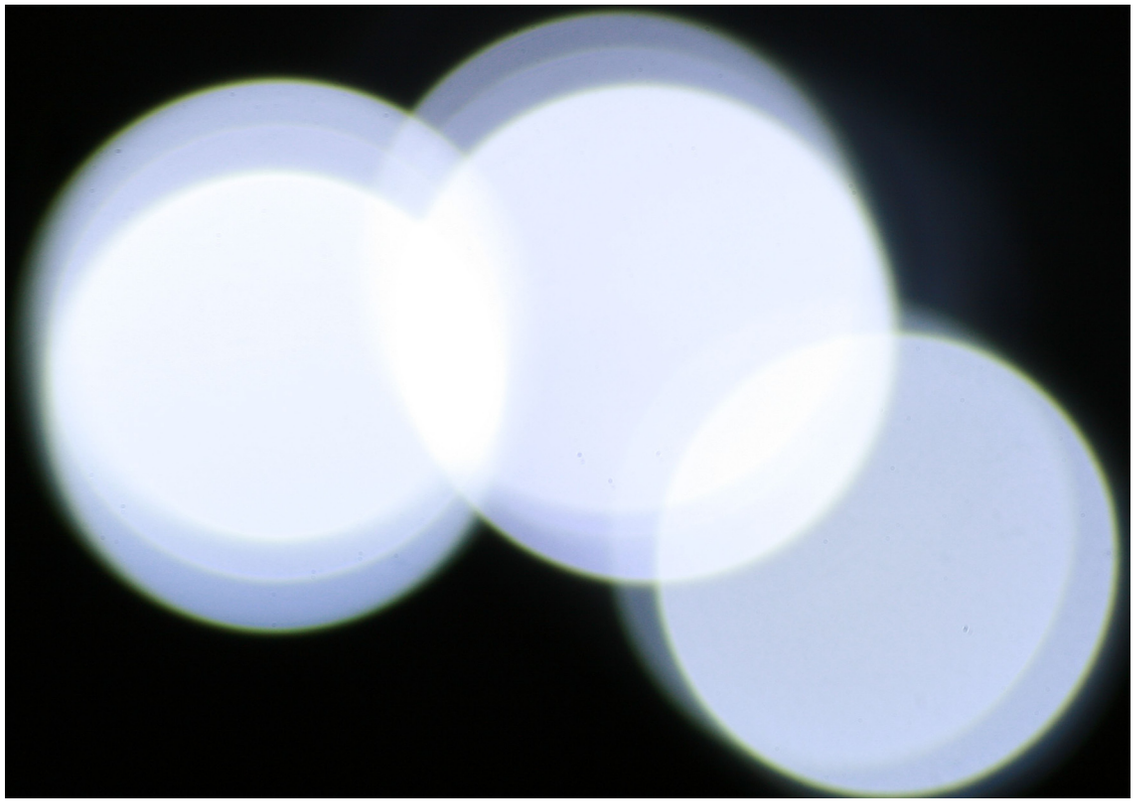
Test av relevans och validitet avseende säkerhetsvärdering

En studie av Försvarsmaktens metoder för säkerhetskravställning och sårbarhetsanalys

JOHAN BENGTSSON OCH JONAS HALLBERG



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
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R--2625--SE
ISSN 1650-1942

Vetenskaplig rapport
December 2008

Informationssystem

Johan Bengtsson och Jonas Hallberg

Test av relevans och validitet avseende säkerhetsvärdering

En studie av Försvarsmaktens metoder för säkerhetskravställning och sårbarhetsanalys

Titel	Test av relevans och validitet avseende säkerhetsvärdering – En studie av Försvarsmaktens metoder för säkerhetskravställning och sårbarhetsanalys
Title	Testing relevance and validity of security assessment methods – A study of the methods for security requirements engineering and vulnerability analysis used by the Swedish Armed Forces
Rapportnr/Report no	FOI-R--2625--SE
Rapporttyp Report Type	Vetenskaplig rapport Scientific report
Månad/Month	12
Utgivningsår/Year	2008
Antal sidor/Pages	56 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten / Swedish Armed Forces
Forskningsområde Programme area	7. Ledning med MSI 7. C4I
Delområde Subcategory	71 Ledning 71 Command, Control, Communications, Computers, Intelligence
Projektnr/Project no	E7046
Godkänd av/Approved by	Martin Rantzer

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

Att uppnå och behålla ändamålsenliga nivåer av informationssäkerhet i Försvarsmaktens IT-system är kritiskt. De tillhörande auktorisations- och ackrediteringsprocesserna måste därför vara effektiva. Inom auktorisations- och ackrediteringsprocesserna tas flera beslut baserat på hur olika alternativ förväntas påverka systemens säkerhetsnivåer. Ändamålsenliga underlag för dessa beslut kräver förmåga att värdera de resulterande säkerhetseffekterna. Effektiv värdering av informationssäkerhet kräver att använda metoder såväl motsvarar användarnas behov som avspeglar verkligheten.

Syftet med denna rapport är att utröna relevans och validitet hos metoder för värdering av informationssäkerhet. Studerade metoder återfinns i processer för framtagande av underlag för auktorisationsbeslut B2. Det arbete som beskrivs i denna rapport har resulterat i följande huvudsakliga bidrag.

- En övergripande beskrivning av framtagandet av underlag för auktorisationsbeslut B2.
- Beskrivning av delprocesserna för framtagande av säkerhetskrav samt sårbarhetsanalys.
- Analyser av relevans och validitet hos de metoder för säkerhetsvärdering som ingår i processerna för framtagande av säkerhetskrav och sårbarhetsanalys.

Nyckelord: Säkerhetsvärdering, auktorisation, ackreditering

Summary

To reach and maintain adequate levels of security in the information systems of the Swedish Armed Forces is crucial. Therefore, the associated authorization and accreditation processes must be efficient and effective. Within the authorization and accreditation processes several decisions are based on the anticipated result on the security levels of the systems. Adequate bases for these decisions require the ability to assess the resulting security levels. Efficient and effective assessment of information security requires methods which fulfills the needs of the users and, at the same time, reflects the reality.

The purpose of this report is to decide the relevance and validity of methods for information security assessment. The studied methods are found in the processes for compilation of data for authorization decision B2. The main contributions of this report are the following.

- An overview of the process for compilation of data for authorization decision B2.
- Descriptions of the sub-processes for security requirements engineering and vulnerability analysis.
- Analysis of the relevance and validity of the methods for security assessment included in the sub-processes for security requirements engineering and vulnerability analysis.

Keywords: Security assessment, authorization, security accreditation

Innehåll

1 Inledning

För att uppnå och behålla ändamålsenliga nivåer av informationssäkerhet i Försvarsmaktens är det väsentligt att ackrediteringsprocessen för IT-system är effektiv. I Direktiv för Försvarsmaktens Informationsteknikverksamhet (DIT 04) (Försvarsmakten, 2004a, s. 67) står ”Syftet med Ackrediteringsprocessen är att säkerställa att Försvarsmaktens IT-system hanterar uppgifter på ett från säkerhetssynpunkt godkänt sätt. […] Ackrediteringsprocessen skall även möjliggöra att ackrediteringsarbetet kan bedrivas rationellt och kostnads-effektivt”. Detta betonar två väsentliga egenskaper hos ackrediteringsprocessen: att den leder till IT-system med rätt säkerhetsnivåer samt att resursbehoven för genomförandet av ackrediteringar minimeras.

Ackrediteringsprocessen innehåller flera delprocesser där beslut tas baserat på vilka konsekvenser olika alternativ får för de framtida systemens säkerhetsnivåer. Ändamålsenliga underlag för dessa beslut kräver förmåga att värdera de effekter, på de framtida systemens säkerhetsnivåer, som de olika beslutsalternativen resulterar i. Effektiv värdering av informationssäkerhet kräver att använda metoder är såväl relevanta, dvs. motsvarar användarnas behov, som valida, dvs. avspeglar verkligheten ändamålsenligt.

1.1 Syfte

Syftet med denna rapport är att utröna relevans och validitet hos metoder för värdering av informationssäkerhet. Studerade processer, vilka innehåller inslag av informationssäkerhetsvärdering, ingår i framtagandet av underlag för auktorisationsbeslut B2, vilket avgör om nästa steg i livscykel (definiera) ska genomföras (Försvarsmakten, 2004a, s. 36). I vidare betydelse är syftet också att skapa förståelse för hur frågor som relaterar till värdering av informationssäkerhet hanteras inom Försvarsmakten.

1.2 Metod

För att beskriva relevans och validitet hos aktuella säkerhetsvärderingsmetoder har följande metod nyttjats.

1. En översiktlig beskrivning av processen för framtagande av underlag för auktorisationsbeslut B2 tas fram baserat på tillgänglig litteratur.
2. Utgående från den framtagna processbeskrivningen väljs två delprocesser vilka innehåller informationssäkerhetsvärdering ut.

3. För att samla in data avseende de utvalda delprocesserna nyttjas en samling av frågställningar.
4. De utvalda delprocesserna beskrivs utifrån erhållna svar på frågeställningarna och tillgänglig litteratur.
5. Testmetoden appliceras på de erhållna delprocessbeskrivningarna för att ge en indikation på de identifierade metodernas relevans och validitet.

1.3 Bidrag

Det arbete som beskrivs i denna rapport har resulterat i följande huvudsakliga bidrag.

- En övergripande beskrivning av framtagandet av underlag för auktorisationsbeslut B2.
- Beskrivning av delprocesserna för framtagande av säkerhetskrav samt sårbarhetsanalys.
- Analyser av relevans och validitet hos de metoder för säkerhetsvärdering som ingår i processerna för framtagande av säkerhetskrav och sårbarhetsanalys.

2 Bakgrund

Avsnitt 2.1 redogör för begrepp avseende värdering av informations- och IT-säkerhet. Avsnitt 2.2 diskuterar auktorisations- och ackrediteringsprocessen. Avsnitt 2.3 återger de, inom forskningsprojektet, tidigare identifierade värderingsaspekterna inom Försvarsmaktens IT-säkerhetsarbete. Slutligen beskrivs den framtagna proceduren för testning av värderingsmetoder i avsnitt 2.4.

2.1 Begrepp avseende värdering av säkerhet

I detta avsnitt redovisas en mängd termer som används inom området värdering av informations- och IT-säkerhet. För att underlätta uppslagning återges termerna i alfabetisk ordning. Eventuella kortformer redovisas inom parenteser.

I denna rapport används delvis det mer generella begreppet säkerhet istället för IT-säkerhet. Det ska dock, om inte annat anges, inte tolkas i vidare mening än IT-säkerhet.

Ackreditering utgör ”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” (Försvarsmakten, 2006b).

Auktorisation innebär ”bemyndigande för produktägare att utveckla Försvarsmaktens IT-verksamhet” (Försvarsmakten, 2006b).

Behov beskriver aktiviteter eller resurser som är nödvändiga för att kunna genomföra uppgifter och uppnå mål. Behov kan vara antingen medvetna eller omedvetna, verkliga eller upplevda samt tillfredsställda eller otillfredsställda. Påtalade behov är ofta relaterade till någon form av inneboende krav på åtgärd.

Behov av IT-säkerhetsvärdering (värderingsbehov) beskriver vilka brister på kunskap som behöver åtgärdas. Dessa utgör motiv för att genomföra IT-säkerhetsvärdering.

Beräkningsmodeller beskriver hur beräkningar av IT-säkerhetsvärden går till, det vill säga hur uppmätta IT-säkerhetsvärden sammanställs till det slutresultat som en IT-säkerhetsvärdering genererar.

Hot utgörs av möjliga oönskade händelser med för en verksamhet negativa konsekvenser (SIS, 2007).

Informationssystem avser system som samlar in, bearbetar, lagrar och distribuerar information. Innebörden är allmän, men oftast avses datorstödda informationssystem (Nationalencyklopedin, 2008a). För att undvika otydligheter avseende vad informationssystem faktiskt inkluderar kan termen IT-system nyttjas.

Informationssäkerhet relaterar till informationstillgångar samt förmåga att upprätthålla säkerhetsrelaterade egenskaper såsom sekretess, korrekthet och tillgänglighet (SIS, 2007). Detta medför att informationssäkerhet är ett väldigt vittomfattande område som inkluderar såväl administrativ som teknisk säkerhet.

IT-system avser system med teknik som hanterar och utbyter information med omgivningen (Försvarsmakten, 2006b). Detta innebär en tydlig koppling till tekniska system.

IT-säkerhet avser säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation (SIS, 2007). Säkerheten i IT-system beror dock inte endast på systemets tekniska lösningar. Därmed behöver beaktande av IT-säkerhet inkludera även andra aktiviteter och rutiner som påverkar den tekniska utrustningen, såsom hanteringen av lösenord, även om dessa aktiviteter och rutiner i sig inte ingår i IT-systemet. Detta medför att resonemangen kan begränsas till IT-säkerhet snarare än att omfattade det vidare området informationssäkerhet, vilket inkluderar aspekter som inte relaterar till IT-system.

IT-säkerhetsegenskaper (säkerhetsegenskaper) är de egenskaper som används för att beskriva IT-säkerheten hos system. Termen *relevanta IT-säkerhetsegenskaper* används för de egenskaper som används för att beskriva IT-säkerheten i system. Om, exempelvis, sekretess, korrekthet och tillgänglighet är de egenskaper som ska används för att beskriva ett IT-systems säkerhet, utgör dessa tre de relevanta IT-säkerhetsegenskaperna för den aktuella värderingen.

IT-säkerhetsvärdering (säkerhetsvärdering, värdering) syftar till att öka kunskapen om kvaliteter avseende IT-säkerhet hos system, detta genom att fastställa nivåer för relevanta IT-säkerhetsegenskaper.

IT-säkerhetsvärden (säkerhetsvärden, värden) är uppmätta eller beräknade värden som motsvarar de IT-säkerhetsegenskaper som används för att beskriva IT-säkerheten hos system.

Krav beskriver vad ett system ska uppfylla i form av funktioner, attribut eller principer (Kulak & Guiney, 2000).

Metod är ett ”planmässigt tillvägagångssätt (för att uppnå visst resultat)” (Nationalencyklopedin, 2008b).

Risk utgörs av ”kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad” (SIS, 2007).

System består av samverkande enheter, som verkar tillsammans med ett syfte.

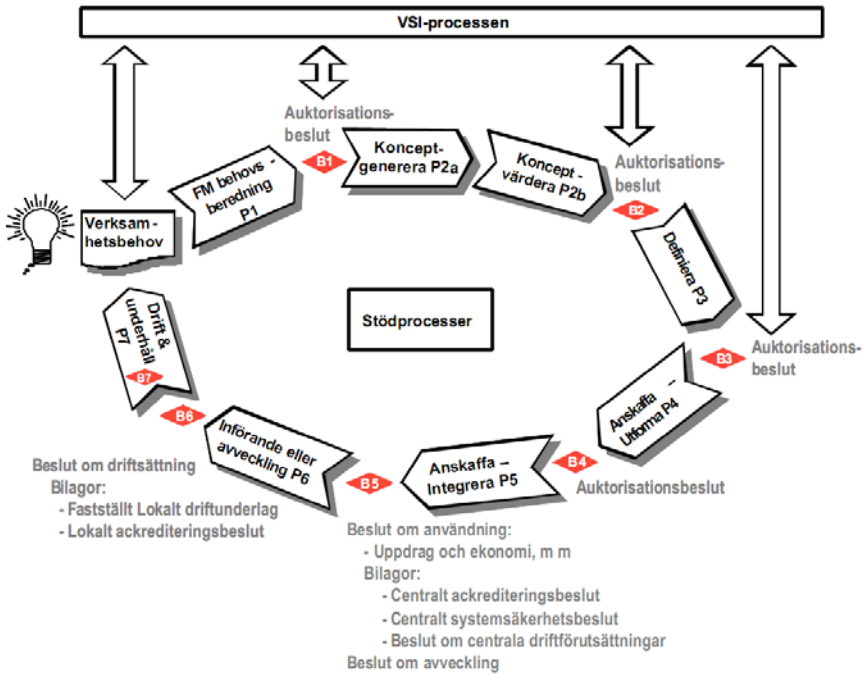
Systemegenskaper karaktäriserar system. IT-säkerhetsrelevanta systemegenskaper kan användas för att beskriva IT-säkerhet hos system.

Verktyg används för att åstadkomma något och utgör därmed realiseringar av metoder. Ibland kan de bakomliggande metoderna vara implicita (enkla). Då metoder sägs användas för att producera resultat, är dessa egentligen realiserade i form av verktyg. Dessa verktyg används för att producera resultaten.

Värderingsaspekter lyfter fram delar av sammanhang, det vill säga aspekter, som indikerar behov av att värdera egenskaper, såsom informations- och IT-säkerhet, hos system. Värderingsaspekter kan baseras på aktiviteter, beslut eller resultat. De aktiviteter som utgör basen för en värderingsaspekt använder värderingsresultat för att producera sina resultat, därav behovet av värdering. Beslut som är grunden för värderingsaspekter har behov av underlag i form av nivåer hos specifika egenskaper hos system, eller delar av system. Resultat, ur vilka värderingsaspekter kan härledas, innehåller element av värderingar av egenskaper.

2.2 Ackrediterings- och auktorisationsprocesser

Ackrediterings- och auktorisationsprocesserna utgör två parallella spår under systems livscykel. I Försvarsmaktens IT-livscykelmodell (Försvarsmakten, 2004a, kap. 6) återfinns auktorisationsprocessen (Försvarsmakten, 2004a, avsnitt B.2) under de tidigare stegen (B1-B4). Ackrediteringsprocessen (Försvarsmakten, 2004a, avsnitt B.3) löper genom hela livscykeln, men med tyngdpunkt vid beslutspunkterna B5-B6. IT-livscykelmodellen återges i Figur 1.



Figur 1: Försvarsmaktens IT-livscykelmodell (Försvarsmakten, 2004a, kap. 6).

Även om ackrediteringsbesluten utgörs av beslutspunkterna B5 och B6 så utgör framtagandet av säkerhetsmålsättningen en viktig del av ackrediteringsprocessen. Säkerhetsmålsättningen tas fram som underlag för beslut B2, vilket är den del av auktorisations- och ackrediteringsprocesserna som studeras i denna rapport.

2.3 Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete

Med syfte att skapa förståelse för hur IT-säkerhet i dagsläget värderas inom Försvarsmakten, har Totalförsvarets forskningsinstitut (FOI) presenterat en kartläggning av värderingsaspekter inom Försvarsmakten (Bengtsson & J. Hallberg, 2008). Detta bland annat för att FOI ska kunna inrikta sitt arbete med utveckling av metoder för värdering av IT-säkerhet så att största möjliga stöd kan ges till Försvarsmaktens IT-säkerhetsarbete.

Resultatet av kartläggningen inkluderar 49 värderingsaspekter med 148 tillhörande frågeställningar. De 49 värderingsaspekter delades in i kategorierna utveckling, ackreditering och drift. Tabell 1 innehåller kategorierna och de

tillhörande värderingsaspekterna samt anger antalet frågeställningar som formulerats för respektive värderingsaspekt och källa, DIT (Försvarsmakten, 2004a), H SÄK IT (Försvarsmakten, 2006b) och FIB 2006:2 (Försvarsmakten, 2006a), inom parentes anges aktuellt avsnitt i aktuellt dokumentet. Arbetet som presenteras i denna rapport utgår från de centrala värderingsaspekterna inom området ackreditering.

Tabell 1: Identifierade värderingsaspekter.

Kategori	**Värderingsaspekt**	**Antal frågest.**	**Källa**
Utveckling	Beslut om IT-säkerhetsgodkännande	5	DIT (1)
	Beslut om vilka bidrag till förebyggande åtgärder inom IT-försvarsområdet som skall tas fram	6	DIT (4.1.10)
	Råd och stöd till utvecklingsprojekt	4	DIT (5.5.1)
	Godkännande av säkerhetslösningar	4	DIT (5.5.1)
	Kriterier för tillämpning av evalueringsnivåer	4	DIT (5.5.2)
	Avgöra produkters säkerhetspåverkan	4	DIT (5.5.2)
Ackreditering	Metoder för säkerhetsgranskning med olika ambitionsnivåer	5	DIT (5.5.2, 6.1.2)
	Konceptvärdering	5	DIT (6.1.1)
	Avgöra vad som utgör ett balanserat skydd	2	DIT (B.3)
	Avgöra vilka lokala åtgärder som krävs	1	H SÄK IT (23.4)
	Ackrediteringsbeslut	1	H SÄK IT (23.3)
	Bedömning av framtagna säkerhetslösningar	2	H SÄK IT (8.1)
	Säkerställa tillräckligt skydd	1	H SÄK IT (23.2)
	Avgöra vilken mängd säkerhetsmekanismer som är relevant och tillräcklig	1	H SÄK IT (23.2)
	Säkerhetskrav och -funktioner	5	H SÄK IT (23.4)
	Beslut om omackreditering	4	FIB2006:2 (11 kap 6§)
	Stöd vid ackreditering	3	DIT (5.5.1)
	Oberoende granskning	4	DIT (B.3)

Kate-gori	Värderingsaspekt	Antal frågest.	Källa
	Bedömning av komplexiteten hos kommande hot-, risk- och sårbarhetsanalyser	1	H SÄK IT (8.1)
	Bedömningar av sannolikheter för att hot skall inträffa	3	H SÄK IT (8.6)
	Metoder och verktyg för genomförande av riskanalys	2	H SÄK IT (8.6)
	Genomförande av sårbarhetsanalys	5	H SÄK IT (8.1, 8.6)
	Kopplingen mellan konsekvensanalyser respektive hot-, risk- och sårbarhetsanalyser	1	H SÄK IT (8.6)
	Beslut avseende hantering av sårbarheter	3	H SÄK IT (8.6)
	Fastslå kravställning av säkerhetsfunktioner	4	H SÄK IT (16.2, 16.5.3, 23.4)
	Fastslå realisering av säkerhetsfunktioner	4	H SÄK IT (8.7, 16.5.3)
	Metod och utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten (MAACK)	4	H SÄK IT (8.6, 23.1)
	Testgodkännande	8	H SÄK IT (11.1)
	Åtgärdsbeslut	3	H SÄK IT (8.6)
Drift	Tillse att skydd är erforderligt	4	DIT (5.5.1)
	Avgöra om regelverket efterlevs	2	DIT (5.5.1)
	Avgöra tillräcklighet hos säkerheten i och kring IT-system	3	H SÄK IT (7.4)
	Avgöra ifall system har otillräcklig säkerhetsnivå	3	DIT (3.9)
	Avgöra ifall skyddet är tillräckligt	3	H SÄK IT (24.1)
	Avgöra vad som utgör brister i skyddet	1	H SÄK IT (24.1)
	Avgöra om ett system är säkert	1	H SÄK IT (24.2)
	Avgöra behov av kontroll	2	H SÄK IT (24.3)
	Avgöra vilken nivå ett systems IT-säkerhet har	2	DIT (3.9)
	Beslut om åtgärdande av identifierade brister	1	H SÄK IT (24.4)

Kate-gori	Värderingsaspekt	Antal frågest.	Källa
	Avgöra behov av utveckling av den tekniska kontrollverksamheten	4	DIT (5.5.2)
	Beslut om åtgärder baserat på tekniska IT-säkerhetskontroller	2	H SÄK IT (24.4.2)
	IT-säkerhetsarbetets effektivitet	3	DIT (5.3.3)
	Mått på informationssäkerhetsverksamheten	6	DIT (5.5.5)
	Beslut om innehåll i IT-säkerhetsplan	3	H SÄK IT (8.9)
	Avgöra om IT-säkerheten upprätthålls	2	H SÄK IT (9.1)
	Beslut om förnyade analyser	2	H SÄK IT (11.1)
	Lägesbild över säkerhetsläget	3	H SÄK IT (9)
	Avgöra ifall informationssäkerheten upprätthålls	1	H SÄK IT (bilaga 1)
	Beslut om begränsning av användning	1	FIB 2006:2 (3 kap 5§)

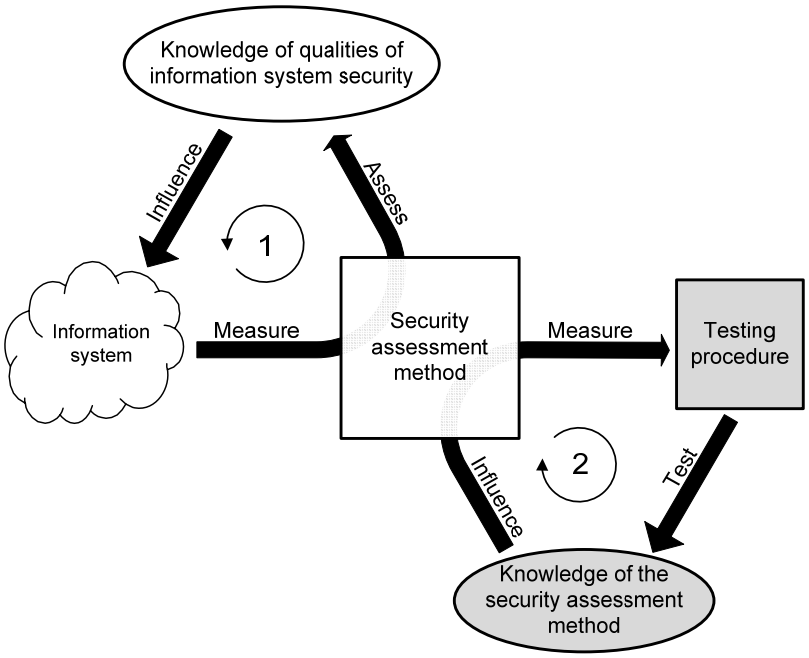
2.4 Procedur för test av relevans och validitet

Proceduren *Test of Security Assessment Relevance and validity*, TSAR, utvecklades för att möjliggöra ett snabbare sätt att genomföra en första utvärdering av en säkerhetsvärderingsmetod. Denna utvärdering resulterar i en beskrivning av till vilken grad säkerhetsvärderingsmetoder uppfyller vissa generella kvaliteter. Med hjälp av dessa kvalitetsvärden ges även möjligheten att kunna jämföra olika metoder. Proceduren är framtagen inom forskningsprojektet *Testning av metoder och verktyg för värdering av informationssäkerhet* för att möjliggöra de tester av värderingsmetoder inom Försvarsmakten som beskrivs i kapitel 4. Testproceduren beskrivs i sin helhet i den separata rapporten *The TSAR procedure – Test of Security Assessment Relevance and validity* (Bengtsson, J. Hallberg, Hunstad, & Löfvenberg, 2008).

2.4.1 Samband mellan säkerhetsvärderingsmetod och testprocedur

I Figur 2 illustreras sambandet mellan säkerhetsvärderingsmetod och testprocedur. Detta samband ger upphov till två stycken loopar vilka har till

uppgift att ge olika typer av återkoppling. Den första loopen beskriver återkopplingen som sker då en säkerhetsvärdering görs på ett informationssystem. Loopen utgår från en systemvärderare som förbereder indata till värderingsmetoden genom att göra mätningar på informationssystemet. Med hjälp av framtagen indata kan en säkerhetsvärdering av informationssystemet genomföras. Säkerhetsvärderingen resulterar i kunskap om olika kvaliteter hos informationssystemet. Dessa kunskaper används sedan av informationssystemets användare för att påverka systemet.



Figur 2: Samband mellan säkerhetsvärderingsmetod och testprocedur.

Den andra loopen i Figur 2 beskriver en liknande återkoppling där det istället är säkerhetsvärderingsmetoden som testas. Loopen utgår från att den testansvarige gör mätningar på säkerhetsvärderingsmetoden. Dessa mätningar används av den testansvarige som indata till testproceduren för att kunna testa säkerhetsvärderingsmetoden. Resultatet av testet används sedan av en systemvärderare för att påverka säkerhetsvärderingsmetoden.

2.4.2 Kvalitetsvärden

Med hjälp av testproceduren tas ett värde fram för var och en av de identifierade kvaliteterna *relevans* och *validitet*. Relevansen återspeglar till vilken grad

säkerhetsvärderingsmetoden motsvarar användarens behov, medan validiteten återspeglar till vilken grad säkerhetsvärderingsmetodens utdata stämmer överens med verkligheten. Dessa två kvaliteter återspeglar således om den testade säkerhetsvärderingsmetoden uppfyller de behov som användaren har samtidigt som den ger resultat som stämmer överens med verkligheten.

För att kunna avgöra till vilken grad de två kvaliteterna är uppfyllda görs mätningar på en mängd definierade egenskaper. Dessa egenskaper finns definierade i *TSAR tables*, som tagits fram i samband med utvecklingen av TSAR-proceduren. I dessa tabeller finns en mängd mätbara egenskaper definierade som har såväl med relevans som med validitet att göra.

2.4.3 Genomförande av test

Testet är indelat i sex stycken aktiviteter där två typer av aktörer deltar. Användaren är den som är i behov av en värderingsmetod, medan testansvarig är den som genomför testet. Den testansvarige kan även ha behov av ytterligare expertis för att genomföra testet.

Aktivitet 1 – Identifiera användarbehov

Den första aktiviteten är att identifiera de existerande användarbehoven. Detta då användarbehoven är grunden till att kunna identifiera en relevant säkerhetsvärderingsmetod. Aktiviteten utförs enbart av användaren, alternativt tillsammans med testansvarig, för att förtydliga vad användaren behöver från en säkerhetsvärderingsmetod. Användarbehoven kan till exempel formuleras med naturligt språk eller som en checklista. Denna aktivitet resulterar i en uppsättning användarbehov.

Aktivitet 2 – Välj relevanta attribut

Användarbehoven som identifierades i den första aktiviteten måste omvandlas till attribut. Med attribut avses de egenskaper hos en säkerhetsvärderingsmetod som man avser mäta. Attributen väljs bland de relevansrelaterade egenskaperna i TSAR-tabellerna. Denna aktivitet utförs av den testansvarige i samarbete med användaren för att säkerställa att omvandlingen genomförs så noggrant som möjligt och för att säkerställa att de identifierade användarbehoven fortfarande återspeglas. Aktiviteten resulterar i en uppsättning relevansrelaterade attribut.

Aktivitet 3 – Tilldela vikter till de relevansrelaterade attributen

Användaren och den testansvarige tilldelar gemensamt vikter till de relevansrelaterade attributen som togs fram i föregående aktivitet. Eftersom alla

relevansrelaterade attribut oftast inte är av samma betydelse för användaren tilldelas de vikter. Tilldelningen av vikter behöver endast göras för de relevansrelaterade attributen, eftersom vikterna för de validitetsrelaterade attributen är fördefinierade i testproceduren.

Det finns två olika tillvägagångssätt definierade när det gäller viktning av attribut. I denna rapport används det enklare tillvägagångssättet där attributen delas in i de två grupperna *mindre viktiga* och *viktiga*. Grupperna ska innehålla ungefär lika många attribut. Vikterna sätts sedan så att varje attribut i gruppen *viktiga* har en vikt som är dubbelt så stor som varje attribut i gruppen *mindre viktiga*. Den totala summan av alla vikter ska vara 1.

Denna aktivitet resulterar i en viktvektor för de relevansrelaterade attributen.

Aktivitet 4 – Mätning av attribut

Den testansvarige modellerar säkerhetsvärderingsmetoden genom att mäta de relevansrelaterade attributen, som valdes i aktivitet 2, och de validitetsrelaterade attributen. I likhet med tilldelningen av vikter i föregående aktivitet så finns det även två definierade tillvägagångssätt för att genomföra mätningen av attribut. Den enklare varianten av mätning innebär att varje attributvärde väljs som antingen 0 eller 1. Ett attribut som är uppfyllt ges värdet 1, medan ett som inte uppfylls ges värdet 0. Den mer avancerade varianten innebär att attribut kan vara delvis uppfyllda, dvs. tilldelas värden mellan 0 och 1. Denna variant kommer dock inte att användas i denna rapport.

Detta resulterar i en vektor med attributvärden för var och en av kvaliteterna relevans och validitet. Dessa vektorer utgör modellen av säkerhets-värderingsmetoden i de följande aktiviteterna. Om de validitetsrelaterade attributen redan mätts i ett tidigare test behöver de inte mätas om. Detta då användarbehoven inte påverkar validiteten hos en säkerhetsvärderingsmetod.

Aktivitet 5 – Beräkna kvalitetsvärden

Beräkningen av kvalitetsvärden för relevans och validitet baseras på de framtagna attributvärdevektorerna samt viktvektorerna. Relevansvärdevektorn multipliceras (inre produkt) med relevansattributens viktvektor, vilket ger ett relevansvärde. Beräkningen för validitetsvärdet görs på samma sätt. Beräkningarna genomförs av den testansvarige.

Aktivitet 6 – Tolka och diskutera resultatet

Efter att ha genomfört testet bör den testansvarige och användaren diskutera och utvärdera testresultatet. Genom att utvärdera resultatet är det möjligt att

säkerställa att användaren förstår anledningen till varför testresultatet blev som det blev. Under genomförandet av denna aktivitet kan det även beslutas om test av andra säkerhetsvärderingsmetoder bör genomföras.

3 Identifierade värderingsmetoder

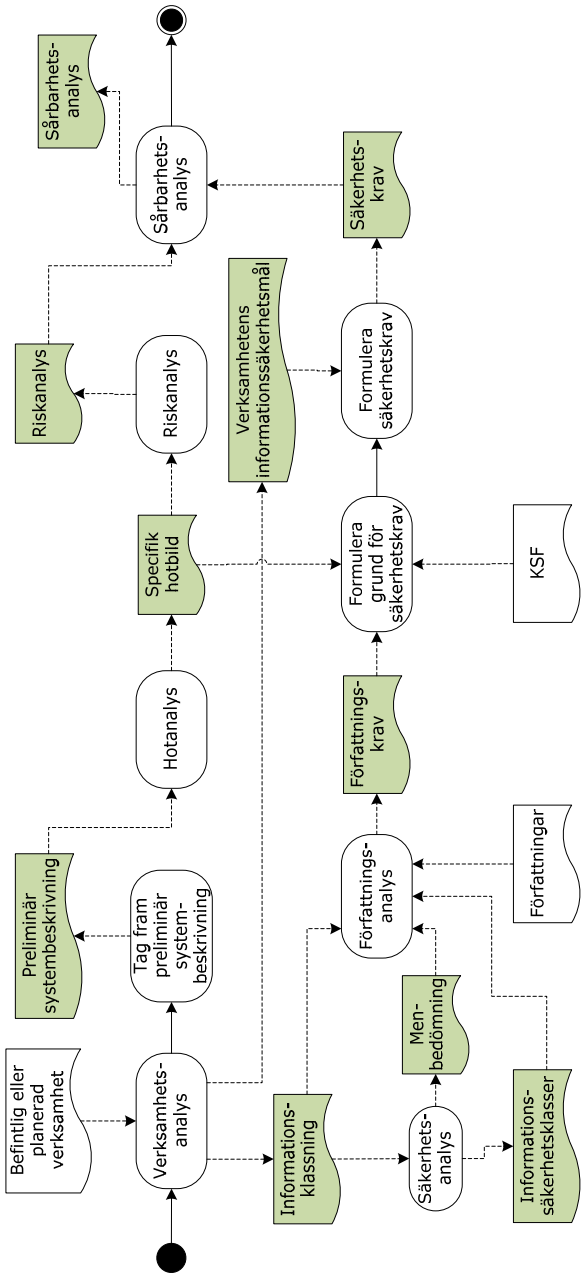
Då Försvarsmaktens ackrediteringsprocess är en omfattande och komplex process har här valts att i ett inledande skede beskriva en utvald del av denna process. En, ur säkerhetssynpunkt, viktig del i processen är framtagandet av underlag för auktorisationsbeslut B2. I detta beslut avgörs till stor del vilket material som behöver tas fram inför följande beslut. Det är således av stor betydelse att underlaget för auktorisationsbeslut B2 är så fullständigt som möjligt.

3.1 Framtagande av underlag för auktorisationsbeslut B2

Följande beskrivning är baserad på tidigare underlag som tagits fram av FOI (Bengtsson & J. Hallberg, 2008). Framtagandet av underlag för auktorisationsbeslut B2, som illustreras i Figur 3, inleds med att en *verksamhetsanalys* genomförs. Syftet med verksamhetsanalysen är att genom en övergripande beskrivning analysera den befintliga eller önskade verksamheten. En verksamhetsanalys omfattar även en informationsklassning där säkerhetsklassen bedöms hos den information som ska behandlas. Den framtagna informationsklassningen ligger till grund för en *säkerhetsanalys* som syftar till att bedöma huruvida de uppgifter IT-systemet ämnar behandla är hemliga. Under säkerhetsanalysen tas även en menbedömning fram.

En *författningsanalys* genomförs för att se över vilka lagar, förordningar, föreskrifter och bestämmelser som ska beaktas vid framtagandet av det berörda IT-systemet. Författningsanalysen resulterar i en uppsättning författningskrav.

För vissa IT-system ska en preliminär systembeskrivning tas fram. Huruvida detta ska göras har beslutats i auktorisationsbeslut B1. Den preliminära systembeskrivningen ska ge en tydligare bild över det planerade IT-systemet. För att avgöra vad som påverkar en myndighets säkerhetskritiska verksamhet genomförs *hot-, risk- och sårbarhetsanalyser*. I de flesta fall genomförs dessa analyser i en samlad analys, även om de egentligen ska genomföras separat. En *hotanalys* görs för att identifiera vilka hot IT-systemet exponeras för, vilket resulterar i en specifik hotbild. Den efterföljande *riskanalysen* genomförs för att identifiera de befintliga riskerna med avseende på den framtagna hotbilden. Innan sårbarhetsanalysen kan genomföras måste en uppsättning säkerhetskrav tas fram. Detta görs i aktiviteterna *formulera grund för säkerhetskrav* samt *formulera säkerhetskrav*. Kravmängden baseras i hög grad på fastställda krav på säkerhetsfunktioner (KSF) (Försvarsmakten, 2004b). En *sårbarhetsanalys* genomförs slutligen.



Figur 3: Framtagande av underlag för auktorisationsbeslut B2.

3.2 Val av studieobjekt

Beskrivningen som gjorts av framtagandet av underlag för auktorisationsbeslut B2 är relativt övergripande. Vi har valt att mer detaljerat beskriva de två delprocesserna *framtagande av säkerhetskrav* och *sårbarhetsanalys*. Delprocessen *framtagande av säkerhetskrav* innehåller aktiviteterna *formulera grund för säkerhetskrav* samt *formulera säkerhetskrav*. För att kunna ta fram en mer detaljerad beskrivning av dessa aktiviteter har frågeformulär, baserade på frågeställningarna i *Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete* (Bengtsson & J. Hallberg, 2008), tagits fram. Frågeformulär har skickats ut i två omgångar där den andra omgången bestod av förtydligade frågor från första utskicket samt några ytterligare frågor som framkommit vid analys av resultatet av första frågeomgången. Frågeformuläret från första omgången återges i Appendix A, medan frågeformuläret från andra omgången återges i Appendix B.

3.3 Sammanställning av resultat

De svar som erhölls på de formulerande frågeställningarna (Appendix A och B) har resulterat i följande sammanställning. Sammanställningen utgår från den struktur som den första uppsättningen med frågor har, det vill säga en fråga avseende den övergripande beskrivningen och ett antal frågor gällande de två studieobjekten. Vissa av frågorna har förtydligats.

3.3.1 Frågeställning avseende övergripande beskrivning

Fråga: Stämmer den övergripande beskrivningen av processen för framtagande av underlag för auktorisationsbeslut B2 som återges i Figur 1 med verkligheten?

> **Resultat:** Den övergripande beskrivningen stämmer med hur framtagande av underlag för auktorisationsbeslut B2 enligt befintlig dokumentation ska gå till.

3.3.2 Frågeställningar avseende formulering av grund för säkerhetskrav

Fråga: I vilken omfattning påverkar hotbild och författningskrav för aktuellt IT-system i realiteten formuleringen av grund för säkerhetskrav?

> **Resultat:** Den specifika hotbilden och författningskraven påverkar i väldigt liten utsträckning formuleringen av grund för säkerhetskrav.

Fråga: Hur visas att uppfyllelse av KSF leder till system med ”godtagbar IT-säkerhet”?

> **Resultat:** Att de krav som finns i KSF leder till system med adekvata säkerhetsnivåer avgörs av MUST.

Fråga: Hur anpassas KSF för en specifik hotbild?

> **Resultat:** KSF utgör en miniminivå. Vid formulering av grund för säkerhetskrav kan kraven skärpas genom att sätta KSF i relation till systemet i fråga och vid behov omformulera kraven.

Fråga: Hur avgörs om KSF, anpassad för en specifik hotbild, uppfyller miniminivån för IT-säkerhet inom FM?

> **Resultat:** Huruvida KSF, anpassad för en specifik hotbild, uppfyller miniminivån för IT-säkerhet inom FM avgörs av MUST och meddelas i yttrande inför B2-beslutet.

Fråga: Vilken status har KSFen? D.v.s. utgör de i KSFen specificerade kraven för aktuell informationsklassning:

- en utgångspunkt för att formulera grund för säkerhetskrav,
- hela grund för säkerhetskrav, eller
- direkt de säkerhetskrav som utgör indata till sårbarhetsanalysen?

> **Resultat:** De i KSFen specificerade kraven för aktuell informationsklassning utgör en utgångspunkt för att formulera grund för säkerhetskrav.

Fråga: Erbjuder IT-säkerhetstjänsten stöd vid framtagande av underlag för auktorisationsbeslut B2, och i så fall i vilka former?

> **Resultat:** IT-säkerhetstjänsten erbjuder inte formellt stöd vid framtagande av underlag för auktorisationsbeslut B2. Medhörning och informella synpunkter på framtagna lösningar erbjuds i mån av tid och lämplighet avseende systemets karaktär.

3.3.3 Frågeställningar avseende formulering av säkerhetskrav

Fråga: Hur påverkas säkerhetskraven av verksamhetens informationssäkerhets-mål?

> **Resultat:** Oftast påverkas inte säkerhetskraven av verksamhetens informationssäkerhetsmål. Indirekt kan verksamheten genom behov av

kommersiella system påverka säkerheten genom att de inkluderar säkerhetsfunktioner utöver det som krävs av ställda säkerhetskrav.

Fråga: Hur specificeras säkerhetskrav så att de är mätbara, entydiga och kompletta?

Resultat: Det är oklart hur detta ska uppnås. Tydlighet i kravställningen är en förutsättning, men hur det ska realiseras finns ej beskrivet. Ramverk och standarder kan vara ett stöd.

Fråga: Hur specificeras krav på avgränsningar mot omgivningen?

Resultat: Krav på avgränsningar mot omgivningen ges indirekt via informationssäkerhetsklasser. Kompletterande krav kan komma från de funktioner som fattar beslut inom auktorisationsprocessen.

Fråga: Vilka aktörer ansvarar för, respektive genomför aktiviteten kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen?

Resultat: Ansvaret för kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen ligger hos produktägaren ofta genom produktansvarig. Vilka aktörer som genomför aktiviteten varierar, oftast är det IT-personal.

Fråga: I vilka fall är det aktuellt att kravställa säkerhetsmekanismer i säkerhetsmålsättningen? Finns det något typfall (exempel) då detta är aktuellt?

Resultat: Det är mycket ovanligt att kravställa säkerhetsmekanismer i säkerhetsmålsättningen och bör endast ske om hot- och riskanalyser ger vid handen att aktuella säkerhetskrav behöver förfinas.

Fråga: Vilken är relationen mellan kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen och sårbarhetsanalysen?

Resultat: Resultatet av sårbarhetsanalysen bör kunna påverka kravställningen avseende säkerhetsfunktioner i säkerhetsmålsättningen, men det är oklart hur detta i så fall sker.

3.3.4 Frågeställningar avseende förutsättningar för sårbarhetsanalys

Fråga: Sårbarhetsanalysen ingår som underlag till B2 (Försvarsmakten, 2007, s. 8), men är det endast där?

Resultat: Sårbarhetsanalysen genomförs endast inför B2.

Fråga: Utgör den tekniska produktspecifikationen underlag för sårbarhetsanalysen?

> **Resultat:** Sårbarhetsanalysen utgör underlag för den tekniska produktspecifikationen som tas fram inför B3.

Fråga: Hur beskrivs systemets funktionalitet, som underlag för sårbarhetsanalysen?

> **Resultat:** En preliminär systembeskrivning utgör underlag för sårbarhetsanalysen. Det är upp till den enskilde handläggaren att avgöra vilken omfattning den preliminära systembeskrivningen ska ha.

Fråga: Behöver *Preliminär systembeskrivning* (Försvarsmakten, 2007, s. 8) tas fram för majoriteten av de system som ska genomgå ackrediteringsprocessen?

> **Resultat:** Troligtvis behöver ingen *Preliminär systembeskrivning* tas fram för majoriteten av de system som ska genomgå ackrediterings-processen. I de fall då systemet påverkar andra system eller innehåller hittills ej använda produkter kan det vara aktuellt. Om en beskrivning tas fram är den oftast väldigt övergripande på grund av att budgeten är ytterst begränsad under de tidiga faserna av livscykeln.

Fråga: Inför vilket auktorisationsbeslut (B2-B4) ska en eventuell *Preliminär systembeskrivning* tas fram?

> **Resultat:** Inför vilket auktorisationsbeslut som en eventuell *Preliminär systembeskrivning* tas fram beror på B1.

3.3.5 Frågeställningar avseende genomförande av sårbarhetsanalys

Fråga: Vilka verktyg (dokumentmallar, mjukvara, etc.) används för att genomföra sårbarhetsanalyser?

> **Resultat:** Det finns inga standardiserade verktyg för genomförande av sårbarhetsanalyser. Återanvändning av tidigare upparbetad kompetens är ett viktigt instrument. Detta innebär i praktiken att genomförandet av sårbarhetsanalyser läggs på någon som har gjort det tidigare.

Fråga: Hur stödjer MAACK genomförandet av sårbarhetsanalyser?

> **Resultat:** MAACK tillhandahåller inget stöd för genomförandet av sårbarhetsanalyser.

Fråga: Vilket metodikstöd (specifikationer av arbetsprocesser) tillhandahålls som stöd för genomförandet av sårbarhetsanalyser?

> **Resultat:** H SÄK IT innehåller det metodikstöd som finns för genomförandet av sårbarhetsanalyser

Fråga: Hur avgörs säkerhetskravens förmåga att eliminera risker?

> **Resultat:** Det är upp till handläggaren att avgöra. Det är ospecificerat vilka metoder som ska användas och några objektiva metoder finns ej.

Fråga: Är det vanligt att sårbarhetsanalysen är iterativ?

> **Resultat:** Det är oklart hur ofta sårbarhetsanalyser är iterativa, det vill säga genomlöps mer än en gång på grund av uppdatering av system-funktionalitet eller säkerhetskrav. Omackreditering är ovanligt; en fastställd säkerhetsmålsättning ligger fast.

Fråga: Hur avgörs det när ”de bedömda resulterande riskvärdena hos sårbarheterna har nått tillräckligt låga och acceptabla nivåer”?

> **Resultat:** Det är upp till handläggaren att avgöra. Olika skalor för riskvärden förekommer. Det är ospecificerat vilka av dessa som ska användas och några objektiva metoder finns ej.

Fråga: Vilka aktörer genomför i praktiken sårbarhetsanalyser för IT-system?

> **Resultat:** Ansvar för genomförandet av sårbarhetsanalys ligger hos produktägaren, ofta genom produktansvarig, men andra aktörer kan stödja. Medverkan från verksamhetsansvariga och användare saknas alltför ofta, vilket ökar sannolikheten för orimliga bedömningar.

Fråga: Vilka kriterier ligger till grund för beslut om hur sårbarheter (kvarvarande risker) ska behandlas, dvs. om funktionalitet ska tas bort, kraven ska uppdateras eller sårbarheterna ska riskhanteras?

> **Resultat:** Exempel på kriterier som ligger till grund för beslut om hur sårbarheter ska behandlas är menbedömning, kostnad för åtgärd och konsekvens ifall sårbarhet utnyttjas.

Fråga: Sårbarheter är risker vars nivåer är för höga för att kunna accepteras. Vad innebär det, i realiteten, att sårbarheter riskhanteras (dvs. vad gör man)?

> **Resultat:** Det är oklart vad som avses med riskhantering. Det finns olika uppfattningar om vad riskhantering innebär. Det finns till och med en risk att det vid systemutveckling kan användas i betydelsen ”inte mitt problem”.

3.3.6 Frågeställningar avseende sårbarhetsanalysers resultat

Fråga: På vilket sätt erhålls konsekvensanalyser ur sårbarhetsanalyser?

> **Resultat:** Det är oklart hur den i H SÄK IT (avsnitt 8.6) omnämnda härledningen av konsekvenser av brist på konfidentialitet, riktighet, tillgänglighet och spårbarhet uppstår under hot-, risk- och sårbarhetsanalyserna.

Fråga: Hur används resultat från genomförda sårbarhetsanalyser, förutom att de ingår som en del i säkerhetsmålsättningen?

> **Resultat:** Ofta används resultat från genomförda sårbarhetsanalyser inte vidare efter att processen har genomförts. I vissa fall används dock resultaten löpande för att följa upp och kontrollera system med tillhörande verksamhet. I vissa fall används resultaten för att jämföra med faktiskt utfall (t ex på kvartalsbasis) av riskerna. Resultaten kan även utgöra grund för utbildningsmaterial.

3.4 Beskrivning av studieobjekt

3.4.1 Framtagande av säkerhetskrav

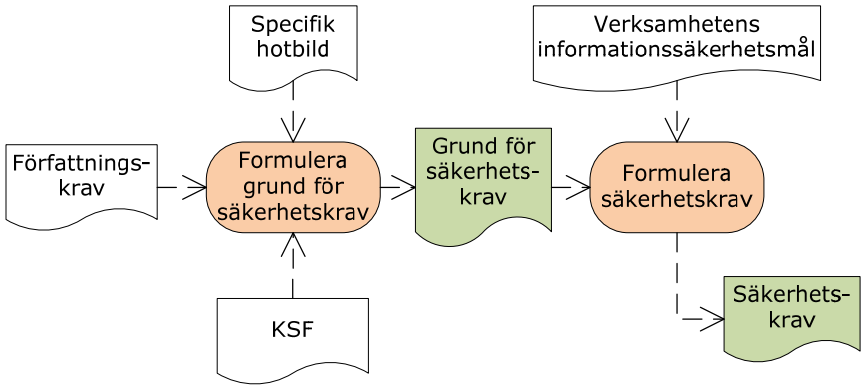
Baserat på dokument och erhållna kommentarer beskriver detta avsnitt processen för framtagande av säkerhetskrav. Processen illustreras i Figur 4. I den textuella beskrivningen återges de aktiviteter och resultat som återfinns i figuren med kursiv text. Den beskrivna processen kan ses som en metod för att fastställa säkerhetskrav vilkas realisering kommer att ge ett system med adekvat säkerhetsnivå. Därmed kan metodens relevans och validitet avseende värdering av säkerhet testas med TSAR-proceduren, se kapitel 4.

Utgående ifrån identifierade *författningskrav*, *specifik hotbild*, samt Försvarsmaktens krav på godkända säkerhetsfunktioner (*KSF*) formuleras en *grund för säkerhetskrav*. I realiteten används författningskraven för att välja en delmängd av de krav som formulerats i KSFen. Om så är påkallat av aktuell hotbild kan säkerhetskraven skärpas.

Grund för säkerhetskrav används sedan tillsammans med verksamhetens informationssäkerhetsmål för att formulera de *säkerhetskrav* som ställs på det framtagna IT-systemet. Det är helt upp till handläggaren huruvida *grund för säkerhetskrav* uppdateras i detta steg eller helt enkelt kommer att utgöra *säkerhetskraven*. Indirekt kan verksamheten genom behov av kommersiella

system påverka säkerheten genom att de inkluderar säkