Något om KSF 3.1 och säkerhet i IT-system

Innehåll

Vad är KSF?

- KSF betyder helt enkelt ”**K**rav **S**äkerhets**F**unktioner”. Det är en kravmassa framtagen av Svenska Försvarsmakten (FM) och används vid upphandling av IT-system för FM och FM-nära myndigheter:
    - Försvarets materielverk (FMV)
    - Försvarets radioanstalt (namnet till trots, en civil signalspaningsmyndighet, FRA)
    - Totalförsvarets forskningsinstitut (FOI)
    - Försvarshögskolan (FHS)
    - Totalförsvarets rekryteringsmyndighet (TRM)
- På senare år har även rent civila myndigheter som har uppgifter inom totalförsvaret visat intresse för att använda KSF. Användningen av KSF förväntas alltså öka.

- Ett exempel på användning är när FMV i Industrisäkerhetsskyddsmanualen (ISM 2013) klippt in delar av den äldre KSF 2.0 från 2004 och ställt kravet att IT-system hos försvarsindustrin ska uppfylla kraven om det system som levereras skall hantera hemlig information som rör rikets säkerhet[1].

- KSF är den mest detaljerade kravspecifikationen för IT-system som överhuvudtaget existerar hos svenska myndigheter.

- KSF kom i version 2.0 redan 2004, men den KSF som gäller i dag i Försvarsmakten är version 3.1 från 2014. Det talas dock om att en ny version borde tas fram, särskilt med tanke på att nya Säkerhetsskyddslagen trädde i kraft 2019, men ännu (november 2020) har inget skett.

- En intressant summering av 12 års riskbedömning av Försvarsmaktens IT-system finns hos FOI.

- Sammanfattande om rutiner och regelverk för godkännande av IT-system kan man läsa här.

- Det finns också andra styrande FM-dokument om IT-säkerhet som man bör känna till, t ex

    - Handbok Säkerhetstjänst Grunder, H SÄK Grunder
    - Handbok Säkerhetstjänst Informationssäkerhet, H SÄK Infosäk

Nya Säkerhetsskyddslagen 2019 (2018:585)

- 2019-04-01 trädde den nya nya svenska säkerhetsskyddslagen i kraft. Den ersätter i stora delar den tidigare

- I den lagen talas det nu om ”**säkerhetsskyddsanalys”**. Med detta menas att utreda behov av säkerhetsskydd (till exempel enligt NIS-direktivet). När analysen är gjord skall man

    - planera och vidtaga de åtgärder som analysen ansett nödvändiga

    - genomföra kontroller av säkerhetsskyddet

- tydligare och mer omfattande krav på organisationer som bedriver säkerhetskänslig verksamhet.

- Krav på att man inventerar och klassificerar IT-system och information.

- Breddad definition av vad som klassas som ”*säkerhetskänslig verksamhet*”

- Lagen har särskilt fokus på konfidentialitet och delar in uppgifter i ”*säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet*”.

- Säkerhetsklassificering görs till någon av dessa kategorier:

[1] ”Rikets säkerhet” ersattes med ”Sveriges säkerhet” i nya Säkerhetsskyddslagen (2019).

Menlighetsbedömning	Säkerhetsskyddsnivå[2]
Synnerligen allvarlig skada för Sveriges säkerhet	KVALIFICERAT HEMLIG
Allvarlig skada för Sveriges säkerhet	HEMLIG
Inte obetydlig skada för Sveriges säkerhet	KONFIDENTIELL
Ringa skada för Sveriges säkerhet	BEGRÄNSAT HEMLIG
Inte mätbar eller inte relevant konsekvens med bäring på Sveriges säkerhet	Ingen säkerhetsskyddsklass (öppen information)

- Lagen fokuserar inte lika mycket på andra aspekter av datasäkerhet, t ex riktighet (ej manipulerade data) eller tillgänglighet (ej utslagna/otillgängliga data), enbart sekretess i meningen konfidentialitet (ej röjda uppgifter). Sådant täcks dock in av andra lagar, där det t ex står att inte uppgifter obehörigen ”*ändras, görs otillgängliga eller förstörs*”.

- I propositionen inför den nya säkerhetsskyddslagen skrev regeringen att det vore ”*mycket svårt för verksamhetsutövare att placera uppgifter i en viss säkerhetsskyddsklass utifrån vilka risker det skulle innebära för Sveriges säkerhet om uppgifterna förvanskas, förstörs eller görs otillgängliga*”.

De 7 säkerhetsfunktionerna

- 7 krav på godkända säkerhetsfunktioner i IT-system (Säkerhetspolisen, SÄPO och Försvarsmakten, MUST):

Säkerhetsfunktion	Säkerhetspolisen (SÄPO)	Försvarsmakten (MUST)
Behörighetskontroll	Ja men endast IT-system som är avsedda att användas av flera personer	Ja men endast IT-system som är avsedda att användas av flera personer
Säkerhetsloggning	Ja men endast IT-system som är avsedda att användas av flera personer	Ja men endast IT-system som är avsedda att användas av flera personer
Skydd mot skadlig kod (t ex antivirus)	Ja	Ja
Intrångsskydd (IDS)	Ja men endast om systemet kommunicerar med andra system	Ja
Intrångsdetektering	Behövs ej om systemet är avsett för hemliga uppgifter som endast ger ringa men	Behövs inte för IT-system högst avsett för hemliga uppgifter upp till HEMLIG/RESTRICTED (fr o m 2019 ”BEGRÄNSAT HEMLIG”)
Skydd mot röjande signaler (RÖS-skydd)	Om det behövs, kräver analys	Behövs inte för IT-system högst avsett för hemliga uppgifter upp till HEMLIG/RESTRICTED (fr o m 2019 ”BEGRÄNSAT HEMLIG”)
Skydd mot obehörig avlyssning	Ja	Ja

[2] Dessa nivåer ersätter de tidigare klasserna ”Hemlig/Top Secret – Hemlig/Secret – Hemlig/Confidential – Hemlig/Restricted” från Offentlighets- och sekretesslagen (2009:400) (OSL) 15 kap 2 §.

- Sammanfattningsvis kan man säga att FM i praktiken ställer tekniska krav på:
    - omfattande loggning av alla viktiga händelser inom systemen
    - inloggning
    - systemen skall vara moderna, supporterade och patchade (gäller inte minst operativsystem och antivirus).

KSF 3.1 (2014)

- KSF 3.1 innehåller 148 krav på säkerhetsförmågor för de sju säkerhetsfunktionerna (***funktionella säkerhetskrav***).

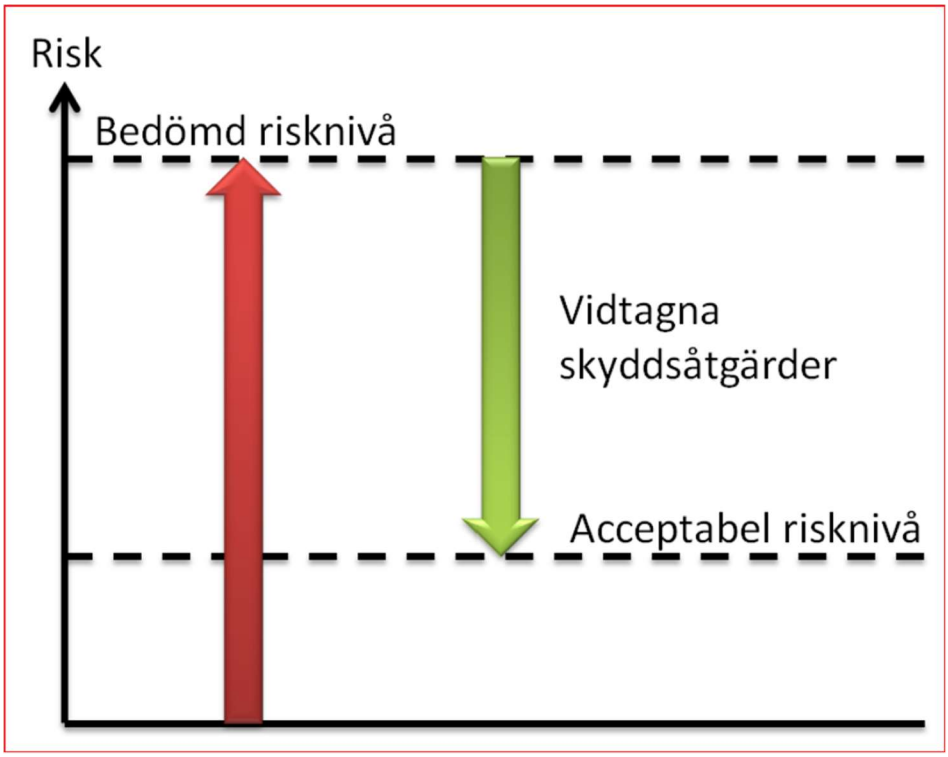
- KSF 3.1 innehåller 275 krav på hur man påvisar förtroende för säkerhetsförmågorna (***assuranskrav***).

- KSF 3.1 är en komplicerad kravmassa som måste tolkas för varje IT-system. Ett funktionellt säkerhetskrav kan innebära att en skyddsåtgärd måste finnas i flera delar av systemet. Det är sådana tolkningar som dokumenteras i IT-säkerhetsspecifikationen (ITSS). Att ta fram ITSS är en stor del av arbetet med de säkra IT-systemen för FM. ITSS tas fram för komponenter/delsystem och för hela lösningen (systemet).

- Det är också denna kravtolkning som sedan kan användas som en kravspecifikation för upphandling.

- De ”nakna” KSF-kraven är sällan meningsfulla att använda för att upphandla utveckling av ett IT-system, utan kräver den tolkning som görs för att kunna nyttjas i upphandling, som produktkrav.

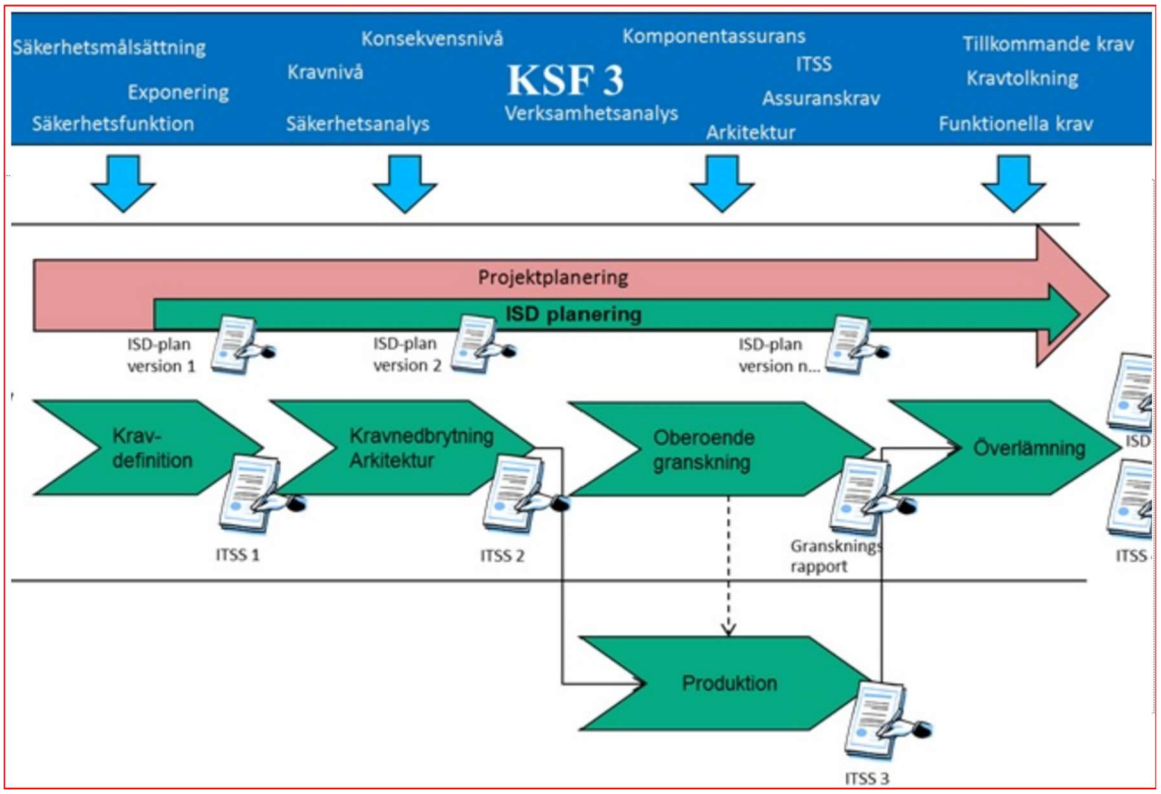
- För varje identifierad risk i utredningen skall en skyddsåtgärd föreslås så att man hamnar på en hanterbar risknivå.



Figur 1 KSFs relation mellan bedömd risk och risknivå efter att skyddsåtgärd är vidtagen.

Översikt över processerna

- FM och FMV använder olika processmodeller som inte riktigt går i ”takt” med varandra:
    - FM: IT-processen
    - FMV: ISD



Figur 2 FMVs flödesbild för ISD-processen

- Nyligen tog FMV fram processen ISD 3.0. Informationssäkerhetsdeklaration (ISD) är en stödprocess för informationssäkerhetsarbetet inom produktionsprocessen på FMV.
- ISD är en omfattande process som täcker in aspekter om bl a
    - Ackrediterbarhet
    - Konstnadseffektivitet
    - Projektaspekter inklusive
        - Risker
        - Definition av Milestones/Tollgates
        - Roller
    - Integration
    - Realiserbarhet
    - Vidmakthållande (svenskt ord för *Maintenance*)
    - Krav på Oberoende granskning
- Arbetet inom processerna utgår från TVÅ ingångsvärden när det gäller att fastställa den kravnivå som ett IT-system[3] måste uppfylla:
    - **Konsekvensnivå**
    - **Exponeringsnivå**
- Dessa värden vägs samman enligt en speciell matris för att bestämma **kravnivån** för systemet, vilken då antingen blir antingen

---

- [3] *Notera att alla frågor kring **kryptoapparater** går helt utanför dessa IT-processer. **Försvarskrypton** har särskilda ”komponentgodkännanden” som utfärdas av MUST.*

    - **Grund**
    - **Utökad**
    - **Hög**
- Kravnivån i sin tur nyttjas till att peka ut de specifika säkerhetskrav som IT-systemet måste uppfylla enligt KSF. Högre nivå innebär sålunda att fler, och mer omfattande, krav måste uppfyllas och dokumenteras.

Konsekvensnivå

- Konsekvensnivå är den skada som uppstår om en incident, till exempel en förlust av informationssekretess, inträffar (alltså exponering av hemliga data).
    - Är direkt beroende av hur informationen är klassad.
    - Anges 1-5:
        5: Synnerligen allvarlig konsekvens vid informationsförlust
        4: Allvarlig konsekvens
        3: Kännbar konsekvens
        2: Lindrig konsekvens
        1: Försumbar konsekvens

Exponeringsnivå

- Exponering kan vara både fysisk och logisk och avse både personer och informationsutbyten.
- Exponering kan ”smitta” mellan system. Tar hänsyn till personer och andra IT-system som kan komma i kontakt med aktuellt system.
- Anges E1-E4 där E1 = lägsta, mycket kontrollerad miljö med enbart behöriga personer, utan koppling till andra IT-system (typ inlåsta stand-alone-datorer utan nätverk), och E4=ej säkerhetsprövade personer, kopplingar till icke-kontrollerade och exponerade system (läs: Internet) enligt:

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

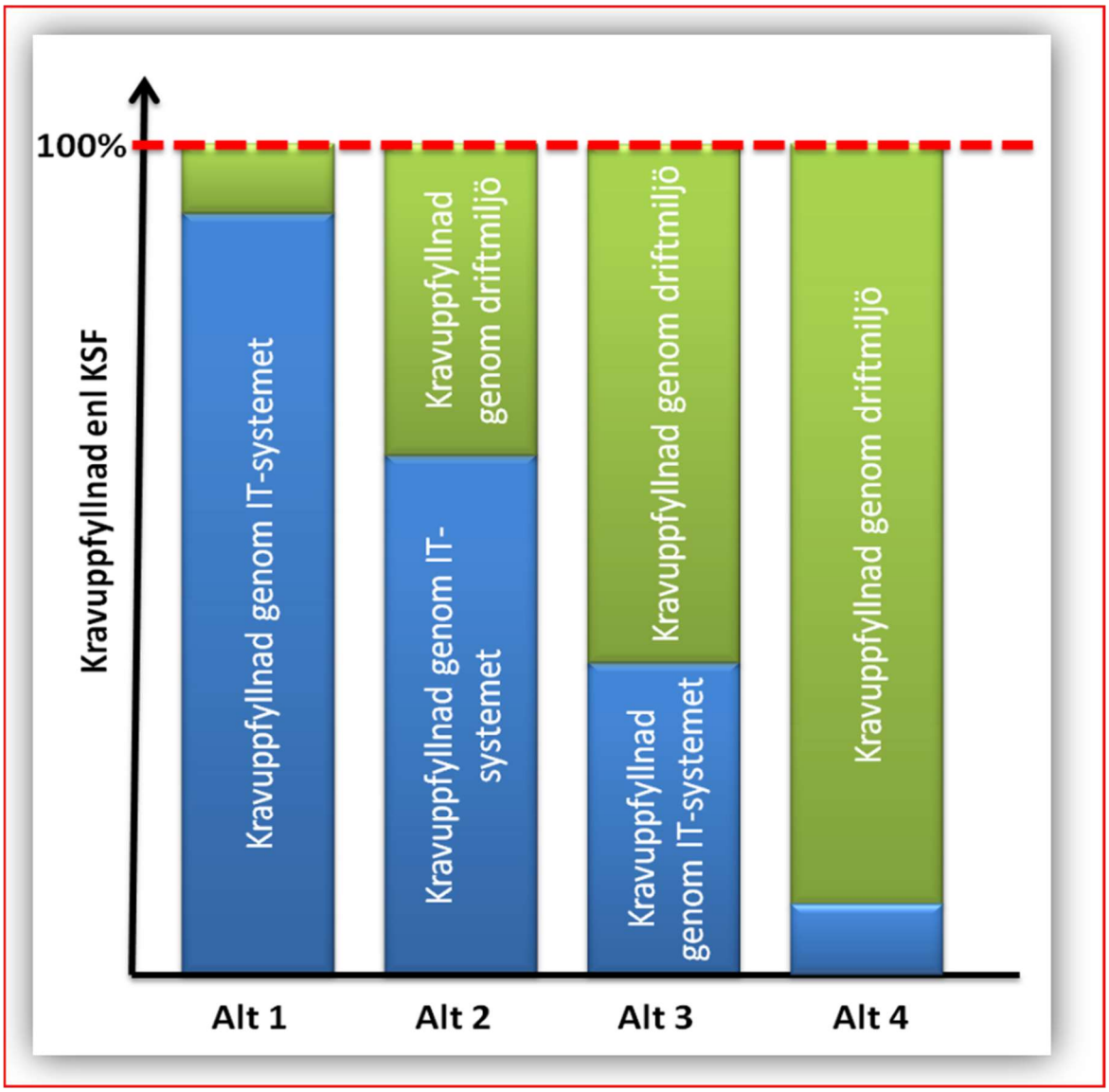
Figur 3 Beskrivning av Exponeringsnivåer

