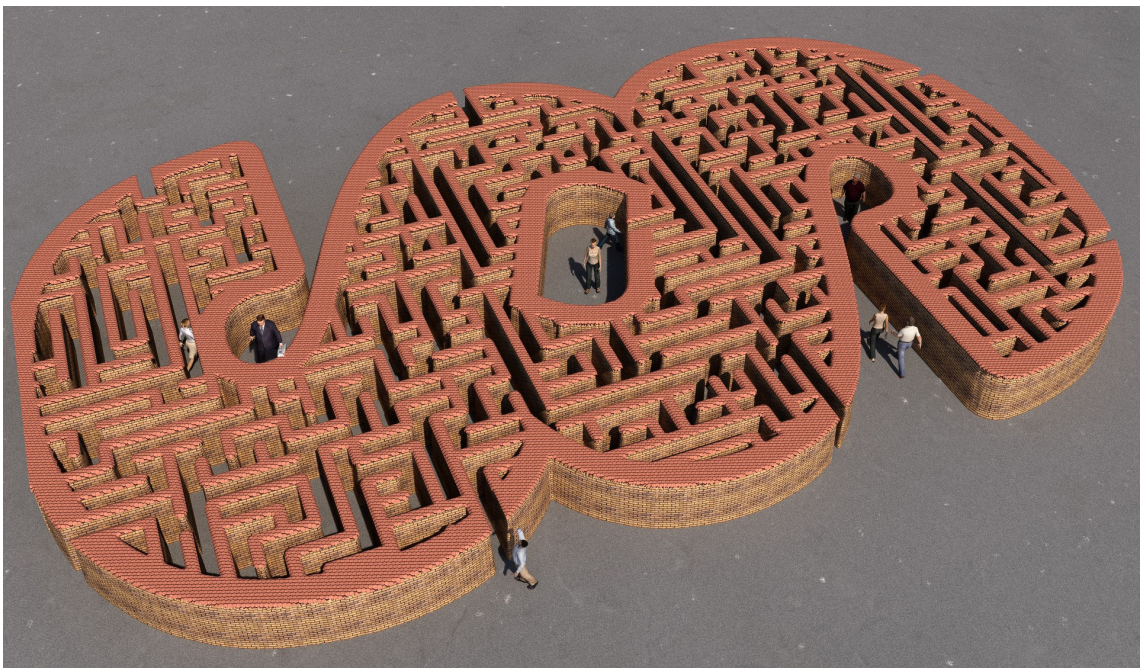
Rutiner och regelverk för att godkänna IT-system i Försvarsmakten

AMUND GUDMUNDSON HUNSTAD



FOI-R--4526--SE
ISSN 1650-1942 December 2017

FOI-R-- 4526 --SE

Amund Gudmundson Hunstad

Rutiner och regelverk för att godkänna IT-system i Försvarsmakten

Titel	Rutiner och regelverk för att godkänna IT-system i Försvarsmakten
Title	Procedures and regulations for approval of IT-systems of the Swedish Armed Forces
Rapportnr/Report no	FOI-R--4526--SE
Månad/Month	December
Utgivningsår/Year	2017
Antal sidor/Pages	27
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E72677
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

Regler och rutiner ställer krav på Försvarsmaktens godkännande av IT-system ur IT-säkerhetsperspektiv för att godkännandet skall bli tillförlitligt och relevant.

Observationer från IT-försvarsdagen 2017 indikerar brister och svårigheter inom cybersäkerhetsområdet. Med detta som startpunkt beskriver denna rapport vad som utgör ramarna för godkännande i termer av normsättande regelverk och hur tre olika rutiner för arbete med godkännande av IT-system har utarbetats vid Försvarets Materielverk och Försvarsmakten. De tre olika rutinerna jämförs på en övergripande nivå.

Studien slutsats är att regler och rutiner är nödvändiga, men att deras användande inte med självklarhet når fram till snabba och tillförlitliga beslut om godkännande. Regler och rutiner har ett fokus på sekretess, samtidigt som tillgänglighet och integritet också är nödvändigt för adekvat och relevant säkerhet.

Nyckelord: IT-säkerhet, ackreditering, auktorisation, informationssäkerhetsdeklaration, Försvarsmaktens IT-process, informell granskning

Summary

Requirements for the Swedish Armed Forces approval from an IT-security perspective of IT-systems is set by procedures and regulations, which contribute to reliable and relevant IT-system approvals.

FOI arranged an IT-defence focused day of seminars the 8th of November 2017, during which observations indicating deficiencies and difficulties within the cyber security domain where made. With these observations as a starting point, this report describes the scope of approval in terms of normative regulations and how three different procedures for handling approval of IT-systems have been developed within the Swedish Defence Materiel Administration and the Swedish Armed Forces. On a general level the three different procedures are compared.

As a conclusion, this study concludes that procedures and regulations are requisites, but it is not obvious that their usage leads to immediate and reliable decisions of approval. Procedures and regulations focus on confidentiality, while availability and integrity also is necessary for adequate and relevant security.

Keywords: IT-security, accreditation, authorization, information security declaration, IT-process of the Swedish Armed Forces, informal inspection

Innehållsförteckning

1 Inledning

Försvarsmaktens IT-system hanterar verksamhetskritisk information och utgör kritiska framgångsfaktorer för Försvarsmaktens syfte, mål och verksamhet. För att uppnå verksamhetens syften och mål krävs såväl detaljerade som övergripande säkerhets- och riskavvägningar med utgångspunkt i verksamhetens behov.

Detta innebär att hur systemutvecklingen genomförs och hur godkännandet av IT-system sker i sig blir kritiska framgångsfaktorer. Systemutveckling beskrivs ofta i termer av olika steg i livscykeln för ett system. Typiska utvecklingssteg kan vara *koncept-utveckling-produktion-drift-underhåll-avveckling*.

Godkännande av system bör beakta olika så kallade funktionella, så väl som icke-funktionella, krav (Hansson, Granlund, Hallberg, 2011). Funktionella krav relaterar till IT-systemens primära roll eller funktion för verksamheterna där de används. Icke-funktionella krav relaterar till övriga, kompletterande krav utöver de primära, funktionella. IT- och informationssäkerhet är exempel på viktiga icke-funktionella krav.

För att säkerställa att godkännande av IT-system baserar sig på väldefinierade underlag och arbetssätt samt ger spårbara resultat, krävs rutiner och regelverk. Syftet med denna studie är att beskriva det spektrum av olika processer, arbetssätt och formaliserade styrdokument och krav som ingår i godkännanden av Försvarsmaktens IT-system. För att tydliggöra och förenkla beskrivningen av detta spektrum används så väl termen *rutiner* som termen *regelverk*.

Med *rutiner* avses vad som också kan beskrivas som processer och arbetssätt. Rutiner kan vara strikt styrda och definierade av grundlagar, lagar, förordningar, myndighetsinterna dokument och handböcker etc. Rutiner kan också vara mer ad hoc-mässiga och med liten eller avgränsad styrning. Med *regelverk* avses här formaliserade styrdokument, lagar, förordningar etc. Regelverk ger därmed en striktare styrning av hur godkännanden av IT-system går till.

1.1 Avgränsningar

Rapportens studiefokus är avgränsat. Fokus är på att övergripande beskriva tre valda exempel på rutiner för godkännande av IT-system. Studien bedömer att dessa tre exempel visar på olika tillvägagångssätt i termer av formella respektive informella rutiner. Vidare visar dessa tre exempel på hur perspektiv på godkännande kan variera mellan Försvarets Materielverk och Försvarsmakten. För att göra detta möjligt krävs ett övergripande klargörande om vad godkännande av IT-system innebär respektive vilka normsättande regelverk som allmänt styr godkännanden.

1.2 Läsanvisningar

Kapitel 2 redovisar grundläggande behov och drivkrafter som inverkar på genomförande av godkännande, däribland vad som utgör normsättande regelverk och hur dessa sätter upp ramar för hur godkännande av IT-system får ske. Kapitlen 3, 4 och 5 presenterar huvuddragen i tre olika exempel på försvarsmaktsrelaterade rutiner med anknytning till godkännande av IT-system. De tre rutinerna är Försvarets materielverks IT-säkerhetsdeklarationsprocess, Försvarsmaktens IT-process respektive Försvarsmaktens metod för informell granskning av produkter före användning i Försvarsmaktens IT-system. Sammanfattande observationer och diskussion utgör kapitel 6.

2 Att godkänna IT-system

I detta kapitel presenteras vad godkännande av IT-system innebär och i korta drag vilka grundläggande behov och drivkrafter som inverkar på genomförande av godkännande.

2.1 IT-försvarsdagen 2017 – några observationer

Den 8:e november 2017 arrangerade FOI i samråd med Försvarsmakten IT-försvarsdagen 2017. Arrangemanget, som tidigare namngavs som IT-säkerhetsdagen, hade ett fokus på försvarsrelaterad IT-säkerhet och är ett forum för presentation och diskussion av problemställningar, verksamhet och resultat från aktuell forskning och utveckling inom IT-domänen[1].

Presentationer under IT-försvarsdagen (FOI, 2017a) och (FOI, 2017b), gjordes av personal från FOI, Försvarsmakten (FM), Försvarets radioanstalt (FRA), Försvarets materielverk (FMV) och Myndigheten för samhällsskydd och beredskap (MSB). Olika teman och observationer med relevans för utmaningen med att godkänna IT-system togs upp under IT-försvarsdagen:

- *Hotbild för kvalificerade cyberattacker[2]:* Vikten av kunskap om hotbilden mot svenska mål och Försvarsmaktsintressen, vilket inkluderar kunskap om hotaktörer och deras intressen respektive drivkrafter.
- *Hur hacking går till i praktiken[3]:* Sårbarheter kan introduceras under hela livscykeln för system. Komplexitet hos IT-system gynnar antagonisten.
- *Utformning, upphandling och tillhandahållande av försvarslogistik[4]:* Detta sker i nära samarbete med FM för att möta olika operativa behov med hög affärsmässighet i olika beredskapsnivåer. Bland annat rör det sig om behov och krav avseende sekretess, tillgänglighet och riktighet, där en del av dessa har formulerats i *Krav på säkerhetsfunktioner KSF3* (Försvarsmakten, 2014)
- *Återbruk av säkerhetslösningar[5]:* Återbruk förväntas innebära
    - Förenklad utvecklingsprocess.

[1] Enligt utskick med inbjudan till IT-försvarsdagen.
[2] Presentationen *Vad ser FRA av hotbilden för kvalificerade cyberattacker,* Fredrik Wallin (FRA)
[3] Presentationen *Hacking i praktiken,* Hannes Holm (FOI)
[4] Presentationen *Utmaningar med att vara leverantör åt FM,* Erik Norrbohm (FMV)
[5] Presentationen *Verktyg för återbruk av säkerhetslösningar,* Ola Winberg (FMV)

  - Enklare produktplanering
  - Minskade utvecklingstider
  - Minskade integrationstider
  - Minskat antal komponenter
  - Förenklad test och evaluering
  - Succesiva produktförbättringar underlättas
  - Mera sammanhållen system- och produktionsledning.

- *Prognoser och framsteg inom cybersäkerhet*[6]*:* IT är av stor och ökande vikt, men det är andra intressen än försvarsintressen som styr IT-utvecklingen. Prognoser avseende IT visar på större träffsäkerhet än många andra tekniska prognoser. En enkel kartläggning indikerar att mera forskning inom cybersäkerhetsdomänen pågår, men på ungefär samma områden som på 80-talet. Stora omdanande tekniska framsteg inom cybersäkerhet verkar inte ha skett. Indikationer finns på att cybersäkerhet är ett omoget område, ty
  - Systematisk formulering av hypoteser och teoribildning verkar vara bristfällig. Design av nya lösningar för aktuella problem dominerar.
  - Noggranna tester är ovanliga.
  - Många viktiga frågor saknar svar, till exempel avseende vilka intrångsdetektionsmetoder som fungerar och vilka designprinciper som är viktigast.
- *Svårigheten med att beskriva och bedöma hot mot IT-system*[7]*:* Förmågan att bedöma risker är central för verksamhet och förmågor inom FM. Samtidigt är det en komplex uppgift med i dagsläget oklara förutsättningar och bristande stöd.

Dessa teman är inte på något sätt heltäckande för vilka faktorer som berör och inverkar på utmaningen att godkänna system. Oavsett detta indikerar de ändå en bredd i vad som krävs för att på ett tillfredsställande sätt kunna utfärda ett systemgodkännande. Det är värt att notera hur komplexiteten i IT-systemen utgör möjligheter för antagonister, samtidigt som det komplicerar för systemägaren. Utifrån denna notering är det bekymmersamt om det stämmer att cybersäkerhetsområdet är omoget som forskningsområde och vi har svårigheter att beskriva och bedöma hot.

[6] Presentationen *Cybersäkerhetsutblickar,* Teodor Sommestad (FOI)
[7] Presentationen *Att beskriva och bedöma hot mot IT-system,* Jonas Hallberg (FOI)

2.2 Grundbegrepp inom informationssäkerhet och relation till godkännande av IT-system

Grundbegreppen konfidentialitet (eller sekretess), riktighet och tillgänglighet sammanfattar större delen av utmaningarna som finns inom domänen informationssäkerhet. Terminologi för informationssäkerhet (SIS, 2015) definierar grundbegreppen enligt följande:

- *Konfidentialitet:* Skydd mot obehörig insyn. Sekretess används ofta i legala sammanhang och ges där en delvis annan innebörd än konfidentialitet.
- *Riktighet:* Skydd mot oönskad förändring.
- *Tillgänglighet:* Åtkomst för behörig person vid rätt tillfälle.[8]

Informationssäkerhet handlar om att, med utgångspunkt i dessa tre grundbegrepp, skydda mot obehörig insyn och oönskad förändring respektive att säkra åtkomst för behöriga när information behövs. Godkännande av IT-system är en kvittens på huruvida systemegenskaper i tillräcklig grad bidrar till att sekretess, riktighet och tillgänglighet uppnås.

Grundbegreppens innebörd så som definierade enligt (SIS, 2015) ger en bild av klar, tydlig och enkel begreppsbildning utan tvetydigheter. Svårigheter uppstår dock i och med att grundbegreppen inte är enkla att åstadkomma i form av implementerad funktionalitet i faktiska system. Grundbegreppen är på systemnivå metaegenskaper som inte är enkelt mätbara. Detta komplicerar processen att godkänna IT-system.

Ett sätt att försöka hantera problematiken är att formulera mera detaljerade krav som tillsammans bidrar till att uppnå vad grundbegreppen uttrycker på en övergripande nivå. Försvarsmaktens *Krav på säkerhetsfunktioner KSF3* (Försvarsmakten 2014) är ett exempel på detta.

Försvarsmakten har en stark sekretesstradition, vilket bland annat indikeras av den omfattning med vilken termen sekretess omnämns i Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet (H Säk Infosäk)[9] (Försvarsmakten 2013a), (Gudmundson Hunstad, 2016). Sekretesstraditionen indikeras också i

[8] (SIS, 2007) definierade tillgänglighet som att ”*informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid*”, vilket inte begränsar tillgänglighet till att avse personers åtkomst till informationstillgångar, vilket nu aktuell version gör.

[9] Träffar på sökord i (Försvarsmakten, 2013) enligt (Gudmundson Hunstad, 2016):
- Sekretess 894
- Riktighet 12
- Tillgänglighet 29

KSF3 med sitt fokus på att hantera risken att en händelse påverkar sekretessen för den information som systemet hanterar. Samtidigt kan det noteras att det även existerar KSF3-krav direkt relaterade till riktighet och spårbarhet (Bengtsson, Sommestad & Holm, 2014).

2.3 Ackreditering och auktorisation

Enligt säkerhetsskyddsförordningens 12§, tredje stycket, får ett system ”inte tas i drift förrän det har godkänts från säkerhetssynpunkt av den för vars verksamhet systemet inrättas” (SFS, 1996a). Försvarsmakten (2013a) använder begreppet ackreditering för godkännande från säkerhetssynpunkt.

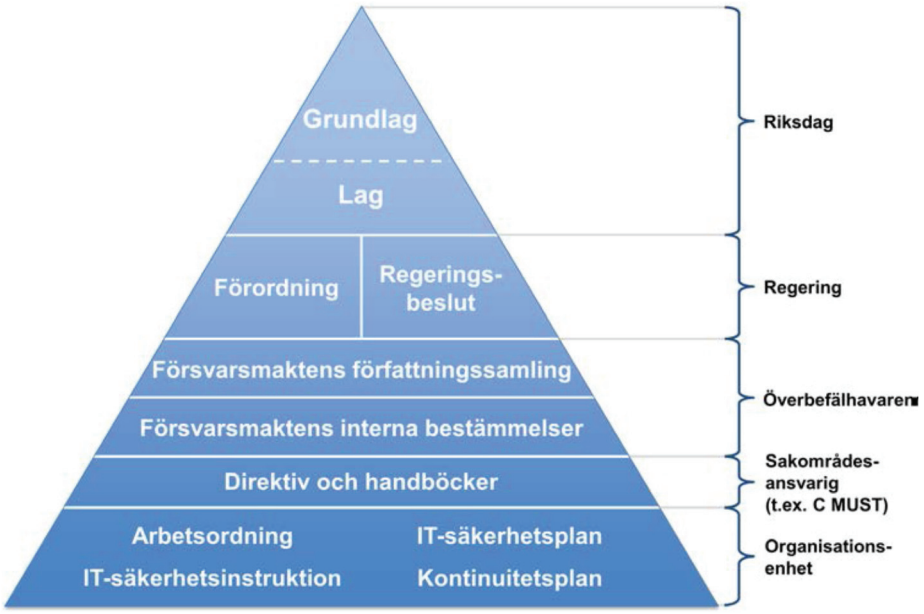
Ackreditering krävs innan driftsättande för IT-system som behandlar utrikesklassificerade eller hemliga uppgifter. IT-system som endast hanterar sekretessklassificerade uppgifter eller uppgifter som ej omfattas av sekretess, kan undantas från ackreditering. Dokumenterade beslut krävs för detta (Försvarsmakten, 2013a).

Inför ackreditering måste först ett auktorisationsbeslut fattas (Försvarsmakten, 2013a). Auktorisation innebär ett bemyndigande för produktägare att utveckla Försvarsmaktens IT-verksamhet (FIB, 2007).

Inför ackreditering krävs säkerhetsgranskning i och kring IT-systemet i fråga, vilket även inkluderar skalskydd och passagekontroll (tillträdesskydd). Avseende system för hemliga och utrikesklassificerade uppgifter krävs yttrande från Militära underrättelse- och säkerhetstjänsten (MUST) innan ackrediteringsbeslut.

2.4 Normsättande regelverk

Normsättande för Försvarsmaktens verksamhet är en hierarki av regelverk från grundlagar på nationell nivå ner till arbetsordning, instruktioner och plandokument på nivån av organisationsenheter inom Försvarsmakten (Figur 1), (Försvarsmakten, 2013a). Ansvar för normsättande varierar inom hierarkin från riksdag och regering ner till respektive FM-organisationsenhet (Figur 1). Hierarkin medför beroenden av normsättande regelverk på högre nivåer, men även en gradvis mera detaljerad specificering på lägre nivåer med ökande närhet till operativ verksamhet.



Figur 1: Normsättande dokument för Försvarsmaktens verksamhet med ansvarsfördelning (Försvarsmakten, 2013a)

Godkännande av IT-system inom FM är beroende av övergripande normsättande regelverk, som till exempel avseende vad säkerhetsskyddslagen (SFS, 1996b) formulerar om rikets säkerhet. Godkännande av IT-system inom FM är också beroende av vad som på nivåer längre ner i hierarkin och mera detaljerat formuleras om rikets säkerhet, exempelvis i FM:s författningar, interna bestämmelser, direktiv och handböcker.

Bengtsson, Sommestad och Holm (2014), Gudmundson Hunstad (2016) och Hakkarainen (2016) diskuterar hur sekretessfrågor har en annan tyngd och fokus i olika normsättande regelverk än vad frågor kring tillgänglighet och integritet har. Tyngden på sekretessfrågor på nivån av laggivning, implicerar behov av att specificera detaljer avseende sekretessfrågor på nivåerna under laggivningen, till exempel i FM:s författningar, interna bestämmelser, direktiv och handböcker. På motsvarande sätt implicerar mindre tyngd på tillgänglighets- och integritetsfrågor på nivån av laggivning ett inte explicit utpekat behov av att specificera detaljer avseende tillgänglighets- och integritetsfrågor på nivåerna under laggivningen, till exempel i FM:s författningar, interna bestämmelser, direktiv och handböcker.

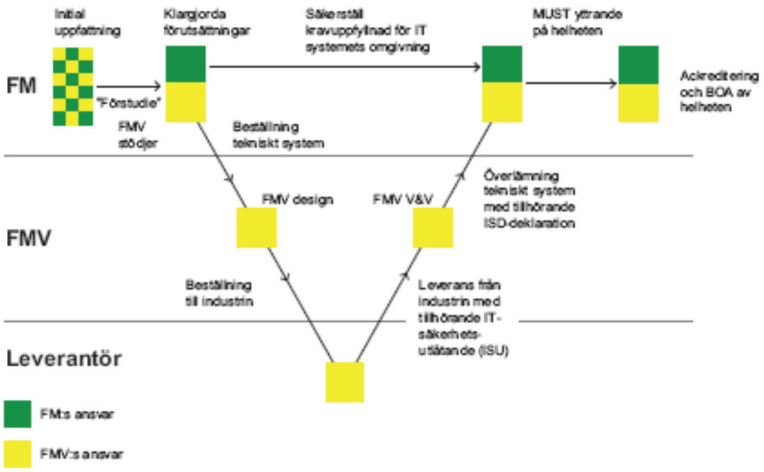
Samtidigt *är* även tillgänglighets- och integritetsfrågor av vikt för att uppnå säkrare IT-system.

3 Process för IT-säkerhetsdeklaration inom Försvarets Materielverk

I detta kapitel presenteras huvuddragen i stödprocessen Informationssäkerhets-deklaration (ISD) som används inom FMV. Beskrivningen av ISD utgår ifrån FMV:s presentationssida om ISD[10] respektive en uppsättning handböcker och andra relevanta dokument om ISD[11].

ISD är enligt FMV (2016a) harmoniserade med FM:s IT-process och KSF. IT-system som är anskaffade och vidmakthållna av FMV som skall ackrediteras av Försvarsmakten skall följa ISD-processen. Vad som övergripande i denna rapport omnämns som att godkänna IT-system kan diskuteras hur det relaterar till ISD-processen. De slutliga stegen i termer av ackreditering, auktorisering och beslut om användande inom FM av bedömd IT-system, genomförs inom FM. Därmed kan argument lyftas för att ISD inte explicit handlar om att godkänna IT-system. Däremot är ISD en stödprocess inför godkännande, vilket poängterar vikten av att här lyfta fram och beskriva ISD.

Tillämpning av ISD-processen innebär en fördelning av ansvar och roller i enlighet med Figur 2.



Figur 2: ISD-processens fördelning av ansvar och roller (FMV, 2016a)

[10] https://www.fmv.se/sv/Verksamhet/ISD---informationsteknik/
[11] Tillgängliga via http://isd.fmv.se/Sidor/default.aspx

ISD skall bidra till god balans mellan ekonomi och säkerhetsrelaterad risk respektive mellan funktion och assurans. För att uppnå detta görs dokumentgranskning, tester och evalueringar. Ett grundläggande syfte är att Försvarsmaktssystem anskaffade via FMV skall kunna opereras med en tolerabel risknivå och etablera spårbarhet från Försvarsmaktens krav till implementering via FMV. ISD skall leda till att rätt typ av granskningar, tester, analyser och evalueringar och med önskad ambition och kvalitet sker och detta för att underlätta FM:s riskbeslut, till exempel avseende beslut om användning av IT-system.

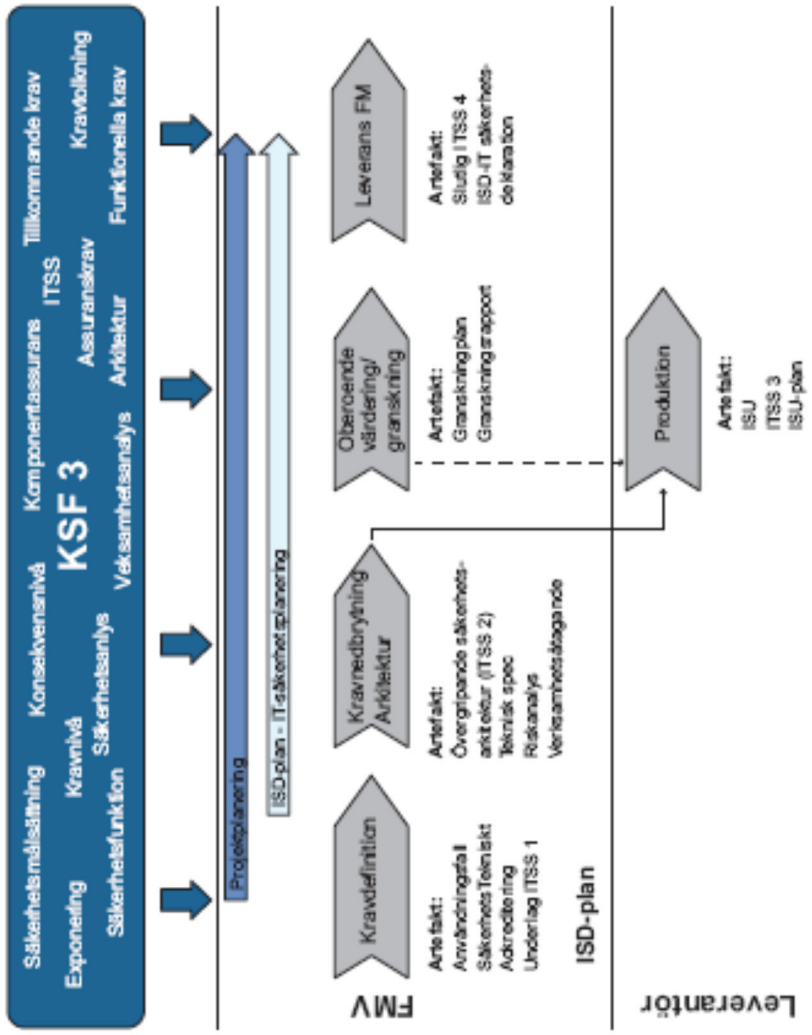
Av vikt är att etablera respektive vidmakthålla förtroende för FMV:s utformning och implementering av funktioner med inverkan på informationssäkerhet. Sådant förtroende skapas med

- strukturerad kravhantering
- bevis för att FM-krav är implementerade
- spårbarhet från krav till implementering
- ökad effektivitet
- ökad kompetensuppbyggnad.

Processen för att nå detta förtroende illustreras i sina huvudsteg i Figur 3. Leverans till FM sker i form av en IT-säkerhetsspecifikation (ITSS) respektive en IT-säkerhetsdeklaration (ISD). För utvecklingsprojekt skall förståelse skapas för det säkerhetsarbete som skall genomföras och vad som i olika faser skall tas fram. ISD skall bidra till att FM får IT-system i rätt tid, till rätt kostnad och med rätt kvalitet avseende IT-säkerhet. Vidare skall ISD säkra att MUST får underlag som underlättar och begränsar MUST:s resursanvändning för att bedöma och godkänna IT-system. Leverantörer till FMV skall få förståelse för ställda IT-säkerhetskrav och förväntat ansvarstagande för IT-säkerheten i levererade system.

Vad som omnämns som vidmakthållande av IT-system hos FMV medför ändringar i IT-systemet. Beroende på eventuell påverkan på kravuppfyllnad i ITSS och ISD, kan ny ackreditering bli nödvändig. Omfattningen av ändringar kan vara av en storlek som resulterar i ett nytt uppdrag med ett helt nytt genomförande av alla steg i ISD-processen.

Som nämndes inledningsvis i detta kapitel, är ISD enligt FMV (2016a) harmoniserade med FM:s IT-process och KSF. Enligt FMV (2016b) är det en *ambition* att integrera ISD med KSF3 och FM:s IT-process. Senare i avsnittet *FM IT-process* i FMV (2016b) beskrivs detta i termer av en *tänkt* koppling.



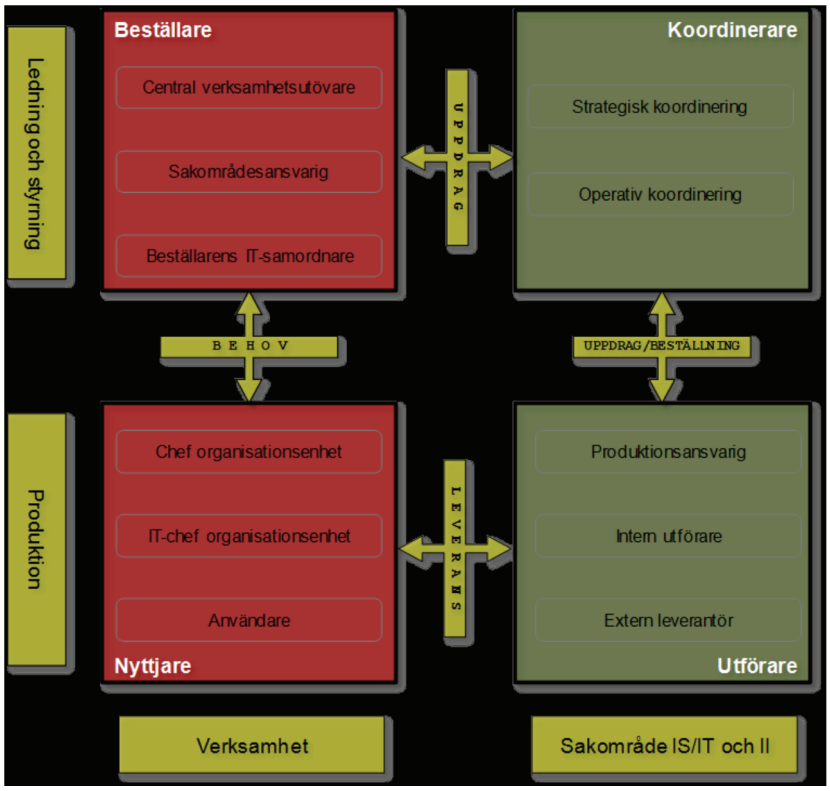
Figur 3: FMV:s stödprocess Informationssäkerhetsdeklaration (ISD) (FMV, 2016a)

FMV (2016c) påpekar i form av en erfarenhetsrapportering att det är otydligt hur ISD-processen interagerar med FM:s IT-process. Svårigheter observeras avseende att beskriva vad som utgör ackrediteringsobjektet och dess gränsytor. Bättre beskrivning av ackrediteringsobjektet omnämns som sätt att underlätta och förenkla. Vidare omnämns ett stort behov av metodstöd avseende hantering av system-av-system inom ISD-processen.

4 Försvarsmaktens IT-process

I detta kapitel presenteras huvuddragen i Försvarsmaktens IT-process. IT-processen skall med utgångspunkt i verksamhetsbehov säkra leverans av effektiva, säkra och mätbara IT-tjänster. Beskrivningar i detta kapitel baserar sig på (Försvarsmakten, 2013b).

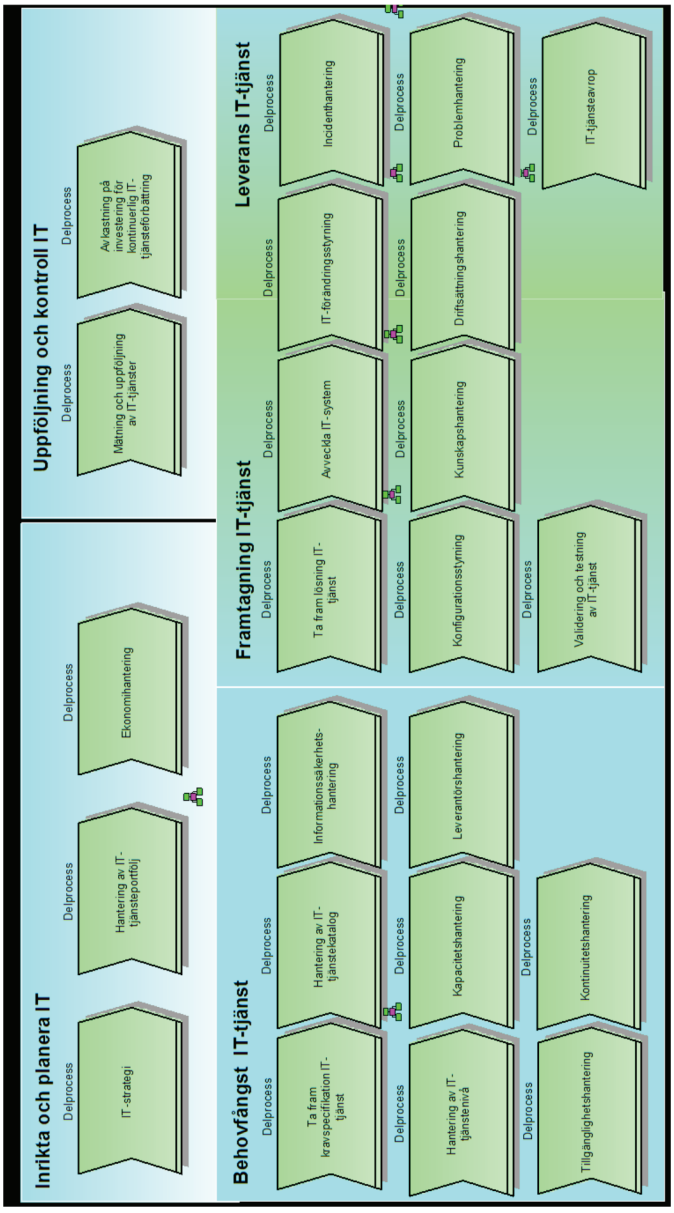
Försvarsmaktens verksamhet definieras av ett fåtal lednings- och huvud-processer. Utöver dessa finns ett antal stödprocesser, varav IT-processen är en. Syftet med IT-processen är att utifrån verksamhetsbehov leverera effektiva, säkra och mätbara IT-tjänster med hög leveransprecision. Processen bygger på ITIL-ramverket.[12] En utgångspunkt är en styrande beställar- och utförarmodell enligt Figur 4.



Figur 4: IT-processens beställar- och utförarmodell (Försvarsmakten, 2013b)

[12] ITIL: Information Technology Infrastructure Library

IT-processens relativt omfattande uppsättning av delprocesser är indelad i huvudområden och delprocesser enligt Figur 5.



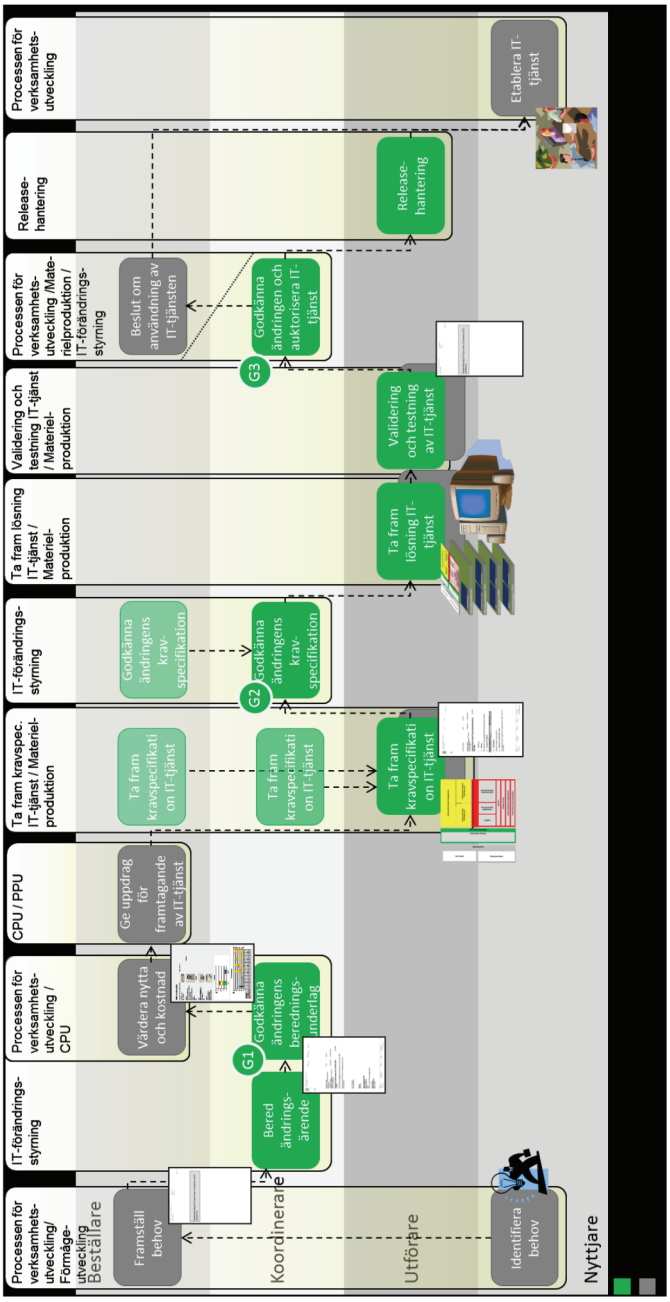
Figur 5: IT-processens huvudområden med ingående delprocesser (Försvarsmakten, 2013b)

Begreppen IT-tjänst respektive IT-objekt används frekvent i IT-processens sammanhang. Med IT-tjänst avses en kombination av IT, människor och processer. Vidare används det relaterade begreppet verksamhetsnära IT-tjänst. Även stödjande IT-tjänster används som begrepp. IT-objekt är ett samlingsbegrepp för olika varianter av IT som kan ingå i IT-tjänster. Det kan till exempel vara tal om hela IT-system, mjukvara, kommunikationslösningar eller hårdvara.

Enligt Försvarsmakten (2013b) skall IT-processen tillämpas på alla IT-tjänster inom FM. IT-objekt kan tas fram av FMV under deras designansvar eller av FM. I det senare fallet när FM tar fram IT-objekt, har koordineringsfunktionen inom FM designansvaret. Koordineringsfunktionen ingår i beställar- och utförarmodellen (Figur 4) och leds av Försvarsmaktens sambands- och informationssystemchef (FM CIO[13]). IT-processen inriktar hur IT-objekt skall utformas respektive hur FM:s hanterande av levererade IT-objekt kan bidra till effektiva IT-tjänster.

FM:s olika lednings-, huvud- och stödprocesser interagerar, vilket exempelvis sker vid framtagande av en ny IT-tjänst i enlighet med Figur 6. Figuren illustrerar på ett förenklat sätt stegen från behovsidentifiering fram till IT-tjänstens införande i verksamheten. Utan att gå in på detaljer kan det noteras att flera steg av vikt för att nå en relevant och adekvat informationssäkerhetsnivå ingår. Detta gäller bland annat behovs- och kravhantering respektive verifiering och validering av IT-tjänster. Vidare omnämner Försvarsmakten (2013b) i text ett komplext steg *Godkänn IT-tjänst* som inte fullständigt framgår ur Figur 6. Markeringen G3 i Figur 6 indikerar den punkt där auktorisering av den nya IT-tjänsten sker efter att godtagbara testresultat har uppnåtts, vilket utgör en del av ovan nämnda komplexa steg. För auktorisering av IT-tjänsten krävs ackreditering (godkännande ur IT-säkerhetsperspektiv) och beslut om godkännande ur systemsäkerhetsperspektiv. I och med auktorisation har kontroll av IT-tjänstens alla delar möjliggjort att leverans och driftsättning kan ske. FM CIO eller chefen för Materielsystemkontor ledningssystem (C MSK Ledsyst) beslutar beroende på tidigare klassificering inom delprocessen IT-förändringsstyrning om ackreditering, systemsäkerhet respektive auktorisering. Vid beslut om användning accepterar beställaren kvarvarande risker för IT-tjänsten. Dessa risker är enligt Försvarsmakten (2013b) preciserade i auktorisationen.

[13] CIO: Chief Information Officer

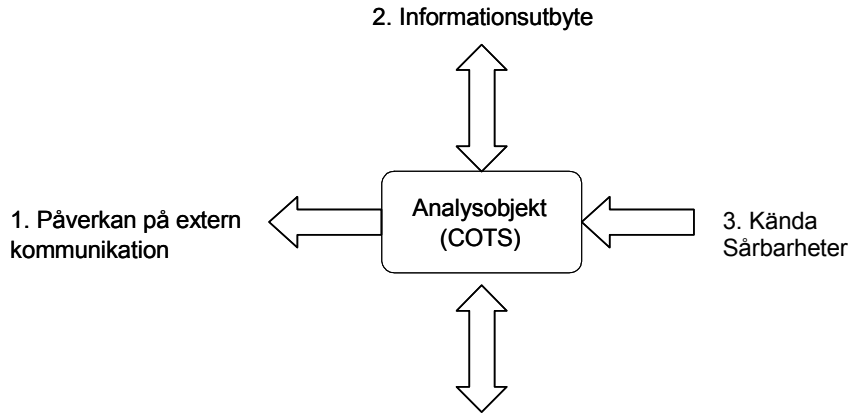


Figur 6: Framtagande av ny IT-tjänst som interaktion mellan delar av IT-processen och andra Försvarsmaktsprocesser (Försvarsmakten, 2013b)

5 Informell granskning av produkter

I detta kapitel presenteras huvuddragen i Försvarsmaktens metod för informell sårbarhetsgranskning av produkter före användning i Försvarsmaktens IT-system (Försvarsmakten, 2007).

Metoden används, enligt (Försvarsmakten, 2007) för att granska programvaror som ännu inte har godkänts genom auktorisation eller som har godkänts, men där en informell granskning före användning krävs. Den informella granskningsmetoden fokuserar på *sårbarhetsgranskning* och avses användas på kommersiellt tillgängliga programvaror eller motsvarande som är tänkta att användas i Försvarsmaktens IT-system. Däremot är inte metoden avsedd att användas för produkter som avses användas i säkerhetshöjande syfte eller som berörs av fördefinierade krav på säkerhetsfunktioner enligt KSF eller för säkerhetsmekanismer. Försvarsmakten (2007) påpekar vidare att metoden inte är lämplig för granskning av programvara med vad som omnämns som komplex funktionalitet. Vad som bedöms utgöra komplex funktionalitet redovisas dock inte närmare.



Figur 7: Informell teknisk granskning, särskilt informationssäkerhetspåverkande egenskaper (Försvarsmakten, 2007)

Såväl teoretisk som teknisk granskning ingår i metoden. Den teoretiska granskningen fokuserar på informationsinsamling via allmänt tillgängliga informationskällor (Internet, leverantör etc) om den granskade programvaran och dess leverantör. Detta resulterar i en sammanställning och en analys av kända sårbarheter och utnyttjande av dessa. Den tekniska granskningen fokuserar på

programvarans beteende vid exekvering och handhavande i samband med exempelvis installation, uppdatering och programvarans interaktion med omgivande system. Bland annat eftersträvas att detektera tänkbar oönskad eller dold kommunikation eller informationsutbyte. Därför granskas utifrån kännedom om sårbarheter påverkan på extern kommunikation, påverkan på det omgivande värdsystemet och informationsutbyte med systemets omgivning enligt Figur 7.

Vid användande av den informella granskningsmetoden skall alltid den teoretiska granskningen genomföras. Teknisk granskning genomförs i fall där granskad programvaras beteende i en systemomgivning är av vikt att kunna bedöma.

För att underlätta för olika verksamheters användande av granskad programvara är det av vikt att granskningen genomförs utifrån generella villkor. Därav följer att specifika egenskaper som verksamhet, miljö och användningsområde där programvaran skall användas inte skall ingå i granskningsrapporten. I en auktorisationsansökan är det däremot lämpligt att ta upp detta. Samtidigt kan det noteras att vid den tekniska granskningen skall *laborationsmiljön* vid granskningen specificeras noggrant.

5.1 Moment vid teoretisk granskning

I den teoretiska granskningen ingår minst följande moment (Försvarsmakten, 2007):

- översikt över granskningsobjektet
- beskrivning av leverantör av granskningsobjektet
- granskning av dokumentation
- identifiering av ingående komponenter
- beskrivning av informationsutbyte
- beskrivning av tillvägagångssätt vid uppdateringar
- konfigurationsanalys
- identifiering av eventuella tidigare genomförda sårbarhetsgranskningar eller andra evalueringar och säkerhetstester
- sårbarhetssökning i allmänna källor
- rekommendation efter genomförd teoretisk granskning.

Metodbeskrivningen ger ett antal konkreta krav, rekommendationer och tips avseende den teoretiska granskningen. Till exempel rekommenderas för upprättande av en översikt över den granskade programvaran att utöver produkt- och leverantörshemsidor även källkritiskt söka information på diskussions- och

säkerhetsforum. I allmänhet påpekas vikten av noggranna källhänvisningar. Vidare påpekas olika metodkrav, såsom avseende beskrivning av informationsutbyte att förekomst i granskad programvara av mobil kod skall undersökas.

Avseende rekommendation efter genomförd teoretisk granskning diskuterar metodbeskrivningen vad som kan ingå, som exempelvis åtgärder för att motverka identifierade sårbarheter, förslag till restriktioner vid användande av granskad programvara respektive krav på implementeringsmiljö.

5.2 Moment vid teknisk granskning

I den tekniska granskningen ingår minst följande granskningsmoment (Försvarsmakten, 2007):

- beskrivning av laborationsmiljö och granskningsobjekt
- systempåverkan vid installation
- systempåverkan vid exekvering
- systempåverkan vid uppdatering
- test av förekomst av skadlig eller oönskad kod
- systempåverkan vid avinstallation
- rekommendation.

Metodbeskrivningen ger ett antal konkreta krav, rekommendationer och tips avseende den tekniska granskningen. För att säkra möjligheten att upprepa tester under likartade villkor påpekar Försvarsmakten (2007) vikten av att noggrant specificera granskningsobjekt och miljön i vilken det testas. Olika typer av systempåverkan och testförfarande skall också dokumenteras noggrant.

Avseende rekommendation efter genomförd teknisk granskning diskuterar metodbeskrivningen vad som kan ingå. Exempelvis berörs åtgärder för att motverka identifierade sårbarheter, förslag till restriktioner vid användande av granskad programvara respektive krav på implementeringsmiljö. Här kan det noteras att detta motsvarar vad som anges även för den teoretiska granskningen, men att rekommendationen från den tekniska granskningen tar sin utgångspunkt i inhämtade erfarenheter från granskningen av granskningsobjektet i en systemomgivning.

6 Diskussion och slutsatser

Försvarsmaktens verksamhet är av en art som nödvändiggör tydliga rutiner och regelverk avseende godkännande av IT-system. Driftsättande av system som brister ur IT-säkerhetssynpunkt kan innebära betydande risker för Försvarsmaktens verksamhet och i förlängningen för rikets säkerhet.

De normsättande regelverken – som bland annat lagar, förordningar, föreskrifter och Försvarsmaktens interna bestämmelser – accentuerar vikten av noggrannhet vid godkännande av IT-system och sätter upp ramar för hur godkännande skall gå till. Ju närmare Försvarsmaktens verksamhet de normsättande regelverken har formulerats, desto mer detaljerade är de.

Observationer från IT-försvarsdagen avseende en påstådd brist i mognad på cybersäkerhetsområdets forskning tillsammans med svårigheter att beskriva och bedöma hot, indikerar tänkbara betydande utmaningar avseende upprättande av adekvata, relevanta och tillförlitliga rutiner för godkännande av IT-system. Vad som någorlunda smidigt kan anges som ramar och krav i normsättande regelverk innebär större utmaningar när rutiner för godkännande formuleras. Det kan antas vara där brister i forskningsmognad och svårigheter att beskriva och bedöma hot riskerar att ge oönskade avtryck.

ISD-processen, Försvarsmaktens IT-process och metoden för informell granskning av produkter kräver alla tre tydlig dokumentation. Särskilt i fallen med de två förstnämnda av dessa tre rutiner torde dokumentationen i allmänhet bli omfattande. I dokumentationen för dessa två ingår ett antal noggrant definierade steg och delprocesser. Trots detta kan det observeras kvarstående problem, som exempelvis otydlighet i hur ISD-processen kan interagera med Försvarsmaktens IT-process och behov av ytterligare metodstöd.

Den informella granskningsmetoden, som beskrivs i kapitel 5, är lättare att få en bild av vad den kan prestera med sitt mera avgränsade fokus på sårbarhetsgranskning. Samtidigt har den metoden också sina kvarstående utmaningar genom att den inte kan användas för granskning av produkter med vad som omnämns som komplex funktionalitet. I sammanhanget skulle det underlätta med ett klargörande av vad komplex funktionalitet innebär.

Sammanfattningsvis är godkännandet av IT-system ur IT-säkerhetsperspektiv ingen uppenbar och enkel företeelse. Med en del arbete är det möjligt att definiera och beskriva i termer av regelverk och rutiner hur godkännanden av IT-system bör gå till. Det är däremot inte lika enkelt att veta i vilken mån beslutet om godkännande ger önskvärda effekter i verksamheten och om kvarvarande risker i slutändan är hanterbara. Denna problematik kan delvis orsakas av det fokus som finns i normsättande regelverk på avvägningar kring sekretess, samtidigt som avvägningar kring tillgänglighet och integritet också behövs. Däremot verkar det finnas betydande utmaningar att i normsättande regelverk

formulera hur dessa senare avvägningar bör genomföras. Icke minst är det en betydande utmaning att balansera de olika avvägningarna kring respektive grundbegrepp mot varandra.

Referenser

Bengtsson, J., Sommestad, T., & Holm, H. (2014). *IT-säkerhetskrav i Försvarsmakten - KSF3 och tillkommande säkerhetskrav.* FOI-R--4000--SE Totalförsvarets forskningsinstitut (FOI).

FIB. (2007) *Försvarsmaktens interna bestämmelser om IT-verksamhet.* FIB 2007:5

FMV. (2016a) *FMV Vägledning för ISD och SE - ISD och SE.* Hämtat från http://isd.fmv.se/Mallar/ISD%20och%20SE.pdf

FMV. (2016b) *Metodstöd för ISD-processen – Övergripande beskrivning: Kundnyttan med ISD-processens metodstöd.* Hämtat från http://isd.fmv.se/Mallar/Kundnyttan%20med%20ISD%20processens%20metodst%C3%B6d.pdf

FMV. (2016c) *Erfarenheter från arbete med oberoende granskning och ISD metodstöd.* Hämtat från http://isd.fmv.se/Sidor/%C3%96vriga-dokument.aspx

FOI. (2017a) *IT-försvarsdagen 2017.* FOI Memo 6219

FOI. (2017b) *Presentationsmaterial från IT-försvarsdagen.* Hämtat från ftp://download.iwlab.foi.se/itsakdagen/ITFD2017.pdf

Försvarsmakten. (2007). *Sårbarhetsgranskning - Informell granskning av produkter före användning i Försvarsmaktens IT-system.* HKV 10 750:72100

Försvarsmakten. (2013a). *Handbok Säkerhetstjänst Informationssäkerhet H Säk Infosäk, M7739-352056) (Ändring 1).* Försvarsmakten.

Försvarsmakten. (2013b). *Fastställande handbok IT-processen*. HKV 09 100:60203

Försvarsmakten. (2014). *KSF: Krav på IT-säkerhetsförmågor hos IT-system, v3.1.* Försvarsmakten.

Gudmundson Hunstad, A. (2016). *Informationssäkerhetsegenskaper - Avvägningar och prioriteringar.* FOI-R--4341--SE.Totalförsvarets forskningsinstitut (FOI).

Hakkarainen, K. (2016). Kim Hakkarainen, Blogg om informationssäkerhet. Hämtat från http://blogg.mrpoyz.net/gemensamma-skyddsnivaer/

Hansson, J., Granlund, H., & Hallberg, N. (2011). *Att uttrycka krav i materielmålsättningar – Formulera och granska.* FOI-R--3250--SE. Totalförsvarets forskningsinstitut, FOI.

SFS. (1996a). *Säkerhetsskyddsförordningen.* SFS nr: 1996:633

SFS. (1996b). *Säkerhetsskyddslagen.* SFS nr: 1996:627

SIS. (2007). *SIS HB 550: Terminologi för informationssäkerhet, utgåva 3.*

SIS. (2015). *Terminologi för informationssäkerhet.* Teknisk rapport.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se