar innehållet i IT-systemets säkerhetsspecifikation (ITSS). ITSS ska beskriva systemet och de säkerhetskrav som systemet skall uppfylla samt hur detta görs.
- Underbilaga 3 definierar de funktionella säkerhetskraven som är indelade i klasser, krav och kravkomponenter. Kravkomponenterna är kopplade till respektive kravnivå
- Underbilaga 4 definierar assuranskraven som är indelade i klasser, krav och kravkomponenter. Kravkomponenterna är kopplade till respektive kravnivå

1.6 Författningsmässiga grunder för KSF

Detta avsnitt beskriver vilket författningsmässigt stöd som föreligger för KSF och utgör inte någon författningsanalys för enskilda system. KSF utgör således ingen sammanställning av aktuella författningskrav för system.



Figur 3: Författningsmässiga grunder för KSF

I säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) finns föreskrifter som rör säkerhetsskydd. Närmare föreskrifter om verkställighet av dessa föreskrifter återfinns i Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd samt i Försvarsmaktens interna bestämmelser (FIB 2007:2) om säkerhetsskydd och skydd av viss materiel. Försvarsmakten har även beslutat Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet[9]. Såväl Säkerhetsskyddsförordningen som Försvarsmaktens föreskrifter om säkerhetsskydd och Försvarsmaktens interna bestämmelser om IT-säkerhet innehåller krav på godkända säkerhetsfunktioner[10]. Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar samt Försvarsmaktens interna bestämmelser om IT-säkerhet innehåller även bestämmelser om IT-säkerhet för system som även är avsedda för

[9] Den sistnämnda författningen ändrades genom FIB 2010:2 (tillika omtryck)
[10] Godkända säkerhetsfunktioner anges för behörighetskontroll, säkerhetsloggning, intrångsdetektering, skydd mot röjande signaler, skydd mot obehörig avlyssning, skydd mot intrång och skydd mot skadlig kod.

behandling av utrikesklassificerade[11] och sekretessklassificerade uppgifter samt uppgifter som inte omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) hädanefter kallat OSL.

1.6.1 Avseende hemliga uppgifter

Av Försvarsmaktens interna bestämmelser om IT-säkerhet framgår att varje system som är avsett för behandling av hemliga uppgifter ska vara försett med av MUST godkända säkerhetsfunktioner.

1.6.2 Avseende utrikesklassificerade uppgifter

Av Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar[12] följer att system som behandlar utrikesklassificerade uppgifter ska ha motsvarande säkerhetsfunktioner som gäller för system som behandlar hemliga uppgifter.

1.6.3 Avseende övriga uppgifter

Av Försvarsmaktens interna bestämmelser om IT-säkerhet framgår att varje system som inte är avsett för behandling av hemliga uppgifter ska vara försett med av MUST godkända säkerhetsfunktioner om systemet är avsett att användas av flera personer.

[11] En uppgift som av en utländsk myndighet eller mellanfolklig organisation eller av en svensk myndighet har klassificerats i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED eller motsvarande och som är sekretessbelagd enligt 15 kap. 1 § offentlighets- och sekretesslagen men som inte rör rikets säkerhet (1 kap. 3 § 2 Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar).
[12] FFS 2010:1 2 kap. 1 §

1.7 Modell och metod

Syftet med modellen för KSF är att på ett entydigt sätt definiera krav på de säkerhetsförmågor som ett visst system måste ha samt de assuranskrav som ger tilltro till att säkerhetsförmågorna existerar och att avsedda skyddsåtgärder därmed uppnås.
För anpassning av säkerhetskraven används två faktorer:

1. Konsekvens av en oönskad händelse som påverkar sekretessen (informationsförlust[13]) för informationen som bearbetas, lagras eller på annat sätt hanteras av systemet samt
2. Hur exponerat systemet är för aktörer som kan påverka systemet.

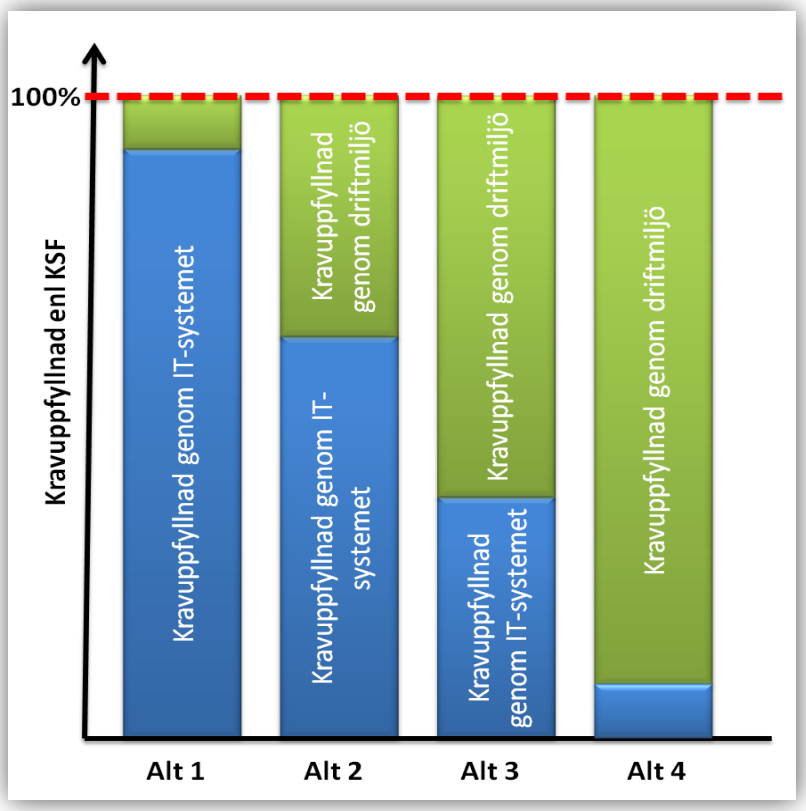
I de fall där olika bedömningar kommer i konflikt med varandra sker avdömning genom dialog med MUST. Exempel på detta kan vara verksamhet där krav på tillgänglighet kommer i konflikt med krav på sekretess.

1.7.1 Funktionella säkerhetskrav

Genom funktionella säkerhetskrav anges vilka säkerhetsförmågor som ett system minst skall uppvisa. Kraven indelas i olika klasser[14]där styrkan i kraven representeras av kravnivåerna Grund (G), Utökad (U) eller Hög (H). Funktionella säkerhetskrav ska alltid uppfyllas vilket dock kan ske på olika sätt. Kraven kan uppfyllas genom tekniska åtgärder i systemet, genom att utnyttja egenskaper i systemets driftmiljö [15] eller genom en kombination av dessa (illustreras i Figur 4).

Det är systemutvecklarens ansvar att för aktuellt IT-system påvisa såväl ATT kravuppfyllnad föreligger som HUR kravuppfyllnad erhålls för de funktionella kraven.

[13] I KSF är skyddsåtgärder endast kopplat till sekretess hos informationen. Eventuella skyddsåtgärder för riktighet och tillgänglighet uppfylls i den grad som kraven på skydd av sekretess även kan tillgodose dessa behov. Detta innebär att modellen för KSF inte specifikt tar hänsyn till krav på riktighet och tillgänglighet. Det hindrar dock inte att man i verksamhetsanalysen identifierar sådana krav och att dessa krav kvalitetssäkras genom att dokumenteras i ITSS och evalueras tillsammans med KSF säkerhetskrav.
[14] Motsvarar de godkända säkerhetsfunktioner som anges i FFS och FIB, dvs. behörighetskontroll, säkerhetsloggning, intrångsskydd, intrångsdetektering, skydd mot skadlig kod, skydd mot obehörig avlyssning samt skydd mot röjande signaler.
[15] Kan vara av t.ex. geografisk, fortifikatorisk, personell eller administrativ karaktär



Figur 4: Illustrativt exempel på alternativa sätt att nå kravuppfyllnad.

1.7.2 Assuranskrav

Assuranskraven anger hur förtroende för säkerhetsförmågor ska påvisas. Assuranskraven är indelade i olika klasser där styrkan i kraven representeras av kravnivåerna Grund (G), Utökad (U) eller Hög (H) på samma sätt som de funktionella säkerhetskraven.
Assurans[16] ska påvisas även för egenskaper i systemets driftmiljö. Med *kravuppfyllnad genom driftmiljö* avses i dessa fall inte möjligheterna att reducera systemets exponering utan istället de egenskaper i driftmiljön som helt eller delvis bidrar till att uppfylla vissa säkerhetsförmågor.

Det är systemutvecklarens ansvar att för aktuellt IT-system påvisa såväl ATT kravuppfyllnad föreligger som HUR kravuppfyllnad erhålls för assuranskraven.

1.7.3 Evaluering och evalueringsmetodik

En evalueringsmetodik beskriver hur granskning av system ska genomföras, dvs. tillvägagångssättet för att verifiera att säkerhetsförmågor och säkerhetskrav är

[16] Förtroende och tillit för att egenskapen ger avsedd effekt.

riktigt identifierade och att systemet uppfyller dem. Evalueringsmetodik beskriver även hur evalueringen ska dokumenteras. Syftet med evalueringsmetodiken är att säkerställa att evalueringar genomförs och dokumenteras på ett enhetligt sätt och med tillräcklig kvalitet.
Evalueringsmetodiken tas fram fristående från funktions- och assuranskraven och riktar sig enbart till den personal som ska evaluera att ett system uppfyller KSF samt till de som ska verifiera att evalueringarna är fullständigt och riktigt genomförda.

2 Säkerhetsmodell för KSF

2.1 Inledning

KSF säkerhetsmodell bygger på en anpassning av säkerhetsförmåga (genom ansatt kravnivå) utgående från konsekvensbedömning av informationsförlust i systemet samt systemets tänkta exponering. Genom att identifiera i vilken omfattning ett system kan utsättas för angrepp eller missbruk kan krav på säkerhetsförmågor anpassas till de bedömda riskerna i den aktuella driftmiljön. De genom säkerhetsmodellen härledda kraven på säkerhetsförmågor, kan uppfyllas genom tekniska åtgärder i systemet, genom att utnyttja egenskaper i systemets driftmiljö [17] eller genom en kombination av dessa.

KSF beskriver, genom assuranskraven, vilket underlag som krävs för att visa att säkerhetsfunktionaliteten i systemet implementerats på ett tillräckligt och effektivt sätt och för att kunna bedöma och beskriva den kvarvarande risken.

2.2 KSF säkerhetsmodell – modellens struktur

De båda kategorierna, assuranskrav och funktionella krav, är i modellen strukturerade på likartat sätt. Kraven är grupperade i klasser som vardera berör en viss typ av säkerhetsförmåga.

Förtroendet för att systemets säkerhetsfunktioner är korrekta och effektiva under de tänkta förutsättningarna benämns assurans och kräver att:

- det finns förtroende för ursprunget till systemet och dess komponenter (då det är mycket svårt att skydda sig mot en opålitlig eller illvillig systemutvecklare)
- de processer som tillämpats i utvecklingsmiljön för leverans till drift- och förvaltning är dokumenterade och pålitliga (då det är mycket svårt att kontrollera allt vid leverans)
- systemet konstruerats på ett strukturerat sätt och att detta dokumenterats (då det annars inte är möjligt att bedöma systemet)
- systemet är testat på ett ur säkerhetssynpunkt relevant sätt (för att säkerställa att det uppvisar de kravställda IT-säkerhetsförmågorna)
- nyttjaren och drift- och förvaltningsorganisationen får instruktioner om hur systemet ska installeras, användas och förvaltas på ett säkert sätt (eftersom systemet annars inte används på ett tänkt och kanske därmed inte heller säkert sätt)
- systemet har analyserats och svagheter eller avvikelser och deras konsekvenser dokumenterats (för att ge underlag för beslutet om systemets verksamhetsnytta överstiger riskerna det medför).

Kraven i kategorin funktionella säkerhetskrav återfinns i underbilaga 3 och kraven i kategorin assuranskrav återfinns i underbilaga 4 till detta dokument.

[17] Kan vara av t.ex. geografisk, fortifikatorisk, personell eller administrativ karaktär

2.2.1 Kravstruktur

Kraven i KSF är indelade i klasser som utgör en gruppering av likartade krav. Varje klass har ett namn på fyra bokstäver som börjar med ”SF” för funktionella säkerhetskrav eller ”SA” för assuranskrav.
Några exempel på kravidentifiering ges nedan:

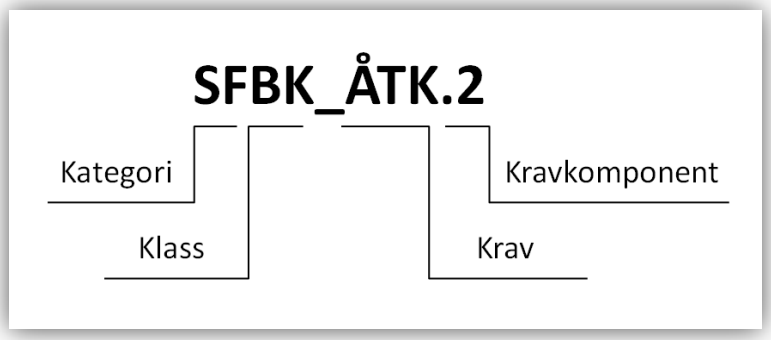
- SFIS – Klassen av funktionella säkerhetskrav som rör intrångsskydd
- SADE – Klassen av assuranskrav som rör IT-systemets arkitektur och design

Inom varje klass finns ett antal krav som beskriver vad som ska uppfyllas. Varje krav har ett unikt namn enligt nedanstående exempel:

- SFIS_HRD – Ett enskilt funktionellt säkerhetskrav tillhörande klassen SFIS
- SADE_ARK – Ett enskilt assuranskravkrav tillhörande klassen SADE

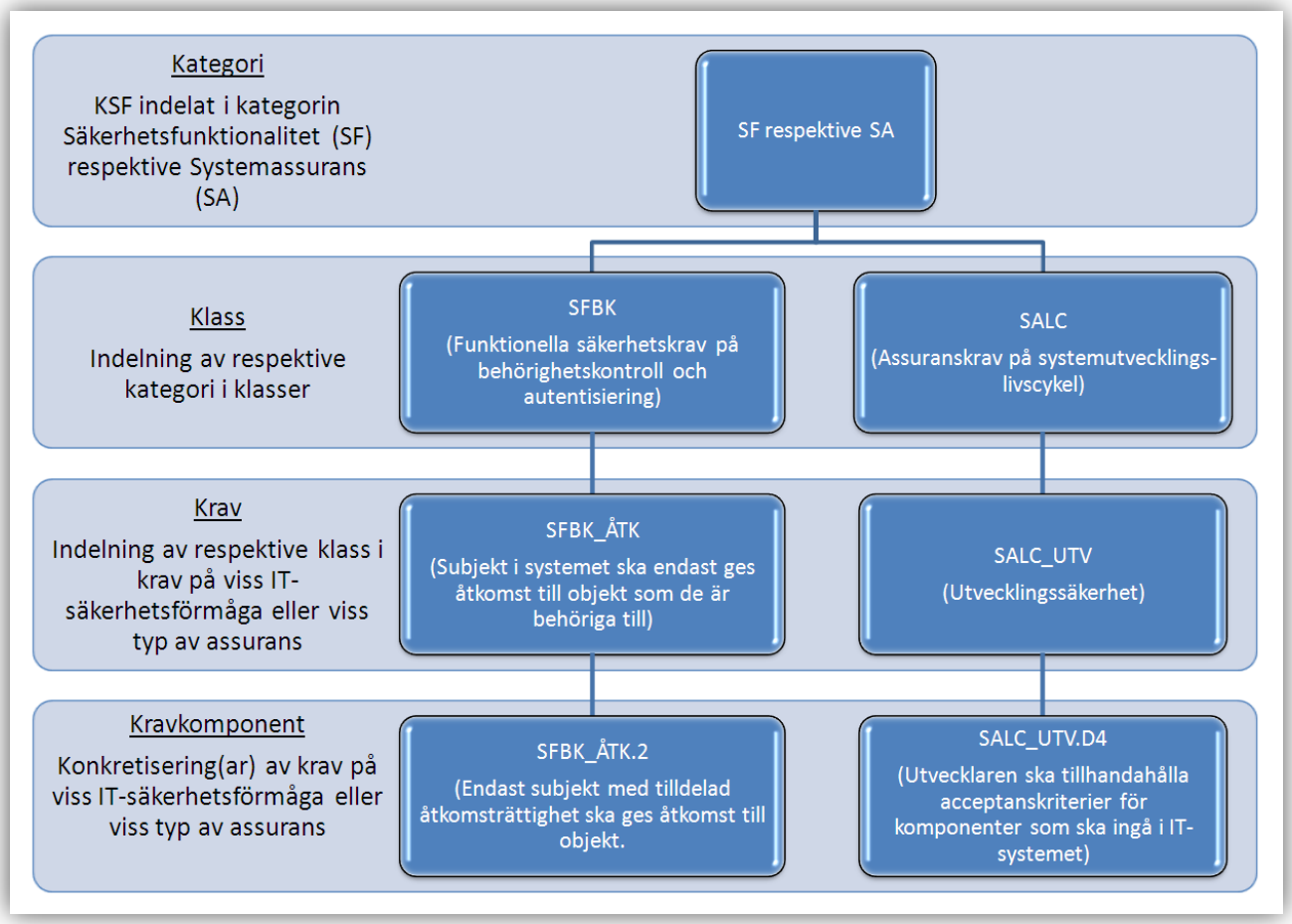
För varje krav finns ett antal kravkomponenter som visar på hur kravet kan uppfyllas. Dessa ges löpnummer enligt nedanstående exempel:

- SFIS_HRD.2 – Andra kravkomponenten från kravet SFIS_ HRD
- SADE_ARK.D1 – Första kravkomponenten från kravet SADE_ ARK



Figur 5: Exempel på kravidentifiering

Dessa kravidentifieringar utgör unika referenser till alla klasser, krav och kravkomponenter i KSF och ska användas när det hänvisas till KSF-krav i dokument eller nedtecknas i sammanställningar av krav etc.



Figur 6: Sammanfattande bild över kravstruktur och kravidentifiering

2.3 Säkerhetskrav för system och komponenter

KSF säkerhetsmodell utgår från att ett system består av en sammansättning av komponenter där vissa komponenter ger systemet dess säkerhetsförmåga.

Ett system som är sammansatt av godkända IT-säkerhetskomponenter går att lita på förutsatt att komponenterna sätts samman och används på avsett sätt. Komponenterna godkänns av MUST utefter en gradering som benämns komponentassuransnivå. Vilken komponentassuransnivå som krävs av komponenterna i ett visst system beskrivs översiktligt, dock inte uttömmande, i kapitel 4. Att sätta samman system av redan godkända komponenter kan innebära en avsevärd tidsbesparing istället för att varje gång återkommande behöva verifiera alla ingående IT-säkerhetskomponenter.

2.3.1 Definition av IT-system

I detta dokument används begreppet IT-system som benämning på den enhet som kravställs och bedöms enligt KSF. Ett sådant system kan i sin tur vara ett ”system av system” utan att för den sakens skull KSF måste tillämpas på varje enskild del.

Vilken nivå KSF skall tillämpas på fastställs inom ramen för Försvarsmaktens IT-process, genom indelning i delsystem kan man dock applicera KSF på mindre enheter, se 2.3.3.

2.3.2 Beroenden av externa komponenter

Vissa system förlitar sig på säkerhetsfunktionalitet som tillhandahålls av komponenter som inte ingår i systemet, exempelvis då systemet utgör en del av ett större system. I dessa fall måste det för varje krav som har ett sådant externt beroende, i IT-säkerhetsspecifikationen (ITSS), tydligt identifieras såväl beroendets art och till vad samt på vilket sätt kravet omhändertas.

Externa beroenden får endast finnas om den externa komponenten är del av ett ackrediterat system med minst samma nivå av funktionella krav och assuranskrav som det system vilket förlitar sig på den externa komponenten. Detta för att man ska kunna förlita sig på en säkerhetsegenskap i ett annat system. Denna egenskap måste ha utvärderats och överensstämma med vad det förlitande systemet förväntar sig. Kravet på ackreditering avser även tilltron till att den externa komponenten kan skydda sig själv så att egenskaperna bibehålls.

2.3.3 Indelning i delsystem

Genom uppdelning av ett system kan kostnadsdrivande krav isoleras till egna delsystem och därigenom sänka totalkostnaden för hela systemets skydd. Den möjliga sänkningen av totala kostnaden står i detta fall i proportion till omfattningen hos de kostnadsdrivande delarna jämfört med omfattningen hos de ej kostnadsdrivande delarna. Skyddet för separationen mellan delsystemen skall dock alltid uppfylla delsystemens högsta nivå.
Delsystemindelning ger en möjlighet att betrakta sitt system som "flera samverkande system". *Ur KSF-perspektiv* betraktas delsystem som självständiga system. Varje delsystem ska uppfylla KSF med avseende på funktionella säkerhetskrav och assuranskrav och självständiga ITSS ska sammanställas för varje delsystem.

2.4 Konsekvensnivå

Nedan beskrivs hur konsekvensnivån identifieras för ett specifikt system.

I säkerhetsanalysen identifieras vilken skyddsvärd information som avses hanteras av systemet. Informationen klassificeras med stöd av FM modell för infoklassning (enligt H SÄK Sekrbed Del A 2011). Resultatet är att informationen antingen är KH, H, UK, SK eller Ej sekretessbelagd. Om informationen är KH, H eller UK ska den dessutom inplaceras i en informationssäkerhetsklass[18]. Det sker genom en förtida men- respektive skadebedömning (konsekvensbedömning). Resultatet avgör bland annat systemets informationsklassificering.

[18] Placering i informationssäkerhetsklass sker genom en förtida menbedömning vilket är detsamma som en förtida bedömning av konsekvensen av att informationen röjs för obehörig

Information vilken efter sekretessbedömning klassificerats till SK bedöms därefter avseende vilken konsekvens som uppstår och omfattningen av denna om uppgifterna röjs. När en informationsmängd genom sekretessbedömning har klassats som SK och därefter bedömts avseende konsekvens kan den även jämföras (prioriteras) med H- och UK-uppgifter.
Principen i KSF är att bedömd konsekvensnivå utgör en faktor för att avgöra systemets nivå av skydd.

För att identifiera aktuell konsekvensnivå används i KSF samma tabell (Tabell 1 nedan) som vid steg 1 i säkerhetsanalysen[19]. I KSF används dock endast skalan 1-5.

Gradering		**Generell konsekvensbeskrivning samt konsekvensbeskrivning vid informationsförlust av sekretessklassificerade uppgifter.**	**Konsekvensbeskrivning avseende informationsförlust av hemliga eller utrikesklassificerade uppgifter**[20]
5	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.
4	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 ut- ländsk myndighet eller mellan- folklig organisation.
3	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.
2	Lindrig	Förväntade konsekvenser är ringa och begränsas till att påverka, försvåra, hindra, undergräva, misskreditera eller störa verksamheten i mindre	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

[19] H SÄK Skydd 2007
[20] Graden av men vid röjande av hemliga uppgifter som rör rikets säkerhet regleras i 1 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2003:7), samt beskrivs utförligt i H SÄK Sekrbed Del A (2011).

Gradering		Generell konsekvensbeskrivning samt konsekvensbeskrivning vid informationsförlust av sekretessklassificerade uppgifter.	Konsekvensbeskrivning avseende informationsförlust av hemliga eller utrikesklassificerade uppgifter[20]
		omfattning.	rikets säkerhet. Hemlig handling som har åsatts beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.
1	Försumbar	Konsekvenser för verksamheten är försumbara.	Uppgifter är inte hemliga eller utrikesklassificerade.

Tabell 2: Bedömning av konsekvens enligt femgradig skala.

2.5 Exponeringsnivå

Med exponeringsnivå avses bedömningen av hur exponerat systemet är avseende någon aktörs möjlighet att påverka systemet. Denna möjlighet kan vara såväl fysisk, d.v.s. att någon kommer åt den tekniska utrustning som utgör systemet, som logisk via systemets olika gränssnitt.
Ett systems exponering uttrycks i fyra nivåer med E1 som lägsta och E4 som högsta exponeringsnivå. Ökade möjligheter för någon aktör att påverka systemet definieras som en högre exponeringsnivå, vilket i sin tur medför högre krav på systemets säkerhetsförmåga.
Kriterierna för de fyra exponeringsnivåerna framgår av tabell 2.
Exponeringsnivån är den lägsta nivån för vilken det som anges för båda kriterierna, dvs. *Tillgång till systemets fysiska och logiska gränsytor* och *Informationsutbyte*, är uppfyllt. Observera att iterationer kan krävas för att identifiera en kostnadseffektiv nivå, t ex genom att förändra förutsättningarna för systemet och dess tänkta driftmiljö.

2.5.1 Exponering från personer

För att personer som tillfälligt vistas i lokaler där de kan få tillgång till ett systems gränsytor inte ska höja systemets exponeringsnivå måste dessa bevakas av någon som är bedömt pålitlig för uppgiften **och** är kompetent nog att avgöra vad som innebär en risk för systemet. Se direktiv om ”Personell bevakning” i skrivelsen HKV 2010-06-23 10.700:60542 [21].

2.5.2 Exponering från informationsutbyte

Med informationsutbyte avses allt utbyte av information med andra IT-system, vare sig det sker över elektroniskt kommunikationsnät eller med flyttbara lagringsmedia. Införande av säkerhetsuppdateringar samt uppdatering av säkerhetsfunktioners kontrollmekanismer och deras styrande data (t.ex.

[21] HKV 2010-06-23 10 700:60542 *Direktiv angående sektionering m.m. i utrymmen för IT och telekommunikation*

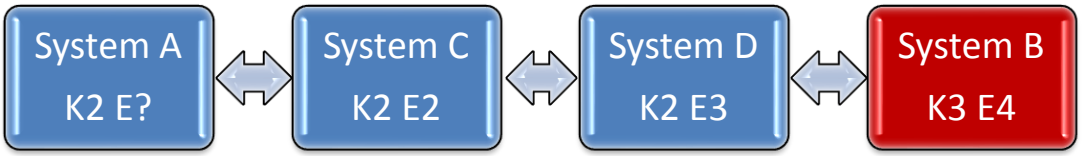
antivirussignaturer) som sker enligt fastställda drift- och säkerhetsinstruktioner, påverkar dock inte exponeringen av IT-systemet.
Vid informationsutbyte med system på samma eller lägre konsekvensnivå exponeras systemet även för de aktörer som kan få tillgång till dessa andra system. För att få hävda att sådant informationsutbyte **inte** innebär en ökad exponering för systemet måste det utförligt beskrivas hur säkerhetsfunktionerna i de andra systemen skyddar systemet från denna oönskade möjlighet informationsutbytet kan innebära.
Observera att i det sista exemplet kan systemet man utbyter information med vara på en geografiskt skild plats där flera andra system vidarebefordrar meddelandet på vägen. I detta fall måste systemet anses ha informationsutbyte med alla de system som hanterat meddelandet. Detta förklaras närmare i exempel 1 nedan.
Används ett signalskyddssystem med godkända intrångsskyddsegenskaper, t.ex. ett VPN-krypto, för informationsutbyte över en bärare, t.ex. ett nätverk, behöver dock inte systemet anses exponerat mot bäraren. Detta förklaras närmare i exempel 2 nedan.
När man skall bedöma exponeringen från informationsutbyte med ett system som inte är föremål för ackreditering av Försvarsmakten så måste systemets IT-säkerhetsförmåga bedömas. Bedömningen görs utifrån gällande avtal med den organisation som är ansvarig för systemet och deras godkännanden av systemet.

Exponerings-nivå	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[22] med tillgång till någon av systemets gränsytor är säkerhetsprövade[23].	**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[24] till en högre konsekvensnivå **eller** Samtliga system som systemet utbyter information med är ackrediterade[25] till samma konsekvensnivå med högst exponeringsnivå E2.
E1	Alla personer med tillgång till systemets gränsytor är behöriga[26] till all information som behandlas i systemet.	**och**	Systemet utbyter ingen information med andra system

Tabell 3: Exponeringsnivåer med tillhörande kriterier

Exempel 1: Fastställande av exponeringsnivå
IT-system A hanterar information med konsekvensnivå 2 och exponeringsnivå skall bedömas. Systemet befinner sig i lokaler där endast behöriga kan komma åt dess fysiska gränsytor. Systemet uppfyller därför kriterierna för exponeringsnivå 2 med avseende på exponering för personer med tillgång till systemets gränsytor. System A har dock informationsutbyte med system B som är ackrediterat för konsekvensnivå 3 med exponeringsnivå 4. Informationsutbytet sker via meddelanden vidarebefordrade av system C och D som är ackrediterade för konsekvensnivå 2 med exponeringsnivå 2 respektive 3.

[22] utländsk personal (vid t.ex. internationella övningar och insatser) hanteras i särskild ordning.
[23] 14 § Säkerhetsskyddsförordningen (1996:633)
[24] I fråga om andra organisationer hanteras detta genom avtal och överenskommelser
[25] I fråga om andra organisationer hanteras detta genom avtal och överenskommelser
[26] 7 kap. 1 § FIB IT-säkerhet.



Figur 7: Exempel 1 - Fastställande av exponeringsnivå

Detta innebär att IT-system A är exponerat för aktörer som har tillgång till antingen system B, C eller D. Eftersom system D är ackrediterat för samma konsekvensnivå med exponeringsnivå 3 ger detta den högsta exponeringen och IT-system A bedöms därför till exponeringsnivå 3.
I detta fall har dock system D säkerhetsfunktioner som säkerställer att de aktörer som utgör ett hot mot systemet inte kan påverka system A. System A kan då beskriva hur det förlitar sig på dessa säkerhetsfunktioner i system D och uppfyller då alla kriterier för exponeringsnivå 2.

Exempel 2: Användande av godkänt signalskyddssystem som intrångsskydd
IT-system X och Y är två system som hanterar information med konsekvensnivå 2 och utbyter information över ett ej ackrediterat nätverk Z. Systemen X och Y har i övrigt ingen exponering som skulle ge högre exponeringsnivå än E2, men bedöms då till exponeringsnivå 4 p.g.a. exponeringen från nätverk Z.

Figur 8: Exempel 2 - Informationsutbyte via ej ackrediterat nätverk

Genom att dela in system X och Y i vardera två delsystem X1, X2 och Y1, Y2 där X1 och Y1 endast består av en signalskyddskomponent med godkända intrångsskyddsegenskaper kan delsystemen X2 och Y2 beskriva hur de förlitar sig på intrångsskyddet som signalskyddskomponenterna i X1 och Y1 erbjuder och kan därmed bedömas till exponeringsnivå E2 som de skulle ha fått om de inte hade kommunicerat via nätverk Z.

Figur 9: Exempel 2 – Informationsutbyte via godkänt signalskyddssystem som intrångsskydd

Eftersom detta förväntas vara ett vanligt förekommande scenario tillåts av KSF ett undantag i bedömningen av exponeringsnivåer där system som har informationsutbyte via signalskyddssystem med godkända intrångsskyddsegenskaper inte behöver anses exponerade mot signalskyddssystemets ”bärare” och därmed tillåts nå lägre exponeringsnivåer utan att genomföra ovan beskrivna indelning i delsystem.

2.6 Fastställande av kravnivå

Säkerhetskraven är uppdelade i tre kravnivåerna Grund (G), Utökad (U) respektive Hög (H). Kravnivåerna bestäms utifrån konsekvensnivå, dvs. konsekvens av informationsförlust, och systemets exponeringsnivå.

Tabellen nedan anger kravnivån för funktionella säkerhetskrav och assuranskrav. Identifierad kravnivå utgör ingångsvärde för att fortsatt arbete med krav och kravkomponenter vilket framgår av underbilaga 3 för de funktionella säkerhetskraven och av underbilaga 4 för assuranskraven.

	Exponeringsnivå			
Konsekvensnivå	**E1**	**E2**	**E3**	**E4**
5	H	H	H	H
4	U	H	H	H
3	U	U	U	H
2	G	U	U	U
1	G	G	G	G

Tabell 4: Kravnivåer för funktionella säkerhetskrav och assuranskrav

2.7 Dokumentation - ITSS

För varje system ska en IT-säkerhetsspecifikation (ITSS) tas fram som beskriver systemet, dess tänkta användning samt de analyser som genomförts för att bestämma informationens konsekvensnivå och systemets exponeringsnivå. En ITSS skall dessutom innehålla alla säkerhetskrav som ställs på systemet, både de som ges av KSF och de som ges av verksamhetsanalysen och säkerhetsanalysen. ITSS är den kravspecifikation för IT-säkerhet som systemet verifieras mot. Strukturen och innehållet i en ITSS är fastställt av KSF och finns beskrivet i underbilaga 2 till detta dokument. Om delar av det innehåll som efterfrågas i ITSS redan finns i andra dokument är det tillräckligt att i ITSS ge en entydig referens till informationen.

För att kunna verifiera att ett system uppfyller sin ITSS krävs olika typer av dokumentation och underlag såsom designdokumentation, testplaner, testresultat,

dokumentation av rutiner för versionshantering och drift av systemet. Vilket underlag som behövs och vilken information som ska framgå bestäms av assuranskraven.

Förutom för ITSS ställer KSF inga krav på format eller utseende på dessa underlag annat än att det är fastställt och innehåller det som krävs av assuranskraven.

2.8 Evaluering

Bedömningen att ett system uppfyller KSF, dvs. att systemet uppfyller alla sina säkerhetskrav och att man har tillräckligt förtroende för detta benämns i KSF evaluering. Metodiken för detta finns beskrivet i KSF Evalueringsmanual som är ett separat dokument. I varje assuranskrav föreskrivs att systemutvecklaren ska producera viss dokumentation för att påvisa förtroendet för systemets säkerhetsförmåga och i KSF Evalueringsmanual finns beskrivningen av hur detta underlag ska granskas.

3 Funktionella säkerhetskrav

Funktionella säkerhetskrav är krav på en viss funktion eller beteende hos ett system som syftar till att helt eller delvis ge systemet en viss säkerhetsförmåga. De funktionella säkerhetskraven är så formulerade att de kan verifieras på ett objektivt sätt och testas genom funktionstester. Säkerhetsfunktionaliteten hos systemet som uppfyller kraven kan lokaliseras till enskilda komponenter och även till specifika delar av dessa komponenter.
För att möta ett hot eller uppfylla ett visst krav är det ofta nödvändigt att flera olika funktioner samverkar. Om krav på säkerhetsförmåga t.ex. är spårbarhet behövs inte bara generering av logghändelser utan även uppföljning av loggen och autentisering för att knyta händelsen till en individ.
KSF definierar åtta olika klasser av funktionella säkerhetskrav enligt nedan. Sju av dessa klasser utgår ifrån de i FFS och FIB angivna *godkända säkerhetsfunktioner* och representerar olika typer av säkerhetsfunktionalitet. Klasserna är indelade så att funktionella beroenden mellan kraven i första hand hålls inom varje klass. Detta gör det möjligt för ett system att ha olika kravnivåer på klasser oberoende av varandra. Vissa funktionella krav är dock tillämpliga för samtliga klasser. Dessa krav har i ett förtydligande syfte samlats i en egen klass, *Gemensamma krav (SFGK)*, istället för att anges inom var och en av de övriga klasserna.
De funktionella säkerhetskraven och deras tillhörande kravkomponenter finns i underbilaga 3.

3.1 Struktur för de funktionella säkerhetskraven

KSF definierar följande klasser av funktionella krav:

- Gemensamma krav (SFGK) – Funktionella säkerhetskrav som är gemensamma för alla säkerhetsfunktioner. Samtliga säkerhetsfunktioner i systemet skall omfattas av, men inte begränsas till, dessa krav.
- Behörighetskontroll (SFBK) – Kraven i klassen behörighetskontroll skall säkerställa kontroll av användares identitet, styra användares behörighet att använda systemet och dess resurser. Dessutom ska SFBK säkerställa att alla användare kan göras individuellt ansvariga för vidtagna åtgärder i systemet.
- Intrångsdetektering (SFID) – Kraven i klassen intrångsdetektering skall säkerställa att pågående samt redan genomförda intrång i systemet kan upptäckas och åtgärdas.
- Intrångsskydd (SFIS) – Kraven i klassen intrångsskydd skall säkerställa att system skyddas mot obehörig åtkomst.
- Skydd mot skadlig kod (SFSK) – Kraven i klassen skydd mot skadlig kod ska säkerställa att skadlig kod inte kan införas, utöva påverkan på, eller spridas via systemet.

- Säkerhetsloggning (SFSL) – Kraven i klassen säkerhetsloggning skall säkerställa att spårning av missbruk, och försök till missbruk av systemet kan genomföras.
- Skydd mot röjande signaler (SFRS) – Kraven i klassen skydd mot röjande signaler ska säkerställa att hemlig information som behandlas i systemet inte oavsiktligt röjs via strålning och läckande signaler.
- Skydd mot obehörig avlyssning (SFOA) – Kraven i klassen skydd mot obehörig avlyssning ska säkerställa att kommunikation är tillräckligt skyddad mot obehörig åtkomst via avlyssningsutrustning i de fall där godkänt signalskydd ej nyttjas.

3.2 Kravuppfyllnad

För att kunna applicera de funktionella säkerhetskraven på alla typer av IT-system är de uttryckta som krav på egenskaper som systemet skall uppvisa. Dessa konkretiseras genom kravkomponenterna som också anger till vilken funktionell nivå kravet skall uppfyllas. Kravkomponenternas formulering är dock inte direkt tillämpbara på alla typer av IT-system, varför ett system kan uppfylla de funktionella kraven på andra sätt än vad som anges av kravkomponenterna. Alla funktionella säkerhetskrav skall dock alltid vara uppfyllda till en nivå som motsvarar den som indikeras av kravkomponenterna. Eventuella alternativa sätt att uppfylla de funktionella säkerhetskraven skall dokumenteras i ITSS under avsnittet kravtolkning.

4 Assuranskrav

4.1 Inledning

Assuranskrav är krav på förtroende för systemets förmåga att tillhandahålla sin säkerhetsfunktionalitet. Assuranskraven indelas i olika klasser som täcker olika assuransområden och avkräver utföraren olika typer av underlag. ***Med stegrande kravnivå ställs ökande krav på underlagens omfattning, fullständighet och detaljeringsgrad***. Det är detta underlag som sedan ska verifieras under evalueringsprocessen.

4.2 Struktur för assuranskraven

I kategorin assuranskrav finns följande sju klasser av krav, vilka beskrivs detaljerat i underbilaga 4:

- IT-Säkerhetsspecifikation (SASS) – Eftersom det är en förutsättning för evaluering av övriga klasser av assuranskrav att systemets ITSS är riktig, komplett och konsistent, ställer denna klass krav som syftar till att säkerställa detta.
- Systemutvecklingens livscykel (SALC) – Klassen omfattar assuranskrav på säkerhetsrelevanta egenskaper i utvecklingsmiljön, så som fysisk miljö, komponenternas ursprung och processer för utveckling och underhåll i miljön där systemet utvecklas.
- Arkitektur och design (SADE) – Klassen omfattar assuranskrav på tekniska egenskaper i IT-systemets design och konstruktion, dvs. egenskaper hos systemet och dokumentationen av dem.
- Installation och drift (SAOP) – Klassen omfattar assuranskrav på dokumentation, processer och rutiner som används i driften och förvaltningen av systemet för att systemet skall fungera på ett säkert sätt.
- Administrativa rutiner (SARU) omfattar assuranskrav på den dokumentation som utvecklaren producerar och som beskriver hur systemets säkerhetsfunktioner ska administreras på ett korrekt sätt för att upprätthålla systemets IT-säkerhetsförmågor.
- Systemintegrationstest (SATS) – Klassen omfattar assuranskraven för systemtestning som visar att systemutvecklaren verifierat IT-säkerhetsfunktionaliteten hos systemet.
- Sårbarhetsanalys och Restriskanalys (SARA) – Klassen omfattar den sårbarhetsanalys som genomförs av evalueraren, till största delen baserat på underlag från andra assuransfamiljer.

4.3 Komponentassurans

Ett system består av en sammansättning av en eller flera IT-komponenter, där vissa tillför säkerhetsfunktionalitet. En IT-komponent är säkerhetsrelaterad om den används för att uppfylla en säkerhetsfunktion eller om den tillhandahåller funktionalitet som en säkerhetsfunktion är beroende av. Eftersom förtroendet för dessa IT-komponenters säkerhetsförmåga är avgörande för förtroendet för hela systemet ingår det i IT-systemets assuranskrav att fastställa vilka komponenter som för ett visst system är säkerhetsrelaterade. För övriga (icke säkerhetsrelaterade) komponenter krävs underlag motsvarande det som beskrivs i skrivelsen HKV 2007-08-23 10.750:72100[27], alternativt en komplett referens till sådana komponenter.
Den nivå av assurans som krävs av de säkerhetsrelaterade IT-komponenterna benämns komponentassuransnivå och beskrivs i fyra nivåer från Nivå 1 till Nivå 4 (N1-N4) där nivå 4 utgör den högsta nivån av komponentassurans. Processen[28] för att godkänna säkerhetsrelaterade IT-komponenter till viss komponentassuransnivå är en fristående process som ligger utanför KSF.

[27] HKV 2007-08-23 10.750:72100 *Sårbarhetsgranskning - Informell granskning av produkter före användning i Försvarsmaktens IT-system*
[28] Komponentassuransprocessen

I orienterande syfte beskrivs i nedanstående tabell den övergripande skillnaden mellan de olika nivåerna. Innehållet i nedanstående tabell ske ej förväxlas med specifika kravangivelser.

Nivå	Övergripande nivåskillnader mellan komponentassuransnivåer
N4	MUST kan godkänna produkter som helt syftar till att uppfylla IT-säkerhetskrav till N4. Utvecklingen av produkten skall ske enligt en formell projektmetod med tydliga avstämningspunkter, t.ex. MIL-STD-1521B. Dessutom måste MUST evaluera och godkänna kravställning, kravtolkning, arkitektur, utvecklingsplan, design, utvecklingsarbete, produkttestning och slutgiltiga leveransobjekt.
N3	MUST kan godkänna produkter vars funktionalitet helt eller till huvudsak syfta till att uppfylla IT-säkerhetskrav till N3. Alternativt kan produkten vara så modulärt uppbyggd att säkerhetsfunktionaliteten enkelt kan avgränsas och evalueras i enskildhet. Komponentutvecklaren ska bistå granskningen med allt granskaren behöver, såsom dokumentation och tillgång till relevanta resurser, t.ex. personal och testmiljö. Komponentutvecklaren ska visa att allt arbete med produkten styrs av en utförlig säkerhetsprocess som omfattar hela produktens livscykel.
N2	MUST kan godkänna IT-säkerhetsfunktioner i generella COTS-produkter till N2. För detta krävs att komponentutvecklaren tillhandahåller tillräcklig information till stöd för granskningen. Exempel på sådan information som kan krävas är ingående dokumentation av produkten, källkod till produkten, dokumentation av utvecklarens tester och rapporter från säkerhetsgranskningar utförda av tredje part. Komponentutvecklaren ska visa att produkten utvecklas och underhålls enligt en dokumenterad säkerhetsprocess som omfattar hela produktens livscykel.
N1	MUST kan godkänna IT-säkerhetsfunktioner i generella COTS-produkter till N1. För detta krävs tillräcklig dokumentation som definierar säkerhetsfunktionen och dess gränsytor. Beroenden av funktioner i och utanför produkten ska också beskrivas. Komponentutvecklaren ska visa prov på gott säkerhetsmedvetande i sitt hanterande av produktens livscykel.

Tabell 5: Övergripande skillnad mellan komponentassuransnivåer.

MUST verifierar IT-säkerhetsfunktionalitet i IT-komponenter och godkänner dem till någon av dessa fyra komponentassuransnivåer.

4.4 Fastställande av komponentassuransnivå

Kravet på komponentassuransnivå hos de säkerhetsrelaterade IT-komponenterna i ett system styrs av informationens högsta konsekvensnivå och systemets exponeringsnivå enligt tabellen nedan.

Konsekvensnivå	Exponeringsnivå			
	E1	**E2**	**E3**	**E4**
K5	N2	N3	N4	N4[29]
K4	N2	N2	N4	N4
K3	N2	N2	N3	N4
K2	N1	N2	N2	N3
K1	N1	N1	N1	N1

Tabell 6: Komponentassuransnivå

När olika säkerhetskomponenter i ett system är utsatta för olika exponering eller används för att skydda information som har olika konsekvensnivå så behöver inte komponentassuransnivån vara lika hög för alla ingående säkerhetskomponenter i systemet.
En säkerhetskomponent med lägre komponentassuransnivå kan användas om det går att visa att komponenten har en lägre exponering än systemets högsta, alternativt endast skyddar information på en lägre konsekvensnivå än systemets högsta. Detta kan kräva att det finns någon annan IT-säkerhetskomponent med högre komponentassuransnivå som garanterar detta. Även vissa egenskaper i systemets arkitektur kan medge användning av komponenter med lägre komponentassuransnivå.
Systemutvecklaren ska identifiera systemets säkerhetsrelaterade komponenter. Om en komponent med lägre komponentassuransnivå än vad som ges av tabellen ovan används i systemet ska systemutvecklaren påvisa varför detta ej påverkar säkerheten negativt. Detta ska dokumenteras i ITSS och kommer att granskas och värderas under evalueringen av systemet.

Exempel 1. Komponent av hög assurans ger lägre exponering
Ett system har en arkitektur som medger en uppdelning i två delar. All kommunikation mellan dessa delar sker via ett filter som endast släpper igenom textfiler. Den ena delen har en större mängd användare och exponering E4. Den andra delen har endast ett fåtal användare som alla är behöriga till all information som behandlas där. Då skulle komponenterna som implementerar skydd mot

[29] För vissa typer av säkerhetsfunktioner räcker inte komponentassuransnivå N4 för att möta denna extrema exponering, system som kräver detta bör alltid diskuteras med MUST då tillkommande åtgärder kan komma att krävas.

skadlig kod i det mindre systemet kunna tilldelas den komponentassuransnivå som ges av exponeringsnivå E2.
Komponentassuransnivån för andra komponenter i systemet skulle inte kunna sänkas i detta fall. Exempelvis skulle komponenterna som realiserar behörighetskontrollen fortfarande ha exponeringsnivå E4, då filtret i detta exempel inte kan avgöra vem som får skicka vilka textfiler genom det.
I båda fallen måste filtret ha en komponentassuransnivå som motsvarar exponeringsnivå E4. Dessutom måste en analys göras som säkerställer att all trafik verkligen går igenom filtret och att det inte finns några andra vägar in för skadlig kod.

Exempel 2. Information på högre konsekvensnivå hålls i separat del av system
Information på hög konsekvensnivå hålls i en separat del av systemet och skyddas av en komponent som endast släpper ut information på lägre konsekvensnivå. Komponentassuransnivån för komponenterna i det övriga systemet skulle då kunna sänkas med motivet att de inte hanterar informationen på den högre konsekvensnivån.
Kravnivån på IT-systemet som helhet och komponenten som implementerar skyddet av informationen på den högre konsekvensnivån kommer att styras av informationen på den högsta konsekvensnivån och inte kunna sänkas.
För att nå en effektiv arkitektur kan systemet och dess skyddsfunktioner designas och placeras på ett sådant sätt att man kan påvisa att information med högst skyddsbehov endast kommer hanteras och skyddas av komponenter som uppfyller tillräckligt höga krav för detta ändamål. På så sätt når man en systemarkitektur anpassad efter verksamheten där inte den högsta konsekvensnivån slår mot alla delar av systemet och därigenom når ett kostnadseffektivt skydd.

Exempel 3. Systemarkitekturen påverkar exponering
Även egenskaper i systemarkitekturen kan påverka komponentassuransnivån. Ett system kan vara kopplat till två andra system med olika exponeringsnivå och skyddas av två olika intrångsskyddskomponenter mot respektive system.
Enligt metoden för fastställande av komponentassuransnivå skulle komponenten som implementerar intrångsskydd mot det lägre exponerade systemet kunna ha en lägre komponentassuransnivå än det andra intrångsskyddet.

Ert tjänsteställe, handläggare | Ert datum | Er beteckning

Vårt tjänsteställe, handläggare | Vårt föregående datum | Vår föregående beteckning

Christian Fenger-Krog, 08-788 88 62,
christian.fenger-krog@mil.se

2012-09-24 | 10 750:64354

Beslut om krav på godkända säkerhetsfunktioner version 3.1 (KSF v3.1)

(1 bilaga och 4 underbilagor)

Bakgrund

KSF utgör de krav som ska vara uppfyllda för de godkända säkerhetsfunktioner som IT-system i Försvarsmakten ska vara försedda med enligt 7-11 kap. Försvarsmaktens interna bestämmelser om IT-säkerhet (FIB 2006:2)[1].

I KSF v2.0 kravställdes godkända säkerhetsfunktioner utifrån om uppgifterna som ett IT-system hanterade var placerade i informationssäkerhetsklass eller inte och vilken informationssäkerhetsklass uppgifterna i så fall var placerade i. Med KSF v3.0 reviderades denna grundsyn för att ge ett bättre och mer balanserat skydd jämfört med v2.0, med hänsyn tagen även till den situation som IT-systemet ska användas i. Målet med KSF v3.0 var följande:

- Uppnå bättre anpassning mot dimensionerande hot, främst genom uppdaterade krav.
- Uppnå bättre möjlighet att balansera skyddsåtgärder, främst genom en modell där även IT-systemets exponering påverkar kraven.
- Uppnå ökad användarvänlighet.
- Möjliggöra ökad tid- och kostnadseffektivitet för Försvarsmakten, främst genom att underlätta återanvändning av komponenter.

[1] Författningen ändrades genom FIB 2010:2 (tillika omtryck).

KSF version v3.0[2] tillämpades fram till 2014-06-30 för vissa utvalda IT-system.

Versionsförändringar

Den största förändringen mellan v3.1 och v3.0 är att v3.1 nu ska användas för alla nya IT-system/IT-tjänster inom Försvarsmakten. Förändringarna i v3.1 är annars små och mest av språklig karaktär.

Utbildning

En förutsättning för att KSF ska ge avsedd effekt är att det finns en grundläggande förståelse för hur KSF är avsett att användas och vad som ska uppnås. Utbildning i KSF kommer initialt att bedrivas som ett samarbete mellan MUST och FMV. Information om KSF-utbildningar kommer att skickas ut via separata skrivelser.

Förvaltning

KSF är ett regelverk som förutom att ge ett skydd för Försvarsmaktens informationstillgångar även i stor utsträckning påverkar kostnads- och tidsaspekter för Försvarsmaktens IT-system/IT-tjänster. KSF måste därför aktivt förvaltas och utvecklas för att hela tiden ge så stor effekt som möjligt med minsta möjliga resursåtgång. Kravmassan måste förändras i takt med omvärlden så att kraven möter hoten på en väl avvägd nivå.

För att säkerställa detta kommer förvaltningen av KSF att under hösten 2014 formaliseras för att på ett strukturerat sätt kunna hantera regelbundna förändringar över tiden.

Stöd och återkoppling

För att MUST ska kunna ge stöd vid användningen av KSF samt för att KSF-intressenter ska kunna ge synpunkter inför kommande versioner av KSF har en funktionsbrevlåda KSF-support@mil.se inrättats.

[2] Beslut om krav på godkända säkerhetsfunktioner version 3.0 (KSF v3.0), HKV 2012-09-24 10 750:64354

Beslut

Med stöd av 7 kap. 3 § andra stycket, 8 kap. 1 § andra stycket, 9 kap. 1 §, 10 kap. 1 § andra och tredje stycket och 11 kap. 1 § andra stycket Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet[3] beslutas att godkänna KSF v3.1 att gälla inom Försvarsmakten för alla nya IT-system/IT-tjänster. Beslut om vilka IT-system/IT-tjänster som klassas som nya fattas i samband med auktorisation av den som är bemyndigad att fatta auktorisationsbeslut. IT-system/IT-tjänster som under övergångsperioden använt KSF v3.0 ska nu använda KSF v3.1. För de IT-system/IT-tjänster som inte faller inom dessa kategorier får KSF v2.0 fortfarande tillämpas.

Detta beslut har fattats av generalmajor Gunnar Karlson. I den slutliga handläggningen har dessutom deltagit överste Mattias Hanson, sektionschef Ulrika Evertsson Hansson och som föredragande Christian Fenger-Krog.

Karlson, Gunnar

Chef för militära underrättelse- och säkerhetstjänsten

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.
Christian Fenger-Krog

[3] Författningen ändrades genom FIB 2010:2 (tillika omtryck)

Sändlista

Som orientering

Regeringskansliets Förvaltningsavdelning, Enheten för Beredskap och Säkerhet
Försvarsexportmyndigheten
Försvarsunderrättelsedomstolen
Statens inspektion för försvarsunderrättelseverksamheten
Säkerhetspolisen
Fortifikationsverket
Försvarshögskolan
Försvarets materielverk (varav 1 ex avsett för CSEC)
Försvarets radioanstalt
Myndigheten för samhällsskydd och beredskap
Totalförsvarets forskningsinstitut
Rekryteringsmyndigheten

Inom Försvarsmakten
LG, I 19, K 3, P 4, P 7, A 9, Lv 6, Ing 2, LedR, TrängR,
1. ubflj, 3. sjöstriflj, 4. sjöstriflj, Amf 1, MarinB,
F 7, F 17, F 21, Hkpflj,
FMLOG, FMTM, SOG,
MHS K, MHS H, MSS, SSS, LSS, HvSS, FMTS, SWEDEC, SkyddC,
FMUndSäkC,
FM HRC, FömedC

Inom HKV
LEDS
INS
PROD
MUST
JURS
HKV AVD

KSF

Krav på IT-säkerhetsförmågor hos IT-system

v3.1

Ordlista och definitioner av begrepp

INNEHÅLLSFÖRTECKNING

1 Ordlista

Denna ordlista definierar termer inom informationssäkerhetsområdet som direkt eller indirekt relaterar till KSF. Terminologin ska i största möjliga mån ansluta till den terminologi som redan används inom Försvarsmakten, EU, NATO samt i svensk och internationell standard (SIS respektive ISO/IEC) inom området.

1.1 Referenser

Som utgångspunkter för val av termer används följande referenser.

Ref	Titel/Beteckning
Säkerhetsskydds-lagen	Säkerhetsskyddslagen (1996:627)
FFS 2010:1	Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.)
FFS 2005:2	Försvarsmaktens föreskrifter (FFS 2005:2) om signalskyddstjänsten inom totalförsvaret
FIB 2006:2	Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet.
Försvarsmaktens informations-säkerhetspolicy	HKV 2005-04-05 10 700:65482 Beslut om FM informationssäkerhetspolicy
KSF	KSF, krav på IT-säkerhetsförmågor
Försvarsmaktens IT-styrmodell	(HKV skr HKV 2011-10-31 09 100:64970)
H SÄK Infosäk	Handbok Säkerhetstjänst Informationssäkerhet, 2013
H SÄK IT	Handbok Säkerhetstjänst Informationsteknologi, 2006, Ändring 1, 2008
HB 550	Terminologi för Informationssäkerhet, SIS HB 550, Utgåva 3

1.2 Begrepp och definitioner

I kolumnen ”Term” står den rekommenderade termen i fet stil. Sedan följer eventuella synonymer, akronymer, förkortningar, var och en på en ny rad och även de i fet stil. I kolumnen ”Engelska” anges motsvarande engelskspråkig term. Därefter följer en definition av det begrepp som termer eller termerna står för.

Term	Engelska	Definition
ackreditering		Dels ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633), dels ett godkännande från säkerhetssynpunkt i övrigt av övriga IT-system.
angrepp	*offensive operation [attack]*	Samordnade aktiviteter syftande till att skada en motståndare eller dennes resurser.
användare	*user*	Person som nyttjar informationstillgångar.
användningsmönster; användarmönster	*user behaviour*	Karakteristiska särdrag hos en användares beteende i ett system.
assurans	*assurance*	Tillit till att ett systems eller en produkts säkerhetsfunktioner uppfyller specificerade krav.
assuranskrav		De krav i KSF på åtgärder och underlag som ska säkerställa att säkerhetsmålen uppfyllts på ett tillräckligt och effektivt sätt
assuransnivå	*assurance level*	Grad av assurans.
autenticitet	*authenticity*	Äkthet avseende uppgivna uppgifter; särskilt rörande påstådd identitet och meddelandes ursprung och innehåll.
autentisering; autenticering	*authentication*	Verifiering av uppgiven identitet eller att meddelandes riktighet.
avvikelsedetektering	*Anomaly detection*	Upptäckt genom registrering av onormalt beteende.
behörighet	*permission; privilege*	Rättighet för en användare att använda informationstillgångar på ett specificerat sätt.
behörighetskontroll		Administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att kontrollera en användares identitet, styra en användares behörighet att använda IT-systemet och dess resurser samt registrera användaren.
behörighetstilldelning	*authorization*	Fastsällande av åtkomsträttigheter för en användare till olika systemresurser.
beställare		De som beslutar, beställer och finansierar en IT-tjänst. Beställaren är ansvarig för verksamhet eller sakområde enligt FM ArbO.
C MUST		Chef för den militära underrättelse- och säkerhetstjänsten i Högkvarteret.
CIO		Försvarsmaktens chief information officer

Term	Engelska	Definition
COTS	*Commercial Off The Shelf*	Kommersiell hyllvaruprodukt
data	*data*	Representation av fakta, begrepp eller instruktioner i form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
definierat säkert tillstånd		Fördefinierat tillstånd där IT-systemet fungerar på avsett vis under kontrollerade former. I det säkra tillståndet anges vilka subjekt, objekt och operationer på objekt som är tillåtna.
distribuerade komponenter		Komponenter som exekverar i fysiskt eller virtuellt åtskilda maskiner
driftmiljö		Ett IT-systems omgivningar och förutsättningar för dess användning
dubellkommando	*dual control*	Metod innebärande att två personer måste samverka för att utföra en operation
elektroniskt kommunikationsnät		System för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.
evaluerare		Den som är ansvarig för genomförandet av en evaluering.
evaluering		Verifiering av ett IT-systems IT-säkerhetsegenskaper genom aktiviteter såsom granskning av dokumentation, källkod och konfiguration, testning av IT-systemets IT-säkerhetsfunktionalitet och granskning av miljön där utveckling av IT-systemet äger rum.
exponering		Mått på hur stora möjligheter hotaktörer har att interagera med ett IT-system.
funktionella säkerhetskrav		De krav i KSF som ska implementeras av IT-systemet dess operativa miljö eller båda i samverkan för att uppfylla säkerhetsmålen
förstärkt inloggning		En av MUST godkänd autentisering som inte enbart förlitar sig på lösenord. Nyttjande av TEID ska eftersträvas. Se HKV 2007-03-27 12 830:65517.
GOTS	*Government Off The Shelf*	Hyllvaruprodukt för myndigheter
granskning		Aktivitet som genomförs för att avgöra lämpligheten, tillräckligheten och verkan hos det aktuella objektet för att uppnå fastställda mål.
grundskydd	*baseline protection; baseline controls*	Lägsta rekommenderade skyddsnivå för system eller organisation.
hemlig uppgift		Uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets

Term	Engelska	Definition
		säkerhet.
hot	*threat*	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten. Hoten avser såväl aktörsdrivna som icke aktörsdrivna.
hotanalys	*threat analysis*	Identifiering av vilka hot som kan finnas och vem eller vad som tänkas utlösa dessa hot, samt vilka resurser samt vilken tid och kompetens som en angripare kan tänkas disponera.
hotbild	*threat profile*	Uppsättning hot som bedöms föreligga mot en viss [typ av] verksamhet.
identitet; identitetsbeteckning	*identity*	Unik beteckning för en viss entitet (person, process, fysisk enhet eller liknande) i ett visst system.
incident, IT-säkerhetsrelaterad		En händelse i eller kring ett IT-system där IT-säkerheten, det vill säga sekretess, tillgänglighet, riktighet eller spårbarhet, har eller skulle kunna påverkas negativt.
incident; tillbud	*incident*	Händelse som potentiellt kan få eller kunnat få allvarliga konsekvenser för verksamheten.
information	*information*	Innebörd av data.
informationssäkerhet	*information security (INFOSEC)*	Med informationssäkerhet avses inom Försvarsmakten följande: • att informationen finns tillgänglig när den behövs, • att informationen är och förblir riktig, • att informationen endast är tillgänglig för dem som är behöriga att ta del av och använda den, samt • att hanteringen av informationen är spårbar
informationssäkerhetsklass		Försvarsmaktens indelning av hemliga och utrikesklassificerade uppgifter (se H Säk Sekrbed del A, kapitel 4).
intrång; penetration	*intrusion; penetration*	Oönskad interaktion med system i strid med systemets policy som kan medföra förändring, störning eller skada.
intrångsdetektering		Administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att detektera förberedelse eller försök till intrång samt intrång.
intrångsskydd		Administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att skydda IT-system mot obehörig åtkomst från datanät.
IT-komponent		Del av ett IT-system

Term	Engelska	Definition
IT-system		System med teknik som hanterar och utbyter information med omgivningen.
IT-system		Ett system med teknik som hanterar och utbyter information med omgivningen, i KSF används oftast ordet system synonymt med IT-system.
IT-säkerhet	*IT security*	Med IT-säkerhet avses i Försvarsmakten åtgärder som syftar till att uppnå och vidmakthålla den nivå av säkerhet som krävs på ett IT-system.1
IT-säkerhetsfunktionalitet		Funktionalitet i ett IT-system som uppfyller eller bidrar till att uppfylla ett IT-säkerhetskrav på IT-systemet
IT-säkerhetsförmåga		Förmåga hos ett IT-system att upprätthålla den nivå av IT-säkerhet som krävs av IT-systemet för att tillräckliga skyddsåtgärder ska anses föreligga
IT-säkerhetskomponent		En IT-komponent som implementerar IT-säkerhetsfunktionalitet som del av ett IT-system
IT-säkerhetskrav		Beskrivning av en delmängd av krävd IT-säkerhetsförmåga hos IT-systemet
IT-säkerhetsspecifikation		Dokument som innehåller den fullständiga kravbilden gällande IT-säkerhetskrav på ett IT-system och hur dessa krav uppfylls av IT-systemet och/eller dess operativa miljö. Innehåll och form för detta dokument kravställs i KSF bilaga 2
kommunikation		Överföring av information via elektroniskt kommunikationsnät eller via flyttbart lagringsmedium
komponent		Del av IT-system, se IT-komponent
komponentassuransnivå		Graderingen av de krav MUST ställer vid godkännande av IT-säkerhetsfunktionalitet i en IT-komponent. Benämns N1 t.o.m. N4.
konsekvens; påverkan	*consequence; impact*	Resultat av händelse med negativ inverkan.
koordinerare		De som ansvarar för att sammanställa och koordinera kravställningen på IT-tjänster. Koordineraren ansvarar också för att inrikta, beställa och följa upp produktionen av IT-tjänster. Ansvarig för sakområde IS/IT och informations-infrastruktur är också ansvarig för koordineringen.
korrekthet	*correctness*	Vid realisering av säkerhetsfunktion, egenskapen att en komponents egenskaper, och dess beskrivning i olika abstraktionsnivåer/ beskrivningsnivåer, överensstämmer mes specificerade säkerhetskrav.
krav		Behov eller förväntning som är angiven, i allmänhet underförstådd eller obligatorisk

[1] Sidan 13, Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik (H SÄK IT), 2006 års utgåva, ändring 1 2008.

Term	Engelska	Definition
kravnivå		Gradering av krav som KSF ställer för att uppfylla säkerhetsmålen i en säkerhetsfunktion. Benämns Grund, Utökad och Hög.
kryptografisk funktion		Metoder och principer för att skydda uppgifter mot insyn med hjälp av kryptering eller för identifiering och autenticering samt äkthetskontroll av meddelanden.
KSF		MUST krav på tillräckliga IT-säkerhetsförmågor hos IT-system
kvalitet		Grad till vilken inneboende egenskaper uppfyller krav.
kvarstående risk	*residual risk*	Risk med hänsyn tagen till den sårbarhet som återstår efter införande av valda skyddsåtgärder.
lagringsmedium		Permanent minnesmedium som används för att kunna lagra och läsa uppgifter.
leverans		En leverans kan bestå av varor och/eller tjänster. En leverans är en specificerad mängd av vara/tjänst, uttryckt i antal/belopp, som är knuten till ett visst datum.
logg	*audit trail; log*	(Kontinuerligt) insamlad information om de operationer som utförs i ett system.
lösenord	*password*	Teckensträng som anges vid identifiering av användare.
manipulering (vid överföring)	*manipulation (of communication)*	Obehörig förändring av överförda data eller meddelanden.
mål		Ett mål beskriver ett önskat resultat eller tillstånd vid en viss framtida tidpunkt.
normalisera (loggar)		Att sammanföra loggar från olika källor (och med olika format) så att de blir indexerbara via ett antal olika attribut t.ex. tid, källa, händelsetyp, subjekt, objekt.
nyttjare		De som använder IT-tjänsterna i verksamheten.
oavvislighet; oförnekbarhet	*non-repudiation*	Skyddsmål att en handling inte i efterhand ska kunna förnekas av utföraren.
obehörig åtkomst	*unauthorised access*	Åtkomst av system, resurs eller annat objekt i strid med gällande säkerhetspolicy.
objekt		Ett objekt är något ett subjekt kan utföra en operation på. Ett objekt kan t.ex. vara information, funktionalitet, IT-system, en databas, en fil eller en dator.
revokering		Återkallande av tidigare utfärdat säkerhetsattribut
riktighet	*data integrity*	Skyddsmål att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning.
risk	*risk*	Ett hot som har bedömts avseende sannolikheten för att

Term	Engelska	Definition
		det inträffar samt vilket men (skada) hotet förorsakar under förutsättning att det har inträffat.
riskanalys	*risk analysis*	Process som identifierar hot mot verksamheten och uppskattar storleken hos relaterade risker.
riskhantering	*risk management*	Samordnade aktiviteter för identifiering, styrning och kontroll av risk.
rollbaserad åtkomstkontroll		Att definiera användarroller i systemet, och att tilldela användare dessa roller istället för att tilldela individuella behörigheter till varje användare.
rollbaserad åtkomstkontroll	*Role-based access control (RBAC)*	Åtkomstkontroll som utgår ifrån i vilken eller vilka roller som en användare kan nyttja ett system.
röjande signaler (RÖS)	*compromising emanations; compromising emissions*	Icke önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs.
sekretess	*confidentiality*	Skyddsmål att innehållet i ett informationsobjekt inte får göras tillgängligt eller avslöjas för obehöriga.
sekretess		Avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga.
sekretessbelagd uppgift		Uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).
sekretessklassificerad uppgift		Uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), men som inte rör rikets säkerhet och som inte är en utrikesklassificerad uppgift.
signalskydd	*communications security*	Förhindra obehörig insyn i och påverkan av telekommunikationer, samt användning av kryptografiska funktioner i IT-system,
skadlig kod		Otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett datanät eller funktioner eller uppgifter i ett IT-system.
skalskyddsklass		Klassificering av elektromagnetiskt skärmade utrymmen med avseende på RÖS-egenskaper. Klasserna benämns SS1 och SS2.
skydd	*protection*	Effekt av handlingar, rutiner och tekniska arrangemang som syftar till att minska sårbarheten.
specifikation		Dokument som anger krav.
spårbarhet	*traceability*	Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en användare.
stark autentisering		En av MUST godkänd autentisering som använder kryptografiska algoritmer på separat medium. Nyttjande av TAK ska eftersträvas. Se HKV 2007-03-27 12 830:65517.

Term	Engelska	Definition
subjekt	*subject*	En entitet i ett IT-system som kan utföra en åtgärd. Ett subjekt kan t.ex. vara IT-systemets representation av en användare, en process eller en dator.
system		se IT-system
systemutvecklare		De som är ansvarig för leveransen av ett visst IT-system. När ett IT-system är sammansatt av färdiga IT-komponenter brukar systemutvecklaren ofta kallas systemintegratör.
sårbarhet	*vulnerability*	Brist i skyddet av en tillgång exponerad för hot.
sårbarhetsanalys	*vulnerability analysis*	Process som identifierar en organisations sårbarhet.
sårbarhetsanalys, teknisk	*vulnerability analysis*	Process som identifierar svagheter i ett system eller i en produkt.
säkerhet	*security*	Egenskap eller tillstånd som innebär skydd mot rik för oönskad insyn, förlust eller påverkan; oftast i samband med medvetna försök att utnyttja eventuella svagheter.
säkerhet	*safety*	Egenskap eller tillstånd som innebär skydd mot skada för liv och lem (personsäkerhet).
säkerhetsadministratör	*security administrator*	Person med ansvar för att säkerhetsregler inom en säkerhetsdomän upprätthålles på ett korrekt sätt.
säkerhetsanalys		Identifiering och prioritering av skyddsvärda tillgångar, bedömning av säkerhetshot, sårbarheter och risker samt prioritering och hantering av risker inklusive beslut om skyddsåtgärder (se H Säk Skydd, kapitel 10).
säkerhetsarkitektur	*security architecture*	Övergripande teknisk beskrivning av i ett system ingående säkerhetstjänster inklusive samverkan och gränssnitt mellan olika komponenter.
säkerhetsattribut	*security attribute*	Säkerhetsrelaterad parameter som hör till ett visst informationsobjekt eller en viss användaridentitet.
säkerhetsfunktion	*security function*	En eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet ska skyddas.
säkerhetsfunktion		Samlingsbegrepp för ett antal relaterade IT-säkerhetsegenskaper som kravställs i KSF funktionella krav
säkerhetskopia; backup; reservkopia	*back-up [copy]*	Kopia av informationsmängd som skapats för att kunna utnyttjas vid förlust av hela eller delar av den ursprungliga informationsmängden.
säkerhetslogg	*security audit trail*	Logg över säkerhetskritiska händelser.
säkerhetslogg	*security audit trail*	Behandlingshistorik över händelser som är av betydelse för säkerheten i eller kring ett IT-system.
säkerhetsloggning		Manuell eller automatisk registrering, eller både manuell och automatisk registrering, av händelser som är av betydelse för säkerheten i eller kring ett IT-

Term	Engelska	Definition
		system.
säkerhetsmål	*security objectives*	Beskrivning av i vilka avseenden säkerheten ska tillgodoses för ett system eller en komponent.
säkerhetsmål		En formulering av IT-säkerhetsegenskaper som KSF kräver av ett IT-system. Alla säkerhetsmål måste vara uppfyllda till den av KSF fastställda nivån för att ett IT-system ska anses uppfylla KSF krav på IT-säkerhetsegenskaper.
säkerhetsmålsättning		”Dokumenterade analyser avseende vilket skydd ett IT-system kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt)
säkerhetsprövning		Det arbete som genomförs innan t ex en anställning i syfte att, ur säkerhetsskyddssynpunkt, erhålla en så god personkännedom som möjligt.
säkerhetsrelaterad IT-komponent		En IT-säkerhetskomponent eller annan IT-komponent som IT-säkerhetskomponenten är beroende av för sin IT-säkerhetsfunktion
säkert tillstånd		Säkert tillstånd avser principen ”fail-safe”, d.v.s. om säkerhetsfunktionen ej fungerar ska den neka åtkomst
tillgänglighet	*availability*	Skyddsmål där informationstillgångar ska kunna utnyttjas i förväntad utsträckning och inom önskad tid.
tillkommande funktionella krav		De krav på IT-säkerhet som ett IT-system måste upfylla, men som kravställs utanför KSF (ex. via författningskrav eller hot-,risk-,sårbarhets-analys)
trafikdata		Information som beskriver observerad trafik i exempelvis elektroniskt kommunikationsnät men inte nödvändigtvis dess fullständiga innehåll
unik referens		Unik identifiering av data och/eller information genom namn eller nummer vilket medger indexering för att skapa tillgång till önskad data/information. Detta kan ske genom att nyttja kombinationer av unika sidnummer, dokumentnummer, versionsnummer, volymsnummer och datum.
utförare		De som producerar och tillhandahåller IT-tjänster. Ett annat sätt att uttrycka det är att de är leverantörer. HKV Intern organisationsenhet inom Försvarsmakten som erhåller uppdrag att leverera hel eller del av IT-tjänst benämns intern utförare, exempel är FMLOG eller FMTM. Andra myndigheter, företag och organisationer som via avtal förbinder sig att leverera hel eller del av IT-tjänst benämns extern leverantör, exempel är FMV eller industrin.
utrikesklassificerad uppgift		En uppgift som av en utländsk myndighet eller mellanfolklig organisation eller av en svensk myndighet har klassificerats i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED eller motsvarande och som är sekretessbelagd enligt 15 kap. 1 § offentlighets- och

Term	Engelska	Definition
		sekretesslagen men som inte rör rikets säkerhet.
utrustningsklass		Klassificering av IT-utrustning med avseende på RÖS-egenskaper. Klasserna benämns U1, U2 och U3.
validering		Bekräftelse genom att framlägga belägg för att krav för en specifik, avsedd användning eller tillämpning har uppfyllts.
verifiering	*verification*	Fastställande av riktighet av något, med avseende på specifikation.
åtkomst	*access*	Interaction mellan ett subjekt och ett objekt som resulterar i överföring av information emellan eller utnyttjande av resurser. Rättigheter för användare att nå eller påverka objekt i ett system.
åtkomstkontroll	*access control*	Funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till olika resurser.
åtkomsträttigheter	*access rights*	Behörigheter till åtkomst. T.ex. Subjekt A har tilldelats åtkomsträttigheterna skapa, läsa och skriva till objekt B.

KSF

Krav på IT-säkerhetsförmågor hos IT-system

v3.1

IT-systemets säkerhetsspecifikation (ITSS)

INNEHÅLLSFÖRTECKNING

1 Allmän strategi

1.1 Syftet med ITSS

IT-systemets säkerhetsspecifikation (ITSS) specificerar vilka IT-säkerhetsförmågor systemet ska ha, och på vilket sätt och i vilken miljö det skall användas för att systemet skall anses vara tillräckligt säkert samt hur systemets säkerhetsfunktioner och driftmiljö samverkar för att säkerställa dessa IT-säkerhetsförmågor. För att nå detta mål måste:

- IT-systemets arkitektur, dess driftmiljö samt dess logiska och fysiska gränser beskrivas.
- IT-systemets funktionella säkerhetskrav och assuranskrav identifieras utifrån KSF säkerhetsmodell genom att värdera systemets konsekvensnivå och exponering.
- Tillkommande säkerhetskrav identifieras utifrån verksamhetskrav, identifierade hot och risker samt författningskrav.
- Säkerhetskrav för systemets driftmiljö identifieras utifrån verksamhetskrav, identifierade hot och risker samt författningskrav**.** Om vissa KSF-krav hävdas vara helt eller delvis uppfyllda genom att utnyttja egenskaper i omgivningen ska även detta dokumenteras som säkerhetskrav för systemets driftmiljö.
- Säkerhetsfunktioner som fullständigt uppfyller systems säkerhetskrav dokumenteras.

1.2 Avsedd användning

ITSS kan användas under kravdefiniering, utveckling, evaluering och ackreditering av systemet samt när systemet tas i drift. ITSS blir därmed en gemensam säkerhetsspecifikation för olika parter så som beställare, utförare, evaluerare och nyttjare.

- Kravdefiniering

  Försvarsmakten (beställaren) ska använda ITSS för att ha den samlade bilden av säkerhetskraven för systemet och dess miljö, och därmed vara säker på att utföraren delar den samlade bilden och att den verifieras av evalueraren. Säkerhetskravbilden består av tillämpliga KSF-krav och andra tillkommande säkerhetskrav samt påföljande säkerhetskrav på systemets driftmiljö.
- IT-systemets utveckling

  Utföraren ska implementera alla identifierade säkerhetskrav för systemet och dokumentera i ITSS hur dessa krav uppfylls.
- Ackreditering

  Evalueraren ska verifiera att system uppfyller sin ITSS. Evalueraren ska verifiera att ITSS är riktig, komplett, tydlig och icke motsägelsefull samt att den motsvarar den faktiska kravbilden.
- Drift

Försvarsmakten ska förvalta ITSS och dokumentera hur säkerhetskravbilden som beskrivs i ITSS påverkas över tiden[1]. ITSS och särskilt säkerhetskraven för systemets driftmiljö ska utgöra underlag för framtagandet av lokala rutiner och instruktioner för systemets drift- och förvaltningspersonal.

2 ITSS obligatoriskt innehåll

Det obligatoriska innehållet i en ITSS presenteras i Figur 1 "ITSS struktur". Varje kapitel i ITSS beskrivs i korthet nedan och beskrivs mer utförligt i de följande underkapitlen.

- I *Inledning* ska ITSS och systemet unikt identifieras och referenser till KSF och eventuella andra dokument eller säkerhetsstandarder som systemet skall uppfylla. *Inledning* ger också en övergripande och korrekt högnivåbeskrivning av systemet.
- I *Systembeskrivning* ges en utförlig beskrivning av systemet. I beskrivningen definieras systemets förutsättningar, arkitektur, gränsytor samt säkerhetsförmågor.
- I *Sammanställning av säkerhetskrav* beskrivs säkerhetskrav för systemet. Dessa säkerhetskrav identifieras utifrån KSF säkerhetsmodell samt säkerhetsanalys, verksamhetsanalys, hot-, risk-, och sårbarhetsanalys och författningsanalys för det specifika systemet.
- I *Säkerhetskrav på omgivningen* beskrivs säkerhetskrav som ställs på systemets driftmiljö. Dessa säkerhetskrav identifieras utifrån säkerhetsanalys, verksamhetsanalys, hot-, risk-, och sårbarhetsanalys och författningsanalys för det specifika systemet. KSF-krav kan hävdas vara helt eller delvis uppfyllda genom att utnyttja egenskaper hos systemets driftmiljö och detta dokumenteras som säkerhetskrav för systemets driftmiljö.
- I *Tolkning av säkerhetskrav* beskrivs en sammanställd kravbild för systemet. För alla funktionella säkerhetskrav som dokumenterats i kapitlet *Sammanställning av säkerhetskrav* beskrivs hur dessa appliceras på det specifika systemet. Säkerhetskraven på systemets driftmiljö refereras till om vissa KSF-krav kan hävdas vara, helt eller delvis, uppfyllda genom att utnyttja egenskaper hos den driftmiljön.
- I *Uppfyllande av säkerhetskrav* ges en komplett högnivåbeskrivning av de säkerhetsåtgärder som implementerats i systemet. Det visas också hur dessa åtgärder uppfyller de specifika säkerhetskraven för systemets säkerhetsfunktioner.

[1] Beskrivning av och krav på en eventuell ITSS förvaltning ingår inte i KSF.

2.1 Inledning

2.1.1 Syfte

I *Inledning* ges en övergripande och korrekt högnivåbeskrivning av systemet.

Syftet med detta kapitel är att ge en översiktlig beskrivning av systemet. En översikt över systemet ska innehålla information om systemets tänkta användning och dess säkerhetsfunktionalitet system.

Beskrivningen av hur ITSS uppfyller olika säkerhetskrav och regelverk ska uttryckas klart och tydligt i detta kapitel. Detta är viktigt av följande skäl:

- läsaren ska kunna identifiera (spåra) kraven,
- utföraren ska kunna visa att systemet har byggts med avseende på specifika säkerhetskrav och
- evalueraren ska kunna avgöra om säkerhetskraven är uppfyllda

2.1.2 Innehåll och presentation

Kapitlet ska ge en översikt över systemet ur följande aspekter:

(a) **ITSS referens:**

ITSS ska innehålla en tydlig referens som unikt identifierar ITSS. En typisk referens kan innehålla titel, version, författare och publiceringsdatum t.ex. “ITSS, v1.2 för system XYZ, Utvecklat av Abc AB, 2014-06-09”.

(b) **IT-systemreferens**

ITSS ska också innehålla en systemreferens som unikt identifierar systemet. IT-systemets referens skall vara densamma som används i Försvarsmaktens IT-process.

(c) **Dokumentreferenser**

ITSS ska innehålla referenser till KSF och andra styrande dokument och internationella standarder. Referenserna ska visa att ITSS på ett acceptabelt sätt representerar KSF-krav, styrande dokument, internationella standarder (t.ex. FIPS 180-3, RFC 425) samt andra säkerhetsstandarder (t.ex. EU-direktiv, NATO-standarder) som systemet skall uppfylla.

Dokumentreferenser i ITSS ska referera till den exakta version av dokumentet och eventuell kravnivå som systemet ska uppfylla, t.ex. “KSF v3.1 Kravnivå U”.

Det bör också specificeras om systemet eller dess IT-komponenter uppfyller alla säkerhetskrav som finns i standarden eller endast uppfyller standarden till vissa delar (t.ex. FIPS 180-3 endast för SHA-256”).

(d) **Systemöversikt**

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

Den tänkta driftmiljön för systemet ska också beskrivas. Varje teknisk eller miljöfaktor som systemet är beroende av ska tas med i beskrivningen.

2.2 Systembeskrivning

2.2.1 Syfte

Systembeskrivning ger en utförlig beskrivning av systemet. Beskrivningen ska ge de som ackrediterar systemet och systemets nyttjare samt drift och förvaltning en djupare förståelse för säkerhetsförmågan i systemet än vad som ges i kapitlet *Inledning*.

Systembeskrivning beskriver systemets förutsättningar, arkitektur, gränsytor samt säkerhetsförmågor:

- Säkerhetsrelevant information kring systemets förutsättningar måste redovisas så att den rätta kravnivån för systemet ska kunna fastställas, därmed måste följande framgå:
  - avsedd användning av systemet, d.v.s. det verksamhetsstöd det erbjuder
  - hur dess driftmiljö är beskaffad, t.ex. vad gäller fysiskt skydd av systemet
  - vilka de tänkta användarna av systemet är
  - vilken information som lagras, överförs och bearbetas i systemet
- IT-systemets arkitektur ska lista alla komponenter och beskriva hur de tillsammans bygger upp systemet.
- IT-systemets alla logiska och fysiska gränsytor ska beskrivas för att ge en bild av den attackyta de utgör.
- IT-systemets säkerhetsförmågor ska beskrivas på en detaljnivå som är tillräcklig för att ge läsaren en allmän förståelse för dessa. Beskrivningen förväntas vara mer detaljerad än den som ges i kapitlet *Inledning.*

När systemets arkitektur och säkerhetsförmågor beskrivs är det av yttersta vikt att det tydligt framgår vilka delar som tillhör systemet och vilka som är externa beroenden.

2.2.2 Innehåll och presentation

Systembeskrivning består av fyra delar: förutsättningar, arkitektur, gränsytor och säkerhetsförmågor.

(a) **Förutsättningar**

För att beskriva systemets förutsättningar är det nödvändigt att definiera

- Avsedd användning av systemet

  Detta är en redogörelse för den tänkta användningen av systemet ur användarens perspektiv i termer av bearbetning, lagring och överföring av information.
- Systemets driftmiljö

  Här ska systemets placering i den driftmiljön beskrivas med information om

fysiskt skydd, tillträdesbegränsning och andra förutsättningar som är säkerhetsrelevanta

- Tänkta användare av systemet

  I denna del ska systemets tänkta användare beskrivas. Alla användarroller i systemet ska redovisas och eventuell gruppering av användare efter åtkomst till resurser och information ska identifieras. För varje användarroll ska dess nivå av tillgång till systemets olika säkerhetsfunktioner och andra säkerhetsrelevanta tillgångar listas. Antalet användare i varje roll och grupp ska också bedömas så att läsaren förstår systemets omfattning.

- Information

  Typ av information, mängd, skyddsvärde, sekretessklassning, eventuella andra hanteringsregler (t.ex. från lagkrav) kring information som lagras, bearbetas, överförs i eller utförs ut ur systemet. En hänvisning till systemets säkerhetsanalys skall också ges.

(b) **Systemets arkitektur**

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

Arkitekturbeskrivningen ska identifiera systemets komponenter och beskriva hur de samverkar. Informationen ska presenteras på en sådan detaljnivå att läsaren får en allmän kunskap om hur systemet fungerar och vilka generella informationsflöden som finns.

(c) **Systemets gränsytor**

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

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

(d) **Säkerhetsförmågor**

Medan systemarkitekturen beskriver systemets uppbyggnad och vilka komponenter som ingår i systemet, beskrivs här systemets säkerhetsförmågor och de säkerhetsfunktioner som systemet tillhandahåller. Säkerhetsförmågorna ska beskrivas på en detaljnivå som är tillräcklig för att ge läsaren en allmän förståelse.

2.3 Sammanställning av säkerhetskrav

2.3.1 Syfte

Syftet med *Sammanställning av säkerhetskrav* är att identifiera de säkerhetskrav som gäller för systemet. Säkerhetskraven kan delas in i två kategorier:

- KSF-krav

I KSF säkerhetsmodell tas hänsyn till systemets konsekvensnivå och exponering för att komma fram till en kravnivå. KSF säkerhetsmodell beskrivs i KSF huvuddokument, kapitel 2.

- Tillkommande säkerhetskrav

Tillkommande säkerhetskrav är sådana krav som har identifieras utanför KSFs säkerhetsmodell, t.ex. som resultat av olika obligatoriska analyser som genomförts. Dessa analyser kan identifiera ytterligare säkerhetskrav som ställs på systemet eller dess driftmiljö. De säkerhetskrav som ställs på systemet ska dokumenteras i detta kapitel medan de säkerhetskrav som måste uppfyllas av systemets driftmiljö ska dokumenteras i kapitlet *Säkerhetskrav på omgivningen*.

2.3.2 Innehåll och presentation

Sammanställning av säkerhetskrav består av två delar: KSF-krav och tillkommande säkerhetskrav.

(a) **KSF-krav**

KSF-kraven definierar två typer av säkerhetskrav: funktionella säkerhetskrav och assuranskrav.

För att identifiera KSF-kraven som gäller för ett system behöver metoden för fastställande av kravnivå appliceras. Denna metod beskrivs i KSF huvuddokument, kapitel 3. Kravnivåerna som används i KSF är:

- Grundläggande IT-säkerhetsskydd (G)
- Utökad IT-säkerhetsskydd (U)
- Högt IT-säkerhetsskydd (H)

Resultatet från fastställandet av kravnivå ska dokumenteras och alla kravkomponenter som följer av kravnivån ska listas under detta kapitel.

(b) **Tillkommande säkerhetskrav**

Tillkommande säkerhetskrav härrör från analyser utanför KSF säkerhetsmodell. Metoder för genomförandet av dessa analyser ingår inte i KSF. Metoder för genomförandet av verksamhets- och säkerhetsanalys beskrivs i H SÄK Infosäk[2]. Metoder för hot-, risk- och sårbarhetsanalys beskrivs i Försvarsmaktens gemensamma riskhanteringsmodell[3]. Även andra analyser kan resultera i säkerhetskrav på systemet, t.ex. från flygsäkerhetskrav, behandling av personuppgifter eller andra regelverk och författningar.

Dessa analyser ska identifiera mätbara säkerhetsmål för systemet eller för dess miljö som erhålls utifrån identifierade hot, verksamhetskrav och författningskrav. Dessa säkerhetsmål för systemet ska jämföras med säkerhetskrav som härrör från KSF och dokumenteras som tillkommande säkerhetskrav. Om säkerhetsmålen redan täcks av säkerhetskrav i KSF, ska referens till detta säkerhetskrav

[2] Handbok Säkerhetstjänst Informationssäkerhet 2013 M7739-352056)
[3] Försvarsmaktens gemensamma riskhanteringsmodell 2009 M7739-350012

dokumenteras. Säkerhetsmål som identifierats för systemets miljö ska även listas som krav i kapitlet *Säkerhetskrav på omgivningen*.

2.4 Säkerhetskrav på omgivningen

2.4.1 Syfte

Syftet med *Säkerhetskrav på omgivningen* är att identifiera de säkerhetskrav som ställs på systemets driftmiljö. Dessa krav kan uppstå då KSF-krav uppfylls med säkerhetsmekanismer i systemets omgivning men kan också identifieras genom analyser utanför KSF säkerhetsmodell.

Dessa analyser identifierar säkerhetsmål för systemet och dess miljö. Säkerhetsmål för systemet redovisas i det tidigare kapitlet *Sammanställning av säkerhetskrav*.

Vissa KSF-krav, eller kravkomponenter, kan hävdas vara helt eller delvis uppfyllda genom att förlita sig på egenskaper hos systemets driftmiljö. Dessa kan vara såväl fysiska, administrativa samt organisatoriska åtgärder. De åberopade åtgärderna kommer därefter att utgöra säkerhetskrav på systemets driftmiljö.

2.4.2 Innehåll och presentation

Identifierade säkerhetsmål tillsammans med åtgärder i operativ miljö och eventuella KSF-krav, eller kravkomponenter, som därmed anses uppfyllda ska dokumenteras.
Dokumentationen bör innehålla en lista över alla de säkerhetskrav som systemets driftmiljö måste uppfylla, så att denna kan användas för verifikation vid systemets driftsättning.

2.5 Tolkning av säkerhetskrav

2.5.1 Syfte

Syftet med *Tolkning av säkerhetskrav* är att beskriva en sammanställd kravbild för systemet och att genomföra och dokumentera kravtolkning utifrån de säkerhetskrav som identifierades i kapitlet *Sammanställning av säkerhetskrav*.
Kraven i KSF formuleras på en allmän nivå som resulterar i att varje system behöver precisera dessa krav med en tolkning av hur kravet appliceras på systemet.
Analyserna som beskrivs i kapitlet *Säkerhetskrav på omgivningen* kan identifiera att vissa KSF-krav kan hävdas vara uppfyllda genom att utnyttja egenskaper i systemets driftmiljö. Om KSF-krav, eller kravkomponenter, ska uppfyllas genom säkerhetskrav på omgivningen ska referens till säkerhetskrav på omgivningen anges i kravtolkningen.

2.5.2 Innehåll och presentation

Tolkning av säkerhetskrav ska beskriva en sammanställd kravbild för systemet.

Alla säkerhetskrav ska dokumenteras i syfte att ta fram en sammanställd kravbild i ITSS. Kravbilden ska användas som grund för systemdesign som ska realisera de ställda säkerhetskraven.

Följande kravtolkningar medges:

- Precisering

Precisering innebär att säkerhetskrav som dokumenteras i kapitlet *Sammanställning av säkerhetskrav* ska beskrivas i termer applicerbara på ett specifikt system. Ett preciserat krav ska vara mer strikt än det ursprungliga KSF-kravet.

- Referens till säkerhetskrav på omgivningen

Referens till säkerhetskrav på omgivningen ska anges för de KSF-krav, eller kravkomponenter, som kan hävdas vara uppfyllda genom att utnyttja egenskaper i systemets driftmiljö. Dessa krav identifieras i kapitlet *Säkerhetskrav på omgivningen*.

2.6 Uppfyllande av säkerhetskrav

2.6.1 Syfte

Syftet med *Uppfyllande av säkerhetskrav* är att ge en beskrivning av hur systemet uppfyller säkerhetskraven som ställs på systemet. Den ska innehålla en beskrivning av vilka komponenter och säkerhetsfunktioner som uppfyller de funktionella säkerhetskraven på systemet. Hur assuranskraven uppfylls behöver inte beskrivas. Inte heller de funktionella kraven som uppfylls av systemets miljö behöver beskrivas.

Informationen ska presenteras på en sådan detaljnivå att läsaren kan förvissa sig om hur alla funktionella säkerhetskrav uppfylls.

Identifieringen av KSF-krav och tillkommande säkerhetskrav beskrivs i kapitlet *Sammanställning av säkerhetskrav*. Hur dessa identifierade KSF-kraven preciseras för ett specifikt system beskrivs i kapitlet *Tolkning av säkerhetskrav*.

2.6.2 Innehåll och presentation

Uppfyllande av säkerhetskrav ska visa hur alla krav listade i kapitlet *Tolkning av säkerhetskrav* är uppfyllda av systemet. Detta sker genom att beskriva den säkerhetsfunktionalitet i systemet som syftar till att uppfylla varje krav. Evalueraren ska utifrån denna beskrivning, och med stöd av *Systembeskrivningen*, kunna förvissa sig om att alla säkerhetskrav är fullständigt uppfyllda av systemet.

Om en komponent med lägre komponentassuransnivå än vad som ges av systemets konsekvensnivå och exponeringsnivå (se kapitel 4 i huvuddokumentet) används i systemet skall detta särskilt motiveras och utföraren måste tydligt visa att detta inte kan påverka systemets säkerhet negativt.

KSF

Krav på IT-säkerhetsförmågor hos IT-system

v3.1

Funktionella säkerhetskrav

INNEHÅLLSFÖRTECKNING

1. Funktionella säkerhetskrav

KSF definierar följande klasser av funktionella säkerhetskrav:

- Gemensamma krav (SFGK) – Funktionella säkerhetskrav som är gemensamma för alla säkerhetsfunktioner. Samtliga säkerhetsfunktioner i IT-systemet ska omfattas av, men inte begränsas till, dessa krav.
- Behörighetskontroll (SFBK) – Kraven i klassen behörighetskontroll ska förhindra åtkomst till IT-systemets subjekt och objekt av användare och subjekt som inte har behörighet och åtkomsträttigheter i IT-systemet. Dessutom ska de säkerställa att alla användare kan göras individuellt ansvariga för vidtagna åtgärder i IT-systemet.
- Intrångsdetektering (SFID) – Kraven i klassen intrångsdetektering ska säkerställa att pågående samt redan genomförda intrång i IT-systemet kan upptäckas och åtgärdas.
- Intrångsskydd (SFIS) – Kraven i klassen intrångsskydd ska förhindra all åtkomst till IT-systemets subjekt och objekt av sådana subjekt som inte har åtkomsträttigheter till IT-systemet.
- Skydd mot skadlig kod (SFSK) – Kraven i klassen skydd mot skadlig kod ska säkerställa att skadlig kod inte kan införas, utöva påverkan på, eller spridas via IT-systemet.
- Säkerhetsloggning (SFSL) – Kraven i klassen säkerhetsloggning ska säkerställa att spårning av missbruk, och försök till missbruk av IT-systemet kan genomföras.
- Skydd mot röjande signaler (SFRS) – Kraven i klassen skydd mot röjande signaler ska säkerställa att hemlig information som behandlas i IT-systemet inte oavsiktligt röjs via strålning och läckande signaler.
- Skydd mot obehörig avlyssning (SFOA) – Kraven i klassen skydd mot obehörig avlyssning ska säkerställa att kommunikation som inte omfattas av signalskydd har ett tillräckligt skydd mot obehörig åtkomst via avlyssningsutrustning.

1.1. SFGK - Gemensamma krav på säkerhetsfunktioner

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.

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 då kunna försättas i ett definierat säkert tillstånd.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFGK_FEL.	**1**	**2**	**3**	**4**
Grund	X	X		
Utökad	X	X	X	
Hög	X	X	X	X

SFGK_FEL.1

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.2

Ett definierat säkert tillstånd ska upprätthållas tills normal drift har återupptagits.

SFGK_FEL.3

Ett definierat säkert tillstånd ska upprätthållas för de delar av systemet som berörs när hela eller delar av säkerhetsfunktionens funktionalitet är korrupt eller oåtkomlig. Detta innebär att fel i funktionalitet måste kunna upptäckas, t.ex. via självtester.

SFGK_FEL.4

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_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

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFGK_TID.	**1**	**2**	**3**
Grund	X	X	
Utökad	X	X	X
Hög	X	X	X

SFGK_TID.1

Systemgemensam tillförlitlig tid ska finnas tillgänglig.

SFGK_TID.2

Säkerhetsfunktioner ska använda den systemgemensamma tiden.

SFGK_TID.3

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.

1.2. SFBK – Behörighetskontroll

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.

SFBK_UID – Subjekt 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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFBK_UID.	**1**	**2**
Grund	X	X
Utökad	X	X
Hög	X	X

SFBK_UID.1

Alla subjekt ska i systemet ha en unik identitet.

SFBK_UID.2

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_AUT – Autentisering av subjekt 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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFBK_AUT.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Grund	X	X	X	X	X	X	X	X	X	X	X	X	X							
Utökad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
Hög	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X

SFBK_AUT.1

Subjekt ska autentiseras vid inloggning och upprättande av session.

SFBK_AUT.2

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.3

Det ska finnas möjlighet till tidsbegränsning av sessioner.

SFBK_AUT.4

Subjekt ska tvingas återautentisera sig när tiden för en tidsbegränsad session har gått ut.

SFBK_AUT.5

Säkerhetsattribut som används för autentisering ska ha en längsta giltighetstid.

SFBK_AUT.6

Säkerhetsfunktionen ska minst använda lösenord eller motsvarande som säkerhetsattribut för autentisering.

SFBK_AUT.7

Kvaliteten på säkerhetsattribut för autentisering ska kunna kontrolleras, exempelvis genom tvingande komplexitetskrav vid tilldelning och byte av lösenord.

SFBK_AUT.8

Systemet ska ha funktioner för att kunna revokera säkerhetsattribut.

SFBK_AUT.9

Säkerhetsattribut får inte överföras i klartext vid autentisering.

SFBK_AUT.10

Säkerhetsattribut ska ha skydd mot obehörig avläsning och modifikation när dessa lagras eller transporteras i systemet.

SFBK_AUT.11

Systemet ska ha möjlighet att reagera på upprepade felaktiga autentiseringsförsök, även sådana där den angivna identiteten förändras mellan försöken.

SFBK_AUT.12

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.13

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.14

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.15

Systemet ska skydda en inloggad session så att den inte kan nyttjas av obehörig.

SFBK_AUT.16

Sessioner ska omfattas av tidsbegränsning.

SFBK_AUT.17

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.18

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.19

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.20

All aktivitet som systemet genomför för en användares räkning ska knytas till den genom stark autentisering fastställda identiteten.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFBK_ÅTK.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Grund	X	X	X	X			
Utökad	X	X	X	X	X	X	
Hög	X	X	X	X	X	X	X

SFBK_ÅTK.1

Subjekts unika och genom autentisering fastställda identitet ska alltid användas vid åtkomstkontroll till objekt.

SFBK_ÅTK.2

Endast subjekt med tilldelad åtkomsträttighet ska ges åtkomst till objekt.

SFBK_ÅTK.3

Funktioner för administration av säkerhetsfunktionalitet ska förses med behörighetskontroll.

SFBK_ÅTK.4

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.5

Det ska finnas möjlighet till märkning av ett objekt med skyddsvärde för styrning av åtkomst.

SFBK_ÅTK.6

Märkningen av objekt med skyddsvärde ska ha minst lika starkt integritetsskydd som alla andra säkerhetsattribut som styr åtkomst till objektet.

SFBK_ÅTK.7

Märkning av objekt med skyddsvärde ska användas vid styrning av åtkomst.

SFBK_ADM - Administration av behörighetskontroll ska ske 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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFBK_ADM.	**1**	**2**	**3**	**4**	**5**	**6**
Grund	X					
Utökad	X	X	X			
Hög	X	X		X	X	X

SFBK_ADM.1

Det ska gå att lägga till, ta bort och förändra vilka åtkomsträttigheter som subjekt har till systemets objekt.

SFBK_ADM.2

Systemet ska kunna åtkomstkontrollera administration av säkerhetslogg, daglig drift och tilldelning av åtkomsträttigheter separat så att rollseparation av dessa sysslor medges.

SFBK_ADM.3

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.4

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.5

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.6

Rollerna för administration av behörighetskontroll och administration av säkerhetslogg ska inte kunna tilldelas samma person.

1.3. SFSL – Säkerhetsloggning

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.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSL_REG.	**1**	**2**	**3**	**4**	**5**	**6**
Grund	X	X	X	X		
Utökad	X	X	X	X	X	
Hög	X	X	X	X	X	X

SFSL_REG.1

Alla händelser som är av betydelse för säkerheten i systemet ska registreras i säkerhetsloggen.

SFSL_REG.2

Datum och tid ska registreras för varje loggad händelse. Se SFGK_TID.

SFSL_REG.3

Subjektets unika identitet ska registreras för varje loggad händelse. Avser såväl användare som övriga subjekt. Se SFBK_UID.

SFSL_REG.4

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.5

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.6

Registrerade händelser ska minst omfatta:

- konfigurationsförändringar i systemet

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSL_OAV.	**1**	**2**	**3**
Grund			
Utökad	X		
Hög	X	X	X

SFSL_OAV.1

Alla förändringar till placering i informationssäkerhetsklass samt förändringar gällande märkning av objekt med skyddsvärde ska bindas till användaren med en oavvislighetsmekanism.

SFSL_OAV.2

Förändringar till mjukvarufiler och relevanta konfigurationer som omfattas av riktighetskontroll enligt SFSK_INT.4 ska bindas till användaren med en oavvislighetsmekanism.

SFSL_OAV.3

Export av skyddsvärd information från systemet, inklusive utskrifter på papper, ska bindas till användaren med en oavvislighetsmekanism.

SFSL_SKY - Säkerhetsloggar ska ej kunna förvanskas eller förstöras

För att garantera möjligheten till spårning behöver säkerhetsloggar skyddas mot avsiktliga eller oavsiktliga förändringar, förluster eller raderingar.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSL_SKY.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Grund	X	X	X				
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SFSL_SKY.1

Händelseposter som registrerats i säkerhetsloggar ska inte kunna förändras.

SFSL_SKY.2

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.3

Säkerhetsloggen ska kunna säkerhetskopieras.

SFSL_SKY.4

Säkerhetsloggar ska lagras åtskilda från driftsloggar.

SFSL_SKY.5

En reserverad yta för lagring av säkerhetsloggar ska finnas i systemet.

SFSL_SKY.6

Registrerade händelser får inte raderas eller skrivas över som en följd av fel på säkerhetsfunktionen eller att säkerhetsloggen är full.

SFSL_SKY.7

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_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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSL_ANA.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Grund	X	X	X	X	X	X	X	X			
Utökad	X	X	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X	X	X

SFSL_ANA.1

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.2

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.3

Det ska vara möjligt att överföra säkerhetsloggar till externt IT-system. Formatet på överförda loggar ska vara väl specificerat.

SFSL_ANA.4

Säkerhetsloggar från flera olika komponenter ska kunna sammanföras och analyseras i analysverktyget.

SFSL_ANA.5

Analysverktyget ska kunna upptäcka kända attackmönster.

SFSL_ANA.6

Analysverktyget ska medge tillägg och anpassningar av attackmönster.

SFSL_ANA.7

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.8

Analysverktyget ska kunna sortera samt söka på alla definierade attribut för registrerade händelser.

SFSL_ANA.9

Alla registrerade händelser i systemet ska sammanföras och normaliseras innan analys.

SFSL_ANA.10

Automatiska återkommande analyser ska vara möjliga att konfigurera i analysverktyget.

SFSL_ANA.11

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.

1.4. SFIS – Intrångsskydd

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.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFIS_HRD.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Grund	X	X					
Utökad	X	X	X	X			
Hög	X	X	X	X	X	X	X

SFIS_HRD.1

Samtliga funktioner som inte stöder systemets primära syfte ska vara avstängda.

SFIS_HRD.2

Ingående delar i systemet ska konfigureras enligt tillverkarens rekommendationer för säker konfiguration. Om sådana inte finns ska av IT-säkerhetsbranchen vedertagna rekommendationer för säker konfiguration av komponenttypen användas.

SFIS_HRD.3

Mjukvarutjänster ska förhindras från att kunna påverka varandra eller övriga systemet med hjälp av existerande funktioner för behörighetskontroll.

SFIS_HRD.4

Säkerhetskänsliga funktioner som inte används, t.ex. sådana som utgör tillgänglig attackyta, ska tas bort ur systemet.

SFIS_HRD.5

Funktioner för att försvåra utnyttjandet av potentiella sårbarheter i mjukvara ska implementeras i systemet.

SFIS_HRD.6

Alla mjukvarutjänster ska vara isolerade från varandra och övriga systemet genom upprätthållandet av en restriktiv resursåtkomstpolicy.

SFIS_HRD.7

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_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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFIS_INT.	**1**	**2**	**3**	**4**	**5**
Grund	X				
Utökad		X	X	X	
Hög			X	X	X

SFIS_INT.1

All säkerhetsrelaterad eller skyddsvärd information ska skyddas mot manipulation vid kommunikation mellan distribuerade komponenter i systemet.

SFIS_INT.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.3

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.4

Vid kommunikation mellan distribuerade komponenter i systemet ska motparten autentiseras. Undantag kan medges för kommunikation som krävs för att göra autentiseringsmekanismerna åtkomliga.

SFIS_INT.5

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_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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFIS_KIN.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Grund	X	X	X	X				
Utökad	X	X	X	X	X	X		
Hög	X	X		X	X	X	X	X

SFIS_KIN.1

Systemets indatakontroller ska minst omfatta:

- Godkända tecken
- Rimligheten hos datastorlekar
- Att uppgifter ligger inom rimliga gränsvärden
- Kodning av teckensträngar
- Kodning av datastrukturer

SFIS_KIN.2

Information ska inte accepteras av systemet utan att säkerhetsfunktionens kontroller används.

SFIS_KIN.3

De kontroller som görs ska vara på applikationsprotokollnivå.

SFIS_KIN.4

Information som ett subjekt får som gensvar vid fel eller nekande av åtkomst ska begränsas.

SFIS_KIN.5

Applikationsprotokollet ska begränsas så att endast den delmängd som krävs för korrekt operation tillåts.

SFIS_KIN.6

Säkerhetsfunktionen ska kontrollera att applikationsprotokollets syntax följer en väl definierad grammatik.

SFIS_KIN.7

Information som passerar in i systemet ska kunna märkas med skyddsvärde.

SFIS_KIN.8

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_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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFIS_KUT.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Grund	X	X					
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SFIS_KUT.1

All informationsöverföring från systemet ska kontrolleras och vara möjlig att begränsa.

SFIS_KUT.2

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.3

Applikationsprotokollet ska begränsas så att endast den delmängd som krävs för korrekt operation tillåts.

SFIS_KUT.4

Säkerhetsfunktionen ska kontrollera att datakommunikationens användning av applikationsprotokollet följer en väl definierad grammatik.

SFIS_KUT.5

Säkerhetsfunktionen ska kontrollera rimligheten hos mängden utgående data över tid.

SFIS_KUT.6

Befintlig märkning av data med skyddsvärde ska upprätthållas och tas hänsyn till vid utförsel.

SFIS_KUT.7

Ett meddelande ska bara kunna överföras till system som tillåts hantera uppgifter med lägst samma skyddsvärde som meddelandet.

1.5. SFID – Intrångsdetektering

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.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFID_DAT.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Grund	X	X	X	X	X	X	X	X		
Utökad	X	X	X	X	X	X	X		X	X
Hög	X	X	X	X	X	X	X		X	X

SFID_DAT.1

Alla säkerhetsloggar ska göras tillgängliga för analys.

SFID_DAT.2

Trafikdata från relevant kommunikation mellan komponenter i systemet ska göras tillgängligt för analys.

SFID_DAT.3

Trafikdata från all kommunikation över systemets gränsytor ska göras tillgängligt för analys.

SFID_DAT.4

Registrerade systemhändelser, t.ex. driftloggar, ska göras tillgängliga för analys.

SFID_DAT.5

Applikationshändelser ska göras tillgängliga för analys.

SFID_DAT.6

Alla händelseposter ska innehålla datum och tid. Se SFGK_TID.

SFID_DAT.7

Alla händelseposter som kan härledas till ett subjekt ska innehålla detta subjekts unika identitet.

SFID_DAT.8

Information som gjorts tillgänglig för analys får inte skrivas över, ändras, eller förstöras innan analys genomförts.

SFID_DAT.9

Information som gjorts tillgänglig för analys ska överföras till en systemgemensam analys- och detekteringsfunktion.

SFID_DAT.10

Information som gjorts tillgänglig för analys får inte skrivas över, ändras, eller förstöras innan den överförts till analys- och detekteringsfunktionen.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFID_ANA.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Grund	X	X	X	X	X	X	X	X						
Utökad	X	X	X	X	X	X	X	X	X	X	X	X	X	
Hög	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SFID_ANA.1

Verktygsbaserad analys av allt tillgängliggjort data ska vara möjlig.

SFID_ANA.2

Analyserna ska kunna upptäcka kända attackmönster.

SFID_ANA.3

Analysfunktionen ska kunna kontinuerligt uppdatera signaturer för kända attackmönster.

SFID_ANA.4

Verktyget ska medge tillägg och anpassningar av attackmönster vid analys.

SFID_ANA.5

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.6

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.7

Verktyget ska ge möjlighet att sortera och söka i händelser på alla definierade attribut.

SFID_ANA.8

All tillgängliggjort data ska i verktyget kunna presenteras i läsbar form.

SFID_ANA.9

All tillgängliggjort data ska sammanföras och analys ska göras på den samlade mängden.

SFID_ANA.10

Tillgängliggjort data ska normaliseras innan analys.

SFID_ANA.11

Automatiska analyser ska ske fortlöpande då nytt data tillgängliggörs.

SFID_ANA.12

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.13

All tillgängliggjort data, analysresultat och åtgärder som vidtagits ska kunna överföras hel eller i delar till en extern miljö.

SFID_ANA.14

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.

1.6. SFSK – Skydd mot skadlig kod

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.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSK_UPD.	**1**	**2**	**3**	**4**	**5**
Grund	X	X	X		
Utökad	X	X	X	X	
Hög	X	X	X		X

SFSK_UPD.1

Systemet ska kunna rapportera exakt programvaruversion för alla i systemet ingående komponenter och dess mjukvarudelar.

SFSK_UPD.2

Systemet ska kunna uppdateras med säkerhetsuppdateringar. Införande av säkerhetsuppdateringar bör ske automatiskt så snart dessa finns tillgängliga.

SFSK_UPD.3

Systemet ska för alla uppdateringar kunna verifiera paketets integritet och säkerställa dess autenticitet innan de accepteras för införande.

SFSK_UPD.4

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.5

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_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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSK_RIK.	**1**	**2**	**3**	**4**
Grund	X	X		
Utökad	X	X	X	
Hög	X	X	X	X

SFSK_RIK.1

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.2

Vid återställning av säkerhetskopior ska riktigheten hos kopiorna verifieras.

SFSK_RIK.3

Riktigheten hos alla mjukvarufiler och relevanta konfigurationer ska verifieras automatiskt när behörig administratör påkallar.

SFSK_RIK.4

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_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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSK_EXE.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Grund	X	X	X	X	X	X	
Utökad	X	X	X	X	X	X	
Hög	X	X	X	X	X	X	X

SFSK_EXE.1

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.2

Objekt ska kontrolleras innan de accepteras för användning.

SFSK_EXE.3

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.4

Vid detektering av potentiellt skadlig kod ska behörig administratör kunna notifieras.

SFSK_EXE.5

Säkerhetsfunktionen ska regelbundet kunna uppdatera kontrollmekanismerna för skyddet mot skadlig kod.

SFSK_EXE.6

System ska för alla uppdateringar av kontrollmekanismerna och dess styrande data verifiera paketets integritet och säkerställa att de kommer från betrodd utgivare.

SFSK_EXE.7

Endast sådan kod som tillhör systemet och vars riktighet verifierats ska accepteras för exekvering. Se SFSK_RIK.4.

SFSK_KUT - Skadlig kod ska ej kunna spridas via systemet

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

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSK_KUT.	**1**	**2**
Grund	X	X
Utökad	X	X
Hög	X	X

SFSK_KUT.1

All information som förs ut ur systemet ska genomsökas efter potentiellt skadlig kod.

SFSK_KUT.2

Vid detektering av potentiellt skadlig kod ska aktuell överföring kunna avbrytas.

SFSK_KIN - Skadlig kod ska ej 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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFSK_KIN.	**1**	**2**	**3**	**4**
Grund	X	X		
Utökad	X	X	X	X
Hög	X	X	X	X

SFSK_KIN.1

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.2

Vid detektering av potentiellt skadlig kod ska aktuell överföring kunna avbrytas.

SFSK_KIN.3

Det ska gå att kontrollera och styra vilka objekttyper och dataformat som accepteras för införsel i systemet.

SFSK_KIN.4

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.

1.7. SFRS – Skydd mot röjande signaler (RÖS)

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 läckage[1]. Skyddet kan realiseras av systemets komponenter, den lokal där systemet befinner sig eller båda i kombination.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFRS_REG.	**1**	**2**
Grund	X	X
Utökad	X	X
Hög	X	X

SFRS_REG.1

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.2

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.

[1] För närmare beskrivning av problematiken kring RÖS se skriften FMV:AK Led 10 755:818/2009 *Broschyr RÖS* med beteckning M7773-001851.

1.8. SFOA – Skydd mot obehörig avlyssning

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.

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SFOA_KBL.	**1**	**2**	**3**	**4**
Grund	X	X		
Utökad	X	X	X	
Hög	X	X		X

SFOA_KBL.1

Kablar, i vilka information placerad i informationssäkerhetsklass HEMLIG/RESTRICTED eller högre sänds utan godkänt signalskydd ska förläggas inom inhägnat och bevakat område.

SFOA_KBL.2

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.3

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.4

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.

KSF

Krav på IT-säkerhetsförmågor hos IT-system

v3.1

Assuranskrav

INNEHÅLLSFÖRTECKNING

1 Assuransmodell för IT-system

Syftet med assuranskraven är att få förtroende för att systemet uppfyller de IT-säkerhetsförmågor som KSF ställer krav på. Detta uppnås genom att försäkra sig om:

- förtroende för systemutvecklaren och dennes utvecklingsprocesser,
- förtroende för arkitekturen, designen och implementation av säkerhetsfunktionerna,
- förtroende för att drift- och förvaltningsdokumentation är korrekt och fullständig,
- genom sårbarhetsanalys och riskanalys påvisa att systemet, för den tänkta användningen, har tillräckliga IT-säkerhetsförmågor.

Assuranskraven har två aspekter:

- Först krävs underlag från systemutvecklaren som beskriver design, tester och administrativa rutiner, samt underlag som visar att dessa rutiner tillämpas och att tester har utförts.
- Därefter granskas detta underlag av evaluerare som kontrollerar om underlaget är fullständigt, tydligt och icke motsägelsefullt. Därefter analyseras systemet av evaluerare, genom bl.a. testning, för att hitta eventuella sårbarheter. Eventuella kvarstående risker identifieras och beskrivs, så att de vid en ackreditering kan bedömas vara acceptabla eller ej.

Modellen bygger på att systemet är sammansatt av komponenter med kända säkerhetsförmågor samt redovisar eventuella osäkerheter. Modellen förlitar sig på att dessa säkerhetsförmågor är kända och dokumenterade genom processer som verifierat dessa komponenter.

Nedan följer en sammanfattning av de olika assuransklasserna:

- Förtroende för IT-säkerhetsspecifikationen (SASS) omfattar assuranskrav på ITSS[1]. SASS ställer krav på ITSS format och innehåll för att säkerställa att ITSS är riktig, komplett, tydlig och icke motsägelsefull för att kunna vara en lämplig specifikation för ett system som ska uppfylla KSF.
- Systemutvecklingens livscykel (SALC) omfattar assuranskrav på säkerhet i utvecklingsmiljö. Med utvecklingsmiljö avses här den miljö där systemet utvecklats, eller integrerats, inte den miljö där ingående komponenter utvecklats. Detta sker genom att ställa krav på beskrivning av systemutvecklarens kontroll av de ingående komponenterna samt andra

[1] Systemets IT-säkerhetsspecifikation

säkerhetsåtgärder i utvecklingsmiljön. Den ställer krav på versions- och konfigurationshantering, livscykelmodell för systemutvecklingen, systemets leverans till drift- och förvaltning samt hur systemutvecklaren tar hand om upptäckta säkerhetsrelaterade brister i systemet eller dess komponenter.

- Arkitektur och design (SADE) omfattar assuranskrav på säkerhetsarkitekturen och på beskrivningar av hur komponenter tillhandahåller säkerhetsfunktionalitet. Detta sker genom att ställa krav på en arkitekturbeskrivning som ska visa hur de olika komponenterna samverkar för att tillhandahålla den samlade säkerhetsfunktionaliteten i systemet. Designen ska också beskriva hur skyddsvärd information flödar i systemet så att man kan verifiera att den kan skyddas. Designen ska också visa hur systemet förhindrar att säkerhetsfunktionaliteten kan kringgås eller manipuleras. Slutligen ska arkitekturen och designen visa vilka externa gränsytor som finns mot omgivningen och till vilken grad systemet förlitar sig på den driftmiljön.
- Installation och drift (SAOP) omfattar assuranskrav på dokumentation, processer och rutiner som används när drift- och förvaltning ska installera och förvalta systemet. Detta sker genom att ställa krav på beskrivning av den tänkta hanteringen som säkerställer att systemet har blivit leveranskontrollerad och installerat i sin driftmiljö enligt systemutvecklarens instruktioner. Assuranskraven omfattar också krav på dokumentation som ska innehålla all information som är nödvändig för att systemet ska kunna användas och underhållas på ett säkert sätt.
- Administrativa rutiner (SARU) omfattar assuranskrav på den dokumentation som systemutvecklaren producerar och som beskriver hur systemets säkerhetsfunktioner ska administreras på ett korrekt sätt för att upprätthålla systemets IT-säkerhetsförmågor
- Systemintegrationstest (SATS) omfattar assuranskrav på systemutvecklarens testning. Detta sker genom att ställa krav på beskrivning av genomförda tester som ska visa att det finns testfall för alla funktionella krav och säkerhetsfunktioner. Funktionstester ska visa att testerna genomförts och att resultatet dokumenterats korrekt.
- Riskanalys och sårbarhetsanalys (SARA) omfattar assuranskrav på identifiering och dokumentering av eventuella avvikelser, sårbarheter och kvarstående risker för att kunna bedöma och hantera dem. Detta sker genom att ställa krav på systemutvecklarens beskrivning av identifierade avvikelser. Dessutom ska en sårbarhetsanalys utföras av evaluerare visa att inga identifierade sårbarheter kan utnyttjas. Eventuella kvarstående risker som identifierades av evalueraren under riskanalysen ska dokumenteras.

2 Assuranskrav

2.1 SASS – Systemets IT-säkerhetsspecifikation

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.

Klassen SASS består av sex krav:

- Inledning (SASS_INL) omfattar ITSS kapitlet *Inledning* för att säkerställa att inledning entydigt identifierar en viss version av ITSS, och refererar till en specifik version av system och version av KSF, samt att den innehåller en övergripande och korrekt högnivåbeskrivning av systemet.
- Systembeskrivning (SASS_SYS) omfattar ITSS kapitlet *Systembeskrivning* för att säkerställa att systembeskrivningen ska ge en detaljerad beskrivning av systemet och att den information som användas för att fastställa kravnivå utifrån KSF säkerhetsmodellen finns dokumenterad.
- Sammanställning av säkerhetskrav (SASS_KRV) omfattar ITSS kapitlet *Sammanställning av säkerhetskrav* för att säkerställa att alla säkerhetskrav som gäller för systemet är identifierade korrekt utifrån KSF-modellen eller utifrån andra externa krav.
- Säkerhetskrav på omgivningen (SASS_OMG) omfattar ITSS kapitlet *Säkerhetskrav på omgivningen* för att säkerställa att alla säkerhetskrav för systemets miljö är identifierade och beskrivna.
- Tolkning av säkerhetskrav (SASS_TOL) omfattar ITSS kapitlet *Tolkning av säkerhetskrav* för att säkerställa att beskrivningen visar en komplett kravbild för systemet och ange kravtolkningen utifrån de KSF-krav som identifierades i ITSS kapitlet *Sammanställning av säkerhetskrav*.
- Uppfyllande av säkerhetskrav (SASS_UPF) omfattar ITSS *Uppfyllande av säkerhetskrav* för att säkerställa att alla funktionella säkerhetskrav som identifierats hanteras av systemet.

SASS_INL – ITSS Inledning

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SASS_INL.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**E1**
Grund	X	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X

SASS_INL.D1
Utvecklaren ska tillhandahålla en *Inledning*

SASS_INL.C1
Inledningen ska bestå av ITSS-referens, systemreferens och systemöversikt

SASS_INL.C2
ITSS referensen ska entydigt identifiera ITSS

SASS_INL.C3
IT-systemreferens ska entydigt identifiera systemet

SASS_INL.C4
IT-systemreferens ska identifiera versionen på KSF-krav, samt vilken kravnivå, som ITSS anger att systemet ska uppfylla.

SASS_INL.C5
IT-systemreferens ska identifiera styrande dokument, internationella standarder samt andra säkerhetsrelaterade dokument som ITSS anger att systemet ska uppfylla

SASS_INL.C6

IT-systemreferens ska visa vilka säkerhetskrav i den aktuella kravsamlingen systemet och dess komponenter ska uppfylla

SASS_INL.C7

Systemöversikt ska beskriva systemets användning och säkerhetsmekanismer i systemet på en hög nivå

SASS_INL.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SASS_SYS – Systembeskrivning

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SASS_SYS.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**E1**
Grund	X	X	X	X	X	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X	X	X	X	X

SASS_SYS.D1

Systemutvecklaren ska tillhandahålla en *Systembeskrivning*

SASS_SYS.C1

Systembeskrivningen ska beskriva vilken information som hanteras i systemet samt konsekvenserna som skulle uppstå vid förlust av denna information

SASS_SYS.C2

Systembeskrivningen ska beskriva systemets exponering

SASS_SYS.C3

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.C4

Systembeskrivningen ska beskriva systemets tänkta användning, användare av systemet och information som ska lagras, bearbetas, överförs i eller utförs ut ur systemet

SASS_SYS.C5

Systembeskrivningen ska beskriva systemets fysiska avgränsning, och alla externt åtkomliga gränsytor

SASS_SYS.C6

Systembeskrivningen ska beskriva syfte och användningssätt för alla externt åtkomliga gränsytor

SASS_SYS.C7

Systembeskrivningen ska beskriva systemets arkitektur och design och ska identifiera de komponenter som systemet består av

SASS_SYS.C8

Systembeskrivningen ska tydligt identifiera de komponenter som är säkerhetsrelevanta

SASS_SYS.C9

Systembeskrivningen ska för alla externt åtkomliga gränsytor innehålla en beskrivning av vilka individuella komponenter som utgör gränsytan

SASS_SYS.C10

Systembeskrivningen ska beskriva systemets säkerhetsförmågor och de säkerhetsfunktioner som systemet tillhandahåller

SASS_SYS.C11

Beskrivningen av systemets förmågor ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS

SASS_SYS.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SASS_KRV – Sammanställning av säkerhetskrav

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SASS_KRV.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**E1**
Grund	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X

SASS_KRV.D1

Systemutvecklaren ska tillhandahålla en *Sammanställning av säkerhetskrav*

SASS_KRV.C1

Sammanställningen av säkerhetskrav ska identifiera de krav som kommer från KSF och de krav som är tillkommande säkerhetskrav

SASS_KRV.C2

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.C3

Sammanställningen av KSF-krav ska beskriva kravnivå för assuranskrav och alla gällandekravkomponenter

SASS_KRV.C4

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.C5

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.C6

Beskrivningen av KSF-krav och tillkommande funktionella krav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS

SASS_KRV.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SASS_OMG – Säkerhetskrav på omgivningen

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.

Kapitlet ska visa att alla nödvändiga förutsättningar på systemets miljö är identifierade och att alla säkerhetskrav som gäller för systemets miljö identifierats och dokumenterats. Dessa förutsättningar ska formuleras som säkerhetskrav på omgivningen så att de entydigt kan omsättas i systemets miljö.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SASS_OMG.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**E1**
Grund	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SASS_OMG.D1

Systemutvecklaren ska tillhandahålla *Säkerhetskrav på omgivningen*

SASS_OMG.C1

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.C2

Säkerhetskraven på omgivningen ska beskriva fysiska, administrativa samt organisatoriska åtgärder i systemets miljö som helt eller delvis uppfyller säkerhetskraven för systemets miljö

SASS_OMG.C3

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.C4

Beskrivningen av säkerhetskraven för systemets miljö ska tydligt visa vilka krav som uppfylls av systemet och vilka som uppfylls av systemets miljö

SASS_OMG.C5

Beskrivningen av säkerhetskraven för systemets miljö ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS

SASS_OMG.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SASS_TOL – Tolkning av säkerhetskrav

Detta krav innebär att säkerhetskraven för systemet måste tolkas (nedbrytas) på ett systemspecifikt sätt så att de konkret kan omsatts 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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SASS_TOL.	**D1**	**C1**	**C2**	**C3**	**C4**	**E1**
Grund	X	X	X	X	X	X
Utökad	X	X	X	X	X	X
Hög	X	X	X	X	X	X

SASS_TOL.D1

Systemutvecklaren ska tillhandahålla en *Tolkning av säkerhetskrav*

SASS_TOL.C1

Tolkningen av säkerhetskrav ska beskriva tolkningen av alla säkerhetskrav för systemet

SASS_TOL.C2

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.C3

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.C4

Beskrivningen av tolkningen av KSF-krav och tillkommande säkerhetskrav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS

SASS_TOL.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SASS_UPF – Uppfyllande av säkerhetskrav

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*.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SASS_UPF.	**D1**	**C1**	**C2**	**C3**	**C4**	**E1**
Grund	X	X	X	X	X	X
Utökad	X	X	X	X	X	X
Hög	X	X	X	X	X	X

SASS_UPF.D1

Systemutvecklaren ska tillhandahålla *Uppfyllande av säkerhetskrav*

SASS_UPF.C1

Uppfyllande av säkerhetskrav ska visa hur alla säkerhetskrav i kapitlet *Tolkning av säkerhetskrav* har uppfyllts av systemets säkerhetsfunktioner

SASS_UPF.C2

Uppfyllande av säkerhetskrav ska visa att alla krav fullständigt uppfylls av systemet

SASS_UPF.C3

Uppfyllande av säkerhetskrav ska för varje krav visa att hela kravet har uppfyllts av systemet

SASS_UPF.C4

Beskrivningen av uppfyllandet av säkerhetskrav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS

SASS_UPF.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

2.2 SALC – Systemutvecklings livscykel

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.

Klassen SALC består av fem krav:

- Säkerheten i systemets utvecklings och integrationsmiljö (SALC_UTV) omfattar systemutvecklarens kontroll av de ingående komponenterna, systemutvecklarens fysiska, administrativa (rutiner), personella och andra säkerhetsåtgärder som upprätthåller säkerheten för systemet under dess utveckling.
- Versions- och konfigurationshantering (SALC_KFG) befattar sig med omfattningen och rutinerna för versions- och konfigurationshantering av de komponenter eller delar som ingår i systemet. Så att visa att förändringar i systemet genomförts av behöriga personer på ett kontrollerat sätt.

- Leverans (SALC_LEV) omfattar de rutiner som systemutvecklaren använder för att säkerställa att leveransen till drift- och förvaltning sker på ett säkert sätt. Det innebär att förhindra eller upptäcka sekretess eller integritetsförlust som skulle kunna leda till brister i systemets säkerhetsförmåga.
- Livscykelmodellen (SALC_LCM) omfattar livscykelmodell för systemutveckling och underhåll hos systemutvecklaren, så att man får förtroende att systemets kvalitetskontroll.
- Bristkorrigering (SALC_BRK) omfattar processen och rutinerna för hur upptäckta säkerhetsrelevanta brister i systemet och i dess komponenter tas om hand och rapporteras till kunden. Den innefattar även hur systemutvecklaren hanterar säkerhetsrelevanta brister som upptäcks och rapporteras av komponentutvecklare för de komponenter som ingår i systemet.

SALC_UTV – Utvecklingssäkerhet

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. Då ett system kan bestå av komponenter från flera olika leverantörer måste man även ha kontroll på leveranskedjan för dessa komponenter. En komponent ska endast integreras i ett system efter att ha genomgått en acceptansprocedur som ska säkerställa förtroendet för leveranskedjan.

Vid högre assuranskrav krävs mer omfattande och fördjupade kontrollmekanismer hos systemutvecklaren för utvecklingsmiljön, acceptansprocedurerna och leveranskedjan.

Notera: Detta krav bygger på att det finns ett förtroende för systemutvecklaren. Hur detta ska fastställas ligger utanför KSF och hanteras inte av SALC_UTV. I vissa fall kan även kriterierna för detta vara beroende av systemet, t.ex. beroende av hur systemet ska användas och vilket information som ska skyddas.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SALC_UTV.	**D 1**	**D 2**	**D 3**	**D 4**	**C 1**	**C 2**	**C 3**	**C 4**	**C 5**	**C 6**	**E 1**	**E 2**
Grund												
Utökad	X	X	X	X	X	X	X	X			X	X
Hög	X	X	X	X	X	X			X	X	X	X

SALC_UTV.D1
Systemutvecklaren ska tillhandahålla systemutvecklingsdokumentation

SALC_UTV.D2
Systemutvecklaren ska tillämpa systemutvecklingsdokumentationen

SALC_UTV.D3
Systemutvecklaren ska tillhandahålla integrationsdokumentation

SALC_UTV.D4
Systemutvecklaren ska tillhandahålla acceptanskriterier för komponenter som ska ingå i systemet

SALC_UTV.C1
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.C2
Systemutvecklingsdokumentationen ska visa att säkerhetsåtgärderna erbjuder ett riktighetsskydd av utvecklingsmiljön som minst är i paritet med det skydd som systemet ska erbjuda

SALC_UTV.C3
Acceptanskriterierna ska beskriva tillräckliga kriterier för acceptans och verifiering av säkerhetsrelaterade komponenter som ingår i systemet

SALC_UTV.C4
Integrationsdokumentationen ska identifiera ursprunget hos alla ingående säkerhetsrelaterade komponenter och dokumentera hur ursprunget identifierades och hur acceptanskontrollen skett

SALC_UTV.C5
Acceptanskriterierna ska beskriva tillräckliga kriterier för acceptans och verifiering av alla IT- komponenter som ingår i systemet

SALC_UTV.C6
Integrationsdokumentationen ska identifiera ursprunget hos alla ingående komponenter och dokumentera hur ursprunget identifierades och hur acceptanskontrollen skett

SALC_UTV.E1
Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SALC_UTV.E2

Evalueraren ska verifiera att systemutvecklingsdokumentationens säkerhetsåtgärder tillämpas

SALC_KFG – Konfigurationsledning

Detta krav omfattar rutiner för versions- och konfigurationshantering i syfte att undvika obehörig eller oavsiktlig ändring av konfigurationsstyrda komponenter. Systemutvecklaren ska ha dokumenterade rutiner och mekanismer som ger skydd för riktigheten vid utveckling och underhåll av system och komponenter. För att unikt kunna identifiera ett system måste varje komponent finnas registrerad i ett konfigurationsledningssystem. För varje system måste man också kunna identifiera vilka komponenter det består av.

Vid produktion ska man med hjälp av konfigurationsledningssystemet kunna påvisa att levererat system är identiskt med det som testats och godkänts. I mjukvaruutveckling kan konfigurationsledning hanteras med hjälp av automatiserade verktyg.

Komplexa system består ofta även av hårdvarukomponenter. I dessa fall ska även relevant information för identifiering av hårdvara inklusive mjukvara finnas i konfigurationsledningssystemet. Detta kan utgöras av t.ex. typbeteckningar och versioner.

Alla system ska kunna följas upp med exakt version av ingående komponenter så att säkerhetsrelaterade ändringar kopplade till versioner av komponenter kan göras och följas upp. Ett konfigurationsledningssystem ska stödja ändringshantering så att den genomförs på ett kontrollerbart sätt och av behörig personal.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SALC_KFG.	**D 1**	**D 2**	**D 3**	**C 1**	**C 2**	**C 3**	**C 4**	**C 5**	**C 6**	**C 7**	**C 8**	**C 9**	**C1 0**	**E 1**	**E 2**
Grund															
Utökad	X	X	X	X	X	X	X	X	X	X	X	X		X	X
Hög	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SALC_KFG.D1

Systemutvecklaren ska tillhandahålla systemet och en unik systemreferens

SALC_KFG.D2
Systemutvecklaren ska använda ett konfigurationsledningssystem

SALC_KFG.D3
Systemutvecklaren ska tillhandahålla dokumentation som beskriver konfigurationsledningssystemet

SALC_KFG.C1
IT-systemet och de ingående komponenterna ska märkas med en unik referens

SALC_KFG.C2
Dokumentationen som beskriver konfigurationsledning ska visa metoder för unik identifiering av konfigurationsstyrda IT- komponenter

SALC_KFG.C3
Dokumentationen som beskriver konfigurationsledning ska visa hur konfigurationsledningen används i systemutvecklingen och systemutvecklarens förvaltning av systemet

SALC_KFG.C4
Alla konfigurationsobjekt som ingår i systemet ska ligga under konfigurationsledningen

SALC_KFG.C5
Dokumentationen som beskriver konfigurationsledning ska beskriva acceptansprocedurer för nya och uppdaterade konfigurationsobjekt

SALC_KFG.C6
Dokumentationen som beskriver konfigurationsledning ska påvisa att de acceptansprocedurer som används tillhandahåller tillräcklig ändringshantering för alla konfigurationsobjekt

SALC_KFG.C7
Underlag ska påvisa att systemet för konfigurationsledning bedrivs i enligheten med dokumentationen som beskriver konfigurationsledning

SALC_KFG.C8
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.C9

Konfigurationsledningssystemet ska tillhandahålla säkerhetsåtgärder för ändringshanteringar som säkerställer att alla ändringar genomförs på ett kontrollerat sätt och av behörig personal

SALC_KFG.C10

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.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SALC_KFG.E2

Evalueraren ska verifiera att konfigurationsledningssystemets säkerhetsåtgärder tillämpas

SALC_LEV – Systemleverans

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. Systemutvecklaren ska ha dokumenterade rutiner och mekanismer som tillhandahåller detta skydd och som medger att mottagaren före installation och driftsättning kan verifiera att ingen åverkan skett. Syftet är alltså att säkerställa kontrollerad leverans av ett visst granskat och godkänt system till drift- och förvaltning.

Det kan vara så att ett system, i synnerhet om det är ett stort, komplext och distribuerat system, består av komponenter som distribueras på olika sätt till olika platser. I sådana fall omfattas alla dessa leveranssätt av SALC_LEV.

SALC_LEV ställer krav på dokumenterade rutiner som beskriver hur systemutvecklaren skyddar nyttjaren från att driftsätta ett system som åverkats under leveransen och därmed inte kan anses som säkert.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SALC_LEV.	**D1**	**D2**	**C1**	**C2**	**C3**	**E1**
Grund	X	X	X	X		X
Utökad	X	X	X	X	X	X
Hög	X	X	X	X	X	X

SALC_LEV.D1

Systemutvecklaren ska tillhandahålla dokumentation som beskriver rutiner och mekanismer för IT system- och komponentleveranser

SALC_LEV.D2

Systemutvecklaren ska använda leveransrutinerna

SALC_LEV.C1

Leveransdokumentationen ska beskriva alla rutiner som är nödvändiga för att upprätthålla säkerheten för systemet under dess leverans till drift- och förvaltningsorganisationen

SALC_LEV.C2

Leveransdokumentationen ska beskriva hur systemets riktighet skyddas under leveransen

SALC_LEV.C3

Leveransdokumentationen ska beskriva hur systemets riktighet kan verifieras av mottagaren vid leverans samt vid godtycklig tidpunkt efter leverans

SALC_LEV.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SALC_LCM – Livscykelmodell

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

Vid integration av komponenter från en eller flera leverantörer ska livscykelmodell definiera vilka acceptansprocedurer som krävs.

En livscykelmodell omfattar procedurer, verktyg och tekniker för att utveckla och underhålla ett system. Exempel på delar i en sådan modell är designmetoder, systemutvecklarens egna granskningsprocesser, projektstyrningsmodeller, procedurer för ändringshantering, testmetoder och acceptansprocedurer. En effektiv livscykelmodell tar hänsyn till alla dessa aspekter i en gemensam styrmodell med uttalad ansvarsfördelning och uppföljning.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SALC_LCM.	**D1**	**D2**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C 9**	**C 10**	**E1**	**E2**
Grund														
Utökad	X	X	X	X	X	X	X	X	X	X			X	X
Hög	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SALC_LCM.D1

Systemutvecklaren ska upprätta en livscykelmodell som ska användas vid utveckling av systemet och systemutvecklarens förvaltning av systemet

SALC_LCM.D2

Systemutvecklaren ska tillhandahålla dokumentation som beskriver livscykel-modellen

SALC_LCM.C1

Livscykelmodellen ska omfatta systemutveckling och systemutvecklarens förvaltning av systemet

SALC_LCM.C2

Livscykelmodellen ska tillhandahålla kontroll över systemutveckling och systemutvecklarens förvaltning av systemet

SALC_LCM.C3

Livscykelmodellen ska beskriva det som behövs för att kunna bedöma säkerhetspåverkan av ändringar i systemet under systemets livscykel

SALC_LCM.C4

Livscykelmodellen ska beskriva det som behövs för att kunna upprätthålla säkerhet i systemet under dess livscykel och systemutvecklarens förvaltning av systemet

SALC_LCM.C5

Livscykelmodellen ska beskriva de delar av design-, drift- och förvaltningsdokumentationen som behövs för att upprätthålla säkerhet under systemets livscykel

SALC_LCM.C6

Livscykelmodellen ska beskriva rutiner för verifiering av komponenternas lämplighet för användning i systemet

SALC_LCM.C7

Livscykelmodellen ska beskriva acceptans- och releaseprocedurer för systemdesign och de ingående komponenterna

SALC_LCM.C8

Livscykelmodellen ska beskriva hur kvalitetssäkring är integrerad i systemets livscykel

SALC_LCM.C9

Livscykelmodellen ska beskriva hur processen för kvalitetssäkring möter liknande krav som ställs i standarden ISO 9001

SALC_LCM.C10

Rutinerna för verifiering av komponenternas lämplighet för användning i systemet skall omfatta bedömmande av varje komponents säkerhetspåverkan på systemet

SALC_LCM.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SALC_LCM.E2

Evalueraren ska verifiera att livscykelmodellen tillämpas

SALC_BRK – Bristkorrigering

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.
Dessa assuranskrav ställer dock inte krav på systemutvecklarens förmåga att upptäcka olika säkerhetsrelevanta brister.
Vissa säkerhetsrelevanta brister kan inte repareras omedelbart, därför ska andra alternativa åtgärder kunna vidtas.
Om systemet är utvecklat och implementerat av systemutvecklaren men avtal reglerar att drift- och förvaltningsorganisationen ska sköta förvaltning av systemet utan fortsatt stöd från systemutvecklaren kan detta krav komma att utgå. I sådana fall överförs ansvaret för bristkorrigering till drift- och förvaltningsorganisationen och systemutvecklaren måste tillhandahålla tillräckliga instruktioner för detta för att bibehålla systemets säkerhet. Kravet på detta underlag finns i klassen SAOP (SAOP_BRK).

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SALC_BRK.	**D1**	**D2**	**D3**	**D4**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**E1**
Grund	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SALC_BRK.D1

Systemutvecklaren ska tillhandahålla dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet

SALC_BRK.D2

Systemutvecklaren ska ha erforderliga avtal och processer för att få information kring säkerhetsrelevanta brister i systemet och ingående komponenter

SALC_BRK.D3

Systemutvecklaren ska tillhandahålla drift- och förvaltningsdokumentation kring säkerhetsrelevanta brister i systemet

SALC_BRK.D4

Systemutvecklaren ska etablera en process för rapportering av säkerhetsrelevanta brister i systemet

SALC_BRK.C1

Drift- och förvaltningsdokumentation ska beskriva hur drift- och förvaltningsorganisationen kan rapportera misstänkta säkerhetsrelevanta brister i systemet

SALC_BRK.C2

Drift- och förvaltningsdokumentation ska identifiera specifik kontaktyta för alla rapporter och förfrågningar angående säkerhetsrelevanta brister i systemet

SALC_BRK.C3

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.C4

Dokumenterade procedurer för hantering av säkerhetsrelevanta brister i systemet ska säkerställa att korrigerande åtgärder identifieras för alla kända säkerhetsrelevanta brister

SALC_BRK.C5

Dokumentationen som beskriver hantering av säkerhetsrelevanta brister ska beskriva hur information kring brister och instruktioner om korrigerande åtgärder tillhandahålls drift- och förvaltningsorganisationen

SALC_BRK.C6

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.C7

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.C8

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.C9

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.C10

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.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

2.3 SADE – Arkitektur och design

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.

Klassen SADE består av fyra krav:

- Gränsytebeskrivning (SADE_GRÄ) omfattar krav på beskrivning av syfte och användningssätt för systemets alla externa gränsytor.
- Säkerhetsarkitektur (SADE_ARK) omfattar krav på arkitekturbeskrivning som systemutvecklaren ska tillhandahålla.
- Dataflödesanalys (SADE_DFA) omfattar krav på identifiering av de komponenter som lagrar och bearbetar kritisk[2] data.
- Designdokumentation (SADE_DES) omfattar krav på beskrivning av alla säkerhetsrelevanta komponenter och hur dessa bidrar med säkerhetsförmågor för att möta systemets säkerhetsmål.

SADE_GRÄ – Gränsytebeskrivning

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. Alla externa gränsytor ska identifieras och beskrivas till den grad att deras säkerhetsrelevans och effekter av vidtagna åtgärder kan avgöras.

Extern kommunikation med andra system måste beskrivas på så sätt att man kan verifiera att dokumentation, så som programmeringsguider, beskriver hur andra system ska programmeras och konfigureras för att på ett säkert sätt kunna samverka med systemet.

Dessutom måste beskrivningen av de externa gränsytorna ge tillräcklig information så att man i sårbarhetsanalysen förstår vilken attackyta som systemet

[2] Kritisk data är antingen skyddsvärd i sig eller data som kan påverka skyddet av sådan data

uppvisar. För att detta ska vara möjligt måste det för varje gränsyta framgå till vilken grad gränsytan är exponerad för specifika attacker utifrån attackscenarion och angriparens kapacitet eller attackpotential och varför gränsytan av specifika skäl, t.ex. antaganden om miljön, inte kan utsättas för en given attack.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SADE_GRÄ.	**D1**	**C1**	**C2**	**C3**	**C4**	**E1**
Grund						
Utökad	X	X	X	X	X	X
Hög	X	X	X	X	X	X

SADE_GRÄ.D1

Systemutvecklaren ska tillhandahålla en beskrivning av systemets gränsytor

SADE_GRÄ.C1

Beskrivningen av systemets gränsytor ska innehålla en analys av vilka externt åtkomliga gränsytor som är säkerhetsrelevanta och vilka som ej är säkerhetsrelevanta

SADE_GRÄ.C2

Beskrivningen av systemets gränsytor ska innehållande en beskrivning av de ur säkerhetssynpunkt relevanta åtgärder som är associerade med varje säkerhetsrelevant gränsyta.

SADE_GRÄ.C3

Beskrivningen av systemets gränsytor ska innehålla en sammanfattning av de säkerhetsfunktioner som är associerade med respektive gränsyta

SADE_GRÄ.C4

Beskrivningen av systemets gränsytor ska innehålla fullständig beskrivning för de interaktioner systemets alla externt åtkomliga gränsytor medger.

SADE_GRÄ.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SADE_ARK – Säkerhetsarkitektur

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. Beskrivningen av arkitekturen ska innehålla den information som behövs för att avgöra till vilken grad arkitekturen är beroende av specifika komponenter och dess egenskaper.

Assuransnivå för komponenter måste anges så att förtroenderelationer som är beroende av komponenters assurans dokumenteras i arkitekturen. För att möjliggöra en bedömning av arkitekturens sundhet och riktighet ska skyddskraven för den information som lagras eller bearbetas på olika komponenter redovisas och gränser mellan olika skyddskrav identifieras. Beskrivningen av arkitekturen måste också omfatta systemets möjligheter att skydda sig själv från manipulation av säkerhetsfunktionalitet och från försök att kringgå säkerhetsfunktionerna.

Det huvudsakliga målet för detta krav är att verifiera att systemets säkerhetsarkitektur är sund och riktig. Det finns beroenden till designbeskrivningen som kan påverka detaljeringsgraden som krävs i arkitekturbeskrivningen. Evalueringen av SADE_ARK behöver därför göras i samband med SADE_GRÄ och SADE_DES.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SADE_ARK.	**D1**	**D2**	**C1**	**C2**	**C3**	**E1**	**E2**
Grund							
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SADE_ARK.D1

Systemutvecklaren ska tillhandahålla en beskrivning av systemets säkerhetsarkitektur

SADE_ARK.D2

Systemutvecklaren ska designa och implementera systemet så att säkerhetsfunktioner ej kan kringgås

SADE_ARK.C1

Beskrivningen av säkerhetsarkitekturen ska påvisa hur komponenterna tillsammans och deras interaktioner resulterar i systemets säkerhetsfunktionalitet

SADE_ARK.C2

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.C3

Beskrivningen av säkerhetsarkitekturen ska påvisa att systemarkitekturen förhindrar att säkerhetsfunktionalitet kan kringgås

SADE_ARK.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SADE_ARK.E2

Evalueraren ska analysera underlaget och verifiera att det inte går att kringgå systemets säkerhetsfunktioner

SADE_DFA – Dataflödesanalys

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. För att säkerställa att ändamålsenliga skyddsmekanismer används för att skydda kritiska data ska systemutvecklaren tillhandahålla en analys som visar på var i systemet kritisk data lagras och bearbetas. Analysen utgör grunden i assuransprofileringen och systemutvecklarens riskanalys.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SADE_DFA.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**E1**
Grund							
Utökad	X	X	X	X	X		X
Hög	X	X	X	X	X	X	X

SADE_DFA.D1

Systemutvecklaren ska tillhandahålla en dataflödesanalys för kritiska data i systemet

SADE_DFA.C1

Dataflödesanalysen ska identifiera all kritisk data som lagras och bearbetas av systemet

SADE_DFA.C2

Dataflödesanalysen ska innehålla en konsekvensnivåbedömning av det kritiska data som lagras eller bearbetas av komponenterna i systemet

SADE_DFA.C3

Dataflödesanalysen ska dokumentera vilka komponenter som lagrar eller bearbetar kritiska data samt de komponenter som inte bearbetar eller lagrar kritiska data

SADE_DFA.C4

Dataflödesanalysen ska dokumentera hur kritiska data överförs mellan komponenter i systemet

SADE_DFA.C5

Dataflödesanalysen ska betrakta all data som kritisk och därför fullständigt beskriva systemets samtliga dataflöden

SADE_DFA.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SADE_DES – Designdokumentation

Detta krav behandlar hur varje komponent bidrar med säkerhetsfunktionalitet till systemet samt hur komponenterna integreras i systemet. Medan SADE_ARK ger en vy ur arkitekturperspektivet, dvs. arkitektoniska krav på komponenter, ger SADE_DES en komponentvy, dvs. hur komponenter bidrar till arkitekturen.

En designbeskrivning (SADE_DES) uttrycks i termer av de logiska komponenter i systemet som tillhandahåller en mer omfattande tjänst eller funktion. Om det i ett system till exempel ingår en brandvägg, skulle designbeskrivningen av denna omfatta de åtgärder som utförs av brandväggen när ett paket anländer till den.

En komponentbeskrivning utgör en del av designen av systemet och tillför en högnivåbeskrivning av vad en specifik del av systemet gör och hur den fungerar.

Syftet med designdokumentationen är att tillhandahålla tillräckligt med information för att kunna avgöra gränserna för komponenter som tillför säkerhetsförmågor i systemet och hur säkerhetsfunktionerna implementerar de säkerhetskrav som ställs på systemet. Omfattningen och strukturen av designdokumentationen beror på komplexiteten i systemet, antalet komponenter och de säkerhetsfunktioner de implementerar.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SADE_DES.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**E1**
Grund								
Utökad	X	X	X	X	X	X		X
Hög	X	X	X	X	X	X	X	X

SADE_DES.D1

Systemutvecklaren ska tillhandahålla designdokumentation för systemet

SADE_DES.C1

Designen ska beskriva systemets struktur i termer av dess ingående komponenter

SADE_DES.C2

Designen ska identifiera alla komponenter som bidrar med säkerhetsfunktionalitet i systemet

SADE_DES.C3

Designen ska beskriva varje komponents beteende i tillräcklig grad för att avgöra vilka komponenter som är säkerhetsrelevanta

SADE_DES.C4

Designen ska innehålla en beskrivning av interaktionen mellan säkerhetsrelevanta komponenter samt mellan säkerhetsrelevanta och icke säkerhetsrelevanta komponenter

SADE_DES.C5

Designdokumentationen ska påvisa att varje externt åtkomlig gränsyta som identifierats i gränsytebeskrivningen är associerad med minst en säkerhetsrelevant komponent

SADE_DES.C6

Designdokumentationen skall visa fullständigt hur systemets komponenter och deras konfiguration ger systemet dess avsedda IT-säkerhetsförmågor

SADE_DES.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

2.4 SAOP – Installation och drift

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.

Klassen SAOP består av tre krav:

- Installation och förberedelser (SAOP_INS) omfattar krav på att systemet bli mottaget och installerat i sin driftmiljö på ett säkert sätt.
- Drift- och förvaltningsdokumentation (SAOP_DOK) omfattar krav på skrivna riktlinjer och procedurer som ska användas av alla olika typer av drift- och förvaltningspersonal som förväntas finnas.
- Bristkorrigering (SAOP_BRK) omfattar krav på rutiner och andra förutsättningar för bristkorrigering av systemet.

SAOP_INS – Installation och förberedelser

Detta krav ska säkerställa att systemet blir mottaget och installerat i sin driftmiljö på ett säkert sätt och som systemutvecklaren avsett. Detta inkluderar att undersöka huruvida systemet skulle kunna konfigureras eller installeras på ett osäkert sätt samtidigt som systemets drift- och förvaltningsorganisation upplever att det är säkert.

Den första processen som täcks av de förberedande åtgärderna är drift- och förvaltningsorganisationens acceptans att det levererade systemet inte manipulerats. Kontrollen sker i enlighet med systemutvecklarens instruktioner. Ett installerat system ska även uppfylla säkerhetsmålen för driftmiljön. Detta kan till exempel omfatta fysiska skydd, RÖS-skydd mm. För system som levereras som flera separata komponenter gäller dessa krav för alla delar av systemet och för varje leverans.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SAOP_INS.	**D1**	**C1**	**C2**	**C3**	**C4**	**E1**	**E2**

Grund	X	X	X	X		X	
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SAOP_INS.D1

Systemutvecklaren ska tillhandahålla systemet med dokumentation som beskriver förberedande åtgärder

SAOP_INS.C1

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.C2

De förberedande åtgärderna ska beskriva alla nödvändiga steg för säker installation av systemet

SAOP_INS.C3

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.C4

De förberedande åtgärderna ska innehålla steg för verifikation av korrekt installation

SAOP_INS.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SAOP_INS.E2

Evalueraren ska tillämpa åtgärderna för att verifiera att systemet kan mottagas och installeras på ett säkert sätt genom att följa beskrivningen av dem

SAOP_DOK – Drift- och förvaltningsdokumentation

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. Krav ställs även på att drift- och förvaltningsdokumentation inte är missvisande eller vilseledande vilket kan leda till felaktig användning av systemet.

Drift- och förvaltningsdokumentationen ska beskriva säkerhetsfunktionaliteten i systemet och tillhandahålla instruktioner (även varningar) för att drift- och förvaltningspersonalen ska förstå systemets säkerhetsförmågor. Drift- och förvaltningsdokumentation innefattar även säkerhetskritiska åtgärder och nödvändig information för att systemet ska kunna användas på ett säkert sätt.

Målet med detta är att minska risken för mänskliga eller andra fel som kan inaktivera, koppla bort eller hindra att säkerhetsfunktionaliteten ger avsedd effekt.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SAOP_DOK.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**E1**
Grund	X	X	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X	X

SAOP_DOK.D1

Systemutvecklaren ska tillhandahålla drift- och förvaltningsdokumentation

SAOP_DOK.C1

Drift- och förvaltningsdokumentation ska för varje användarroll beskriva de användargränssnitt och säkerhetsfunktioner som är tillgängliga för användaren

SAOP_DOK.C2

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.C3

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.C4

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.C5

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.C6

Drift- och förvaltningsdokumentation ska för respektive användarroll dokumentera alla tillåtna systemkonfigurationers kritiska beroenden mellan de olika komponenterna konfigurationer

SAOP_DOK.C7

Drift- och förvaltningsdokumentation ska beskriva processer för rapportering av säkerhetsrelaterade händelser, t.ex. förlust av utrustning eller röjda säkerhetsattribut

SAOP_DOK.C8

Drift- och förvaltningsdokumentation ska vara tydlig och rimlig för de tänkta användarna

SAOP_DOK.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SAOP_BRK – Bristkorrigering

Detta krav ska säkerställa att drift- och förvaltningsorganisationen har förutsättningar att ta emot och implementera åtgärder för att hantera säkerhetsrelevanta brister i systemet. Normalt innebär detta att instruktioner finns för hur brister identifieras, hur mottas från systemutvecklaren och hur dessa implementeras i systemet.

Om systemet är utvecklat och implementerat av systemutvecklaren men avtal reglerar att drift- och förvaltningsorganisationen skall sköta förvaltning av systemet utan fortsatt stöd från systemutvecklaren, måste drift- och förvaltningsorganisationen överta ansvaret för bristbevakning och bristkorrigering från systemutvecklaren för att säkerheten i systemet ska kunna bibehållas. Dessa instruktioner måste i sådant fall vara mer omfattande, då det ska vara möjligt för drift- och förvaltningsorganisationen att själva bevaka information om brister i ingående komponenter och själva inhämta information om korrigering av upptäckta brister.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SAOP_BRK.	**D1**	**D2**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**E1**
Grund	X	X	X	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X	X	X

SAOP_BRK.D1

Systemutvecklaren ska tillhandahålla instruktioner som möjliggör för drift- och förvaltningsorganisationen att utföra bevakning av brister samt bristkorrigering

SAOP_BRK.D2

Systemutvecklaren ska tillhandahålla nödvändiga kontakter till drift- och förvaltningsorganisationen för att bristkorrigeringsinformation för systemets komponenter ska kunna bevakas

SAOP_BRK.C1

Instruktionerna ska innehålla processer för bevakning av källor till information om säkerhetsrelevanta brister i systemet och dess ingående komponenter

SAOP_BRK.C2

Instruktionerna ska innehålla processer för hur säkerhetsrelevanta brister följs upp och korrigeras

SAOP_BRK.C3

Instruktionerna ska beskriva hur uppföljning av säkerhetsrelevanta brister ska dokumenteras och visa att dokumentationen ska innehålla källor, analys, slutsats och rekommenderade åtgärder

SAOP_BRK.C4

Instruktionerna ska innehålla processer för integrering av säkerhetsuppdateringar i systemet, inklusive avinstallering

SAOP_BRK.C5

Instruktionerna ska innehålla metoder för säkert mottagande av bristinformation och bristkorrigering för systemet och dess ingående komponenter

SAOP_BRK.C6

Instruktionerna ska innehålla rutiner för verifiering av riktighet och ursprung hos säkerhetuppdateringar innan de införs i systemet

SAOP_BRK.C7

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.C8

Instruktionerna ska innehålla rutiner för att testa säkerhetsuppdateringar för att säkerställa att säkerhetsfunktionaliteten fortfarande är intakt efter införandet

SAOP_BRK.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

2.5 SARU – Administrativa rutiner

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.

Klassen SARU består av sex krav:

- Krav på rutiner för tilldelning och återkallning av åtkomsträttigheter (SARU_BEH)
- Krav på rutiner för kvaliteten hos säkerhetsattribut för autentisering (SARU_ATT)
- Krav på rutiner för att upptäcka och spåra intrång och missbruk i systemet (SARU_INT)
- Krav på rutiner för hur säkerhetsuppdateringar av systemet ska ske (SARU_UPD)
- Krav på rutiner för hur konfigurationsstyrning av systemet ska ske (SARU_KON)
- Krav på rutiner för hur säkerhetsutbildning av användare ska ske (SARU_UTB)

SARU_ÅTK – Åtkomsträttigheter

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

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARU_ÅTK.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**E1**
Grund	X	X	X	X	X	X					X
Utökad	X	X	X	X	X	X	X	X		X	X
Hög	X	X	X	X	X	X	X	X	X	X	X

SARU_ÅTK.D1

Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för tilldelning och återkallning av åtkomsträttigheter

SARU_ÅTK.C1
Rutinerna ska beskriva hur åtkomsträttigheter tilldelas och återkallas

SARU_ÅTK.C2
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.C3
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.C4
Rutinerna ska beskriva hur uppföljning av tilldelning sker för att säkerställa att systemets användare och subjekt har korrekt tilldelade roller och åtkomsträttigheter

SARU_ÅTK.C5
Rutinerna ska beskriva att endast behörig driftspersonal ska tilldelas åtkomsträttigheter till administrativa funktioner för säkerhetsfunktioner, deras konfiguration och styrande data

SARU_ÅTK.C6
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.C7
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.C8
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.C9

Rutinerna ska beskriva att endast den person som ansvarar för administration av säkerhetslogg får tilldelas åtkomsträttigheter till systemets säkerhetsloggar

SARU_ÅTK.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SARU_ATT – Säkerhetsattribut för autentisering

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

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARU_ATT.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**E1**
Grund	X	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X

SARU_ATT.D1

Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för kontroll av kvaliteten på säkerhetsattribut som används för autentisering

SARU_ATT.C1

Rutinerna ska beskriva en lägsta acceptabel kvalitetsnivå för lösenord som väljs av användare

SARU_ATT.C2

Rutinerna ska beskriva att alla tilldelade lösenord genereras slumpmässigt och hur detta sker

SARU_ATT.C3

Rutinerna ska visa att slumpmässigt genererade lösenord alltid består av minst 12 tecken

SARU_ATT.C4

Rutinerna ska visa att lösenord byts vid driftsättning av systemet samt löpande med en bestämd intervall

SARU_ATT.C5

Rutinerna ska beskriva att regelbunden uppdatering av revokeringslistor för certifikat ska ske

SARU_ATT.C6

Rutinerna ska visa att varje användaridentitet i systemet kan bindas till en specifik person

SARU_ATT.C7

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.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SARU_INT – Upptäcka och spåra intrång och missbruk

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.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARU_INT.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**E1**
Grund	X	X	X	X	X	X	X	X			X	X
Utökad	X	X	X	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X	X	X	X

SARU_INT.D1

Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att upptäcka och spåra intrång och missbruk i systemet

SARU_INT.C1

Rutinerna ska beskriva hur länge säkerhetsloggar ska sparas och visa att de överensstämmer med minst den tid som de gällande föreskrifterna påbjuder

SARU_INT.C2

Rutinerna ska beskriva hur och med vilken regelbundenhet som verktygsbaserad analys av registrerade händelser i säkerhetsloggen ska ske

SARU_INT.C3

Rutinerna ska beskriva hur analys av driftsrelaterade felhändelser i systemet ska ske och hur de ska dokumenteras

SARU_INT.C4

Rutinerna ska beskriva hur analysresultat klassificeras och visa hur klassificeringsbeslutet samt beslut om åtgärd dokumenteras

SARU_INT.C5

Rutinerna ska beskriva att analys och klassificering av analysresultat endast utförs av utbildad operatör

SARU_INT.C6

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.C7

Rutinerna ska beskriva hur alla identifierade incidenter ska utredas och rapporteras

SARU_INT.C8

Rutinerna ska beskriva hur säkerhetskopiering av säkerhetsloggen ska ske regelbundet till annat lagringsmedium

SARU_INT.C9

Rutinerna ska beskriva hur säkerhetskopian av säkerhetsloggen ska förvaras och visa att den ska förvaras fysiskt separerat från säkerhetsloggen

SARU_INT.C10

Rutinerna ska beskriva att analysresultat fortlöpande ska hanteras i enlighet med organisationens fastställda IT-säkerhetsplan

SARU_INT.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SARU_UPD – Säkerhetsuppdateringar

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

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARU_UPD.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**E1**
Grund	X	X	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X	X

SARU_UPD.D1

Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att utföra regelbundna säkerhetsuppdateringar av systemet

SARU_UPD.C1

Rutinerna ska innehålla detaljerade instruktioner för hantering av säkerhetsuppdateringar för samtlig mjukvara i systemet

SARU_UPD.C2

Rutinerna ska beskriva processer för säker uppdatering av de säkerhetsfunktioner som är beroende av extern tillförsel av säkerhetsmekanismer eller styrande data

SARU_UPD.C3

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.C4

Rutinerna ska visa att alla säkerhetsrelaterade brister i systemet ska korrigeras inom ett dokumenterat tidsintervall ifrån kännedomstillfället

SARU_UPD.C5

Rutinerna ska beskriva att säkerhetsuppdateringar till någon av systemets komponenter ska införas så snart det är möjligt efter att dessa gjorts tillgängliga

SARU_UPD.C6

Rutinerna ska beskriva att säkerhetsuppdateringars riktighet och ursprung ska verifieras innan de införs i systemet

SARU_UPD.C7

Rutinerna ska beskriva hur efterlevnad av rutiner för bristhantering och säkerhetsuppdatering dokumenteras på sådant sätt att kontroller enkelt kan genomföras

SARU_UPD.C8

Rutinerna ska beskriva hur riskminimerande åtgärder ska vidtas omedelbart efter att en säkerhetsrelaterad brist i systemet konstaterats

SARU_UPD.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SARU_KFG –Konfigurationsstyrning

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

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARU_KFG.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**E1**
Grund	X	X	X	X			X
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SARU_KFG.D1

Systemutvecklaren ska tillhandahålla dokumenterade administrativa rutiner för att genomföra konfigurationsstyrning av systemet

SARU_KFG.C1

Rutinerna ska beskriva hur aktuell version och uppdateringsnivå för all mjukvara i systemet ska dokumenteras

SARU_KFG.C2

Rutinerna ska beskriva hur aktuell konfiguration av alla komponenter i systemet ska vara dokumenterad

SARU_KFG.C3

Rutinerna ska beskriva hur återkommande kontroller av att dokumentationen stämmer överens med systemet ska genomföras av driftspersonal

SARU_KFG.C4

Rutinerna ska beskriva hur alla förändringar till systemets mjukvara och konfiguration ska beslutas och dokumenteras innan de genomförs

SARU_KFG.C5

Rutinerna ska beskriva hur ändringsbeslut dokumenteras och visa att de ska innehålla anledning, syfte och dokumentera exakt vilka förändringar som ska genomföras

SARU_KFG.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SARU_UTB – Säkerhetsutbildning av användare

Detta krav skall se till att systemutvecklare tillhandahåller utbildningsunderlag för alla olika användare av systemet. Utbildningsunderlaget skall vara tillräckligt för att med givna förutsättningar ge tillräckliga färdigheter så att användaren kan använda systemet på ett säkert sätt. Olika utbildningsunderlag skulle kunna finnas för olika användare av systemet.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARU_UTB.	**D1**	**D2**	**C1**	**C2**	**C3**	**C4**	**C5**	**E1**
Grund	X	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X

SARU_UTB.D1

Systemutvecklaren ska tillhandahålla underlag för utbildning

SARU_KFG.D2

Systemutvecklaren ska tillhandahålla rutiner för utbildning av användare

SARU_KFG.C1

Utbildningsunderlag ska finnas för alla typer av användare av systemet

SARU_KFG.C2

Utbildningsunderlag ska innefatta beskrivningar av hur användare ska rapportera säkerhetsrelaterade incidenter och vilka typer av incidenter som ska rapporteras

SARU_KFG.C3

Utbildningsunderlag ska för varje typ av användare ange förutsättningar såsom förkunskaper

SARU_KFG.C4

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_KFG.C5

Rutinerna för utbildning ska visa att användare ska ha genomgått utbildning med godkänt resultat innan de ges behörighet att använda systemet

SARU_KFG.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

2.6 SATS – Systemintegrationstest

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.

Klassen SATS består av fyra krav:

- Testtäckning (SATS_TTK) omfattar krav på att alla säkerhetsfunktioner har täckts av test och att i synnerhet alla externa gränsytor och komponenter testats på ett tillfredsställande sätt.
- Funktionstester (SATS_FUN) omfattar krav på systemutvecklaren att genomföra funktionstester av säkerhetsfunktionaliteten och därmed ge förtroende att sannolikheten för brister i säkerhetsfunktionaliteten är relativt liten.
- Angripartester (SATS_ANG) omfattar krav på systemutvecklaren att genomföra tester av säkerhetsfunktionaliteten ur angriparperspektiv i syfte att visa att den inte går att kringgå.
- Evaluerarens testning (SATS_EVL) omfattar krav på evalueraren att verifiera resultatet i (SATS_FUN) och (SATS_ANG).

Kraven för testtäckning (SATS_TTK), funktionstester (SATS_FUN) och angripartester (SATS_ANG) definierar det underlag som systemutvecklaren måste ta fram för testningen. Evaluerare måste inte bara verifiera detta underlag utan även använda detta underlag för att genomföra egna tester som en del av evaluerarens testning (SATS_EVL).

SATS_TTK – Testtäckning

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. Detta sker genom att systemutvecklaren ska visa att hur testfallen korrelerar med kraven, säkerhetsfunktionerna och de komponenter som implementerar dem i enlighet med SADE_DES.

Målet är att bekräfta att alla säkerhetsfunktionella krav testats och att säkerhetsfunktioner och komponenter testats så som de beskrivs i designdokumentationen.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SATS_TTK.	D1	C1	C2	C3	C4	C5	E1
Grund	X	X					X
Utökad	X	X	X	X			X
Hög	X	X	X	X	X	X	X

SATS_TTK.D1

Systemutvecklaren ska tillhandahålla en analys av testtäckningen för funktionella- och angripartester

SATS_TTK.C1

Analysen skall innehålla en motivering till varför de genomförda funktionella testerna och angripartesterna anses tillräckliga och omfattar alla systemets säkerhetsfunktioner

SATS_TTK.C2

Analysen ska visa hur testfallen i testdokumentationen överensstämmer med de säkerhetsfunktionella kraven, säkerhetsfunktionerna och komponenterna så som de beskrivs i designdokumentationen

SATS_TTK.C3

Analysen ska visa att alla kravkomponenter i alla funktionella säkerhetskrav testats

SATS_TTK.C4

Analysen ska visa att alla systemets säkerhetsfunktioner testats i alla de säkerhetsrelevanta komponenter som implementerar dem

SATS_TTK.C5

Analysen ska visa att alla säkerhetsrelevanta komponenters säkerhetsfunktionalitet för systemet testats för komponentens alla gränsytor

SATS_TTK.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SATS_FUN – Funktionstester

Detta krav innebär att funktionstester av säkerhetsfunktionalitet ska genomföras av systemutvecklaren för att säkerställa att säkerhetsfunktionaliteten fungerar enligt specifikationen. Funktionstesterna fokuserar på att visa att kraven för systemets säkerhetsfunktionalitet så som det specificeras i ITSS uppnås med komponenternas säkerhetsfunktionalitet och att de fungerar så som beskrivs i designdokumentationen.

Kraven på testtäckning (SATS_TTK) och funktionstester (SATS_FUN) definierar det underlag som systemutvecklaren måste ta fram för testningen. Evaluerare måste inte bara verifiera detta underlag utan även använda detta underlag för att genomföra tester som en del av evaluerarens testning (SATS_EVL).

SATS_FUN ställer krav på systemutvecklaren att tillhandahålla testplan, testfall, testresultat och resursåtgång för att kunna återupprepa testningen svid behov. Detta för att få förtroende för att testerna i testdokumentationen genomförts och att resultatet dokumenterats korrekt.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SATS_FUN.	**D1**	**D2**	**D3**	**C1**	**C2**	**C3**	**C4**	**C5**	**E1**
Grund	X	X		X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X

A.1.1.1 SATS_FUN.D1

Systemutvecklaren ska testa systemet och producera testdokumentation

SATS_FUN.D2

Systemutvecklaren ska tillhandahålla en testrapport

SATS_FUN.D3

Systemutvecklaren ska tillhandahålla testdokumentation

SATS_FUN.C1

Testrapporten ska bestå av beskrivning av hur testerna genomförts, testernas övergripande resultat samt eventuella anmärkningar avseende utfallet av testerna

SATS_FUN.C2

Testdokumentationen ska bestå av testplaner, förväntat resultat och faktiskt resultat

SATS_FUN.C3

Testplanerna ska beskriva de tester som ska genomföras och scenariot för varje test. Beskrivningarna ska vara så detaljerade att testerna kan reproduceras

SATS_FUN.C4

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.C5

Det faktiska testresultatet ska överensstämma med det förväntade testresultatet

SATS_FUN.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SATS_ANG – Angripartester

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. Angripartester ska ge förtroende för att sannolikheten för brister i säkerhetsfunktionaliteten är förhållandevis liten.

Angripartesterna fokuserar på att visa att komponenternas säkerhetsfunktionalitet inte bara finns och fungerar utan även att de är integrerade i systemet på ett sådant sätt att de inte kan kringgås.

Kraven på testtäckning (SATS_TTK) och angripartester (SATS_ANG) definierar det underlag som systemutvecklaren måste ta fram för testningen. Evaluerare måste inte bara verifiera detta underlag utan även använda detta underlag för att genomföra tester som en del av evaluerarens testning (SATS_EVL).

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SATS_ANG.	**D1**	**D2**	**D3**	**C1**	**C2**	**C3**	**C4**	**C5**	**E1**
Grund	X	X		X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X	X	X

SATS_ANG.D1

Systemutvecklaren ska testa systemet och producera testdokumentation

SATS_ANG.D2
Systemutvecklaren ska tillhandahålla en testrapport

SATS_ANG.D3
Systemutvecklaren ska tillhandahålla testdokumentation

SATS_ANG.C1
Testrapporten ska bestå av beskrivning av hur testerna genomförts, testernas övergripande resultat samt eventuella anmärkningar avseende utfallet av testerna

SATS_ANG.C2
Testdokumentationen ska bestå av testplaner, förväntat resultat och faktiskt resultat

SATS_ANG.C3
Testplanerna ska beskriva de tester som ska genomföras och scenariot för varje test. Beskrivningarna ska vara så detaljerade att testerna kan reproduceras

SATS_ANG.C4
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.C5
Det faktiska testresultatet ska överensstämma med det förväntade testresultatet

SATS_ANG.E1
Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SATS_EVL – Evaluerarens testning

Detta krav omfattar den testning som evalueraren ska genomföra för ett system. Evaluerarens testning omfattar både att upprepa systemutvecklarens funktionella och angripartester (helt eller delvis) och att utöka dessa tester (omfattning och djup) med evaluerarens egna tester. Dessa utökade tester är tänkta att komplettera, inte ersätta, systemutvecklarens tester på ett meningsfullt sätt. Evaluerarens testning måste därmed bygga på såväl en analys av de befintliga testerna som komplexiteten hos systemet och dess säkerhetsfunktionalitet.

Ett system är möjligt att testa bara om det görs tillgängligt för evalueraren. Detta inbegriper dock inte bara systemet, utan hela testmiljön, med verktyg, dokumentation och testsviter. Ett system och dess testmiljö kan dock vara för

stort eller komplext för att kunna transporteras till evalueraren. För dessa fall skulle evaluerare kunna ges möjlighet att genomföra sina tester hos systemutvecklaren så länge det garanterar insyn och oberoende för testresultatet. Komponenter i detta krav stegras genom att mängden oberoende testning som evalueraren måste genomföra ökas.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SATS_EVL.	**D1**	**D2**	**C1**	**E1**	**E2**	**E3**	**E4**
Grund	X	X	X	X	X		
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SATS_EVL.D1

Systemutvecklaren ska tillhandahålla systemet för testning

SATS_EVL.D2

Systemutvecklaren ska tillhandahålla motsvarande uppsättning testresurser som de som systemutvecklaren använde vid den funktionella testningen

SATS_EVL.C1

IT-systemet ska vara i testbart skick

SATS_EVL.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SATS_EVL.E2

Evalueraren ska, om denne finner det nödvändigt, upprepa ett representativt antal av systemutvecklarens tester och bekräfta att systemutvecklarens testresultat för dessa testfall

SATS_EVL.E3

Evalueraren ska analysera systemutvecklarens testfall och komplettera dessa testfall med egna testfall

SATS_EVL.E4

Evalueraren ska genomföra de egna testfallen, dokumentera resultatet och bekräfta att systemet fungerar enligt specifikation

2.7 SARA – Riskanalys och sårbarhetsanalys

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.

Klassen SARA består av tre krav:

- Avvikelseanalys (SARA_AVV) omfattar krav på systemutvecklaren att identifiera alla avvikelser och dokumentera dessa, avvikelserna verifieras därefter av evalueraren.
- Sårbarhetsanalys (SARA_SBH) omfattar krav på evaluerare att leta efter möjliga sårbarheter och för varje upptäckt sårbarhet se om den skulle kunna utnyttjas i systemets tänkta miljö.
- Restriskanalys (SARA_RRA) omfattar krav på avdömning huruvida avvikelserna (osäkerheterna) och eventuellt identifierade sårbarheter i det totala systemet innebär en kvarstående risk som kan anses vara acceptabel eller ej.

SARA_AVV – Avvikelseanalys

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. Systemutvecklaren ska visa att åtgärderna är tillräckliga för att förvissa sig om att risken med avvikelsen korrekt beskrivits.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARA_AVV.	**D1**	**C1**	**C2**	**C3**	**C4**	**C5**	**E1**
Grund	X	X	X	X	X	X	X
Utökad	X	X	X	X	X	X	X
Hög	X	X	X	X	X	X	X

SARA_AVV.D1

Systemutvecklaren ska tillhandahålla en avvikelseanalys

SARA_AVV.C1

Avvikelseanalysen ska omfatta alla avvikelser från den godkända konfigurationen för alla systemets säkerhetsrelevanta komponenter

SARA_AVV.C2

Avvikelseanalysen ska omfatta alla avvikelser från den i godkännandet avsedda användningen av alla systemets säkerhetsrelevanta komponenter

SARA_AVV.C3

Avvikelseanalysen ska omfatta alla avvikelser från de i godkännandet beskrivna antaganden om systemets utformning för alla systemets säkerhetsrelevanta komponenter

SARA_AVV.C4

Avvikelseanalysen ska för varje avvikelse visa vilken inverkan den har och hur den har hanterats

SARA_AVV.C5

Avvikelseanalysen ska visa att åtgärderna som vidtagits för att hantera avvikelserna är effektiva

SARA_AVV.E1

Evalueraren ska verifiera att informationen i underlaget möter alla krav på innehåll och presentation

SARA_SBH – Sårbarhetsanalys

Kravet innebär att en sårbarhetsanalys ska genomföras för att identifiera eventuella sårbarheter i systemet som skulle kunna utnyttjas i systemets driftmiljö. Det är evalueraren som ska leta efter sårbarheter. Det är systemutvecklarens ansvar att se till att systemet befinner sig i ett testbart skick som möjliggör att sårbarhetsanalys och praktiska tester kan genomföras.

Sårbarhetsanalysen är inte en isolerad evalueringsaktivitet för evalueraren utan det åligger evalueraren att under alla andra evalueringsaktiviteter aktivt använda den information som sammanställts för att leta efter potentiella sårbarheter som senare används vid sårbarhetsanalysen.

Komponenter i detta krav stegras genom en ökad grad av metodik och formalism i sårbarhetsanalysen som evalueraren ska genomföra. Innebörden av metodisk och semiformell beskrivs av den evalueringsmetodik som evalueraren ska följa.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARA_SBH.	**D1**	**C1**	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E7**
Grund	X	X	X	X	X	X			
Utökad	X	X	X	X	X		X		X
Hög	X	X	X	X	X			X	X

SARA_SBH.D1

Systemutvecklaren ska tillhandahålla systemet för testning

SARA_SBH.C1

IT-systemet ska vara i testbart skick

SARA_SBH.E1

Evalueraren ska verifiera att informationen i leverantörens dokumentation är tillräcklig för att utföra en grundlig sårbarhetsanalys av hela systemet

SARA_SBH.E2

Evalueraren ska använda tillgängliga källor för att komplettera leverantörens dokumentation, t.ex. publik sårbarhetsinformation

SARA_SBH.E3

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.E4

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.E5

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.E6

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.E7

Evalueraren ska genomföra praktiska tester av systemet för att avgöra om de potentiella sårbarheterna kan utnyttjas i den tänkta användningen av systemet

SARA_RRA – Restriskanalys

Kravet syftar till att identifiera sårbarheter och osäkerheter för systemets säkerhetsförmågor. Identifierade osäkerheter ska värderas tillsammans med de resterande sårbarheter som eventuellt identifierats under sårbarhetsanalysen för att ge ett beslutsunderlag för en avdömning av systemet.

Restriskanalysen sker uteslutande av evalueraren med hjälp av det underlag som krävts under de andra assuranskraven, inget ytterligare underlag eller analys erfordras från systemutvecklaren. Det innebär att restriskanalysen sker som det sista steget i en systemevaluering.

Av följande tabell framgår vilka kravkomponenter som gäller vid respektive kravnivå:

SARA_RRA.	**E1**	**E2**	**E3**
Grund	X	X	X
Utökad	X	X	X
Hög	X	X	X

SARA_RRA.E1

Evalueraren ska verifiera att alla andra evalueringsaktiviteter är genomförda med godkänt resultat

SARA_RRA.E2

Evalueraren ska genomföra restriskanalys för att identifiera kvarvarande osäkerheter kring systemets IT-säkerhetsförmågor

SARA_RRA.E3

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