Konsekvensnivå	Exponeringsnivå			
	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

Figur 4 Nivåmatris som funktion av konsekvens och exponering i KSF.

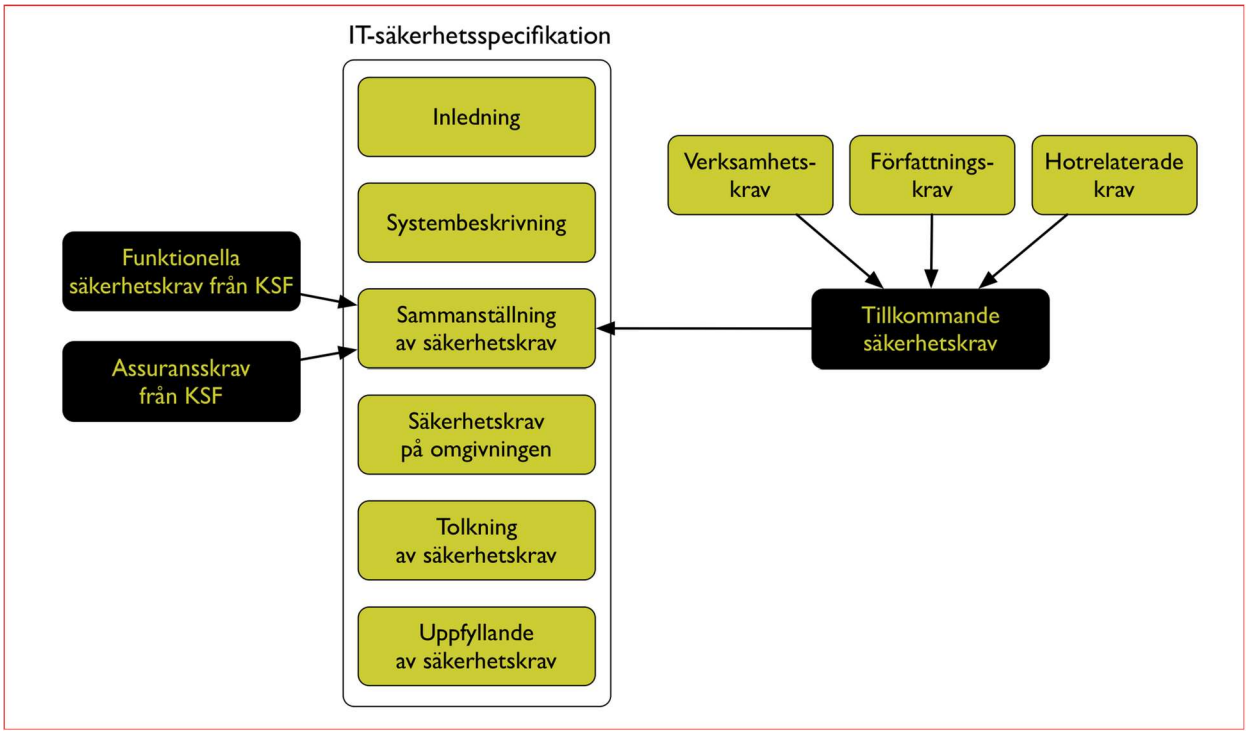
Kravnivåer

- När ett system hamnar på en högre nivå än **GRUND** i KSF innebär det att fler säkerhetskrav måste uppfyllas.
- Krav kan uppfyllas *antingen* helt som en teknisk lösning, eller helt som en handhavande-regel (dvs lösas ute i driftmiljön) *eller* som en sorts blandning av dessa, men det måste visas för varje säkerhetskrav hur det skall lösas:



Figur 5 figur ur KSF-instruktionerna. Ett säkerhetskrav måste uppfyllas till 100%, men detta kan göras på olika sätt – Alt 1 visar hur IT-systemet uppfyller nästan hela kravet, Alt 4 visar hur driftmiljön (instruktioner, handhavanderegler, reglemente, fysiskt skydd, bevakning…) istället får uppfylla kravet. Exempelvis kan en dator med hemlig uppgift som ej har inloggning istället bevakas 24 timmar om dygnet.

- Det är systemutvecklarens ansvar att för aktuellt IT-system påvisa såväl ATT kravuppfyllnad föreligger som HUR kravuppfyllnad erhålls för de funktionella och assuranskraven. Detta är det stora säkerhetsarbetet när ett IT-system skall tas fram åt Försvarsmakten!



Figur 6 tillkommande säkerhetskrav som kommer från analyser utanför KSF tas in i ITSS-arbetet.

ITSS (IT Säkerhetsspecifikation) och tillkommande krav

- Beskriver systemet, vilka säkerhetskrav som systemet ska uppfylla samt hur systemet uppfyller kraven.
- Strukturen på en ITSS för ett system och det förväntade innehållet är tydligt angivet i KSF.
- KSF-kraven är inte uttömmande, då det inte är möjligt att genom generella krav förutse alla tänkbara säkerhetsegenskaper som ett IT-system måste ha. KSF är således en miniminivå.
- I ITSS finns plats för *tillkommande säkerhetskrav*, vilka kommer från analyser som ligger utanför KSF. Exempelvis
    - verksamhetens krav på tillgänglighet
    - författningskrav som gäller för verksamheten som systemet ska stödja eller informationen i systemet
    - hotrelaterade krav unika för den plats där systemet ska finnas

Klasser av funktionella krav i KSF

De olika underkraven per område gäller i olika utsträckning för om man jobbar med ett system på kravnivå Grund, utökad eller Hög. Här visar vi bara den första nivån av kravdetaljering, men det finns ytterligare nivåer av underkrav i KSF.T ex gäller kravet **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.” enbart för kravnivå HÖG.*

- **Gemensamma krav (SFGK)** – Funktionella säkerhetskrav som är gemensamma för alla säkerhetsfunktioner. Samtliga säkerhetsfunktioner i systemet skall omfattas av, men inte begränsas till, dessa krav.
    - SFGK_FEL - Säkerhetsfunktioner ska kunna upprätthålla ett säkert tillstånd vid fel

    - SFGK_TID - Säkerhetsfunktionen ska använda systemets gemensamma tid

- **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.
    - SFBK_UID – Subjekt ska ha en unik identitet
    - SFBK_AUT – Autentisering av subjekt ska ske
    - SFBK_ÅTK - Subjekt ska endast ges åtkomst till objekt som de är behöriga till
    - SFBK_ADM - Administration av behörighetskontroll ska ske på ett säkert sätt
- **Intrångsdetektering (SFID)** – Kraven i klassen intrångsdetektering skall säkerställa att pågående samt redan genomförda intrång i systemet kan upptäckas och åtgärdas.
    - SFID_DAT - Information från relevanta datakällor ska vara tillgängliga för analys
    - SFID_ANA - Intrång och missbruk ska kunna upptäckas och spåras
- **Intrångsskydd (SFIS)** – Kraven i klassen intrångsskydd skall säkerställa att system skyddas mot obehörig åtkomst.
    - SFIS_HRD – Systemets komponenter ska härdas mot intrång
    - SFIS_INT - Kommunikation ska skyddas mot otillbörlig åtkomst och manipulation
    - SFIS_KIN - Information som passerar in genom systemets gränsytor ska kontrolleras
    - SFIS_KUT - Information som flödar ut ur systemet ska kontrolleras
- **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.
    - SFSK_UPD - Funktioner för hantering av säkerhetsuppdateringar ska finnas
    - SFSK_RIK - Riktighetskontroll av mjukvara och konfigurationer ska vara möjlig
    - SFSK_EXE - Endast godkänd mjukvara ska kunna exekvera i systemet
    - SFSK_KUT - Skadlig kod ska ej kunna spridas via systemet
    - SFSK_KIN - Skadlig kod ska ej kunna föras in i systemet
- **Säkerhetsloggning (SFSL)** – Kraven i klassen säkerhetsloggning skall säkerställa att spårning av missbruk, och försök till missbruk av systemet kan genomföras.
    - SFSL_REG - Säkerhetsrelaterade händelser ska registreras
    - SFSL_OAV - Användare ska kunna göras individuellt ansvariga för sina åtgärder

    - SFSL_SKY - Säkerhetsloggar ska ej kunna förvanskas eller förstöras
    - SFSL_ANA - Säkerhetsloggar ska analyseras för att upptäcka intrång och missbruk
- **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.
    - SFRS_REG - RÖS krav från gällande regelverk ska uppfyllas
- **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.
    - SFOA_KBL – Hemliga uppgifter i elektroniska kommunikationsnät ska skyddas

Struktur för assuranskraven i KSF

Med stegrande kravnivå (Grund → Utökad → Hög) ställs ökande krav på underlagens omfattning, fullständighet och detaljeringsgrad.

- **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.
    - SASS_INL – ITSS Inledning
    - SASS_SYS – Systembeskrivning
    - SASS_KRV – Sammanställning av säkerhetskrav
    - SASS_OMG – Säkerhetskrav på omgivningen
    - SASS_TOL – Tolkning av säkerhetskrav
    - SASS_UPF – Uppfyllande av säkerhetskrav
- **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.
    - SALC_UTV – Utvecklingssäkerhet
    - SALC_KFG – Konfigurationsledning
    - SALC_LEV – Systemleverans
    - SALC_LCM – Livscykelmodell
    - SALC_BRK – Bristkorrigering

- **Arkitektur och design (SADE)** – Klassen omfattar assuranskrav på tekniska egenskaper i IT-systemets design och konstruktion, dvs. egenskaper hos systemet och dokumentationen av dem.
    - SADE_GRÄ – Gränsytebeskrivning
    - SADE_ARK – Säkerhetsarkitektur
    - SADE_DFA – Dataflödesanalys
    - SADE_DES – Designdokumentation
- **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.
    - SAOP_INS – Installation och förberedelser
    - SAOP_DOK – Drift- och förvaltningsdokumentation
    - SAOP_BRK – Bristkorrigering
- **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.
    - SARU_ÅTK – Åtkomsträttigheter
    - SARU_ATT – Säkerhetsattribut för autentisering
    - SARU_INT – Upptäcka och spåra intrång och missbruk
    - SARU_UPD – Säkerhetsuppdateringar
    - SARU_KFG –Konfigurationsstyrning
    - SARU_UTB – Säkerhetsutbildning av användare
- **Systemintegrationstest (SATS)** – Klassen omfattar assuranskraven för systemtestning som visar att systemutvecklaren verifierat IT-säkerhetsfunktionaliteten hos systemet.
    - SATS_TTK – Testtäckning
    - SATS_FUN – Funktionstester
    - SATS_ANG – Angripartester
    - SATS_EVL – Evaluerarens testning
- **Sårbarhetsanalys och Restriskanalys (SARA)** – Klassen omfattar den sårbarhetsanalys som genomförs av evalueraren, till största delen baserat på underlag från andra assuransfamiljer.
    - SARA_AVV – Avvikelseanalys

- SARA_SBH – Sårbarhetsanalys
- SARA_RRA – Restriskanalys

Tekniska aspekter från Försvarsmakten

- Virtualisering innebär en abstraktion mellan applikation och hårdvara. Detta möjliggörs med hjälp av en s k Hypervisor, ett virtualiseringslager, mellan den riktiga hårdvaran och det som snurrar ovanför. Fördelarna är att portabilitet ökar, vilken applikation som helst kan köras på vilken hårdvara som helst. Detta är särskilt populärt och eftertraktat inom ffa containertekniken (t ex Kubernetes/Docker) och virtuella maskiner (VMar), tekniker som används frekvent inom moderna Cloudbaserade miljöer.
    - MUST har givit ut en vägledning (skrivelse FM2017-5296:2) om virtualisering och säkerhet. Hypervisorer skall inte anses säker teknologi för att separera säkerhetsdomäner. Alltså kan man inte i en FM-godkänd lösning köra olika applikationer med olika informationssäkerhetsklasser på samma hypervisor. ”*Vad gäller IT-system med höga säkerhetskrav avseende åtkomstseparation för drift och förvaltning, (separation of duties) kan virtualisering vara ett olämpligt val av lösning. Svårigheten är att korrekt kunna definiera roller och behörigheter på ett sådant sätt att en person inte får för stor tillgång till viktiga infrastrukturkomponenter såsom virtuella switchar, brandväggar, databaser etc*”.

- VLAN är inte fullgod separationsteknik mellan säkerhetsdomäner.
- I princip kan man säga att inga kommersiella tekniker klarar Försvarsmaktens krav på sekretess. Där duger bara de egna kryptona, som komponentgodkännes i separata processer, som vi skrivit tidigare. Således kan VPN, IPsec, TLS, etc enbart anses vara skydd över en förbindelse/länk, men aldrig anses skydda något klassat innehåll.
- IPv6: Redan 2005 beslutade FMV (VO LED 12870:74627/2005) att ”*maskin- och programvara som anskaffas av FMV för ändsystems (hosts) IP-kommunikation skall ha dubbla protokollstackar och kunna fungera som host i såväl nät med IPv4 som nät med IPv6. Ändsystemen skall kunna fungera i IPv6-nät med protokollstacken för IPv4 avstängd eller avinstallerad.”*

Kritik och brister i KSF

- De höga nivåerna på kraven gör att det är svårt att evaluera dem. Ingen metodik eller manual finns för detta. Evalueringar genomförs kanske inte alls, eller så genomförs de på olika sätt och med olika måttstockar i olika projekt, och de löper risken av att vara av för låg kvalitet.
- KSF anses vara en komplicerad uppsättning krav som är svårt att bemästra, även för säkerhetsexperter. Detta gäller i synnerhet assuranskraven.
- Det finns ingen utbildning i KSF-metodik (även om det förr har funnits inom FMV). Det finns ingen mall för hur ITSS skall utformas.

- Fel rättas inte, ingen förvaltning som underhåller KSF finns idag. En del obegripligheter kvarstår sedan många år.
- Guider saknas, för hur krav skall uppfyllas. Detta vore av särskilt intresse i de fall där det finns alternativa lösningar, t ex vid arkitekturval. Även i de fall där teknologiutveckling skett saknas guider. Ett tydligt exempel är problemen med virtualisering och hypervisorer.
- Tillkommande krav till ITSS- arbetet från nya säkerhetsskyddslagens säkerhetsanalys – nya krav kan komma in från hot/risk/sårbarhetsanalys.
- Inga andra aspekter av CIA-triaden (Confidentiality, Integrity, Availability) än C tas om hand.
- Somliga bedömare anser konsekvensnivå/exponering vara för snäva kriterier vilket försvårar säkerhetsarbetet, eftersom man i praktiken ofta tvingas utgå från den högsta hotbilden, vilket i sin tur driver kravnivån onödigt högt upp. Fler faktorer som skulle kunna påverka kravnivån tas inte om hand i befintligt regelverk. Som exempel kan nämnas obfuscation, system som hålles okända, vilken profil en hotvektor kan förväntas ha (skillnad på t ex tonårshacker och ryska GRU). Även faktorer som antal användare, antal platser och inloggningar, informationsmängder skulle kunna tas med som faktorer som påverkar kravnivån, menar man.

Summering

- KSF är den mest omfattande myndighetsspecifikation för högnivåkrav på IT-system som existerar i landet.
- KSF används som indatakrav i de processer (SD, IT-processen) som FMV och FM använder.
- KSF behöver tolkas och tillkommande krav måste tas in. Detta görs i de olika ITSS-dokumenten.
- KSF, ITSS och ISD är omfattande processer som, rätt implementerade, säkerställer att högt ställda krav på säkerhet i IT-system realiseras och dokumenteras. Detta är nödvändigt för att system som bär sekretess och viktiga uppgifter åt totalförsvaret alls skall kunna existera och göra nytta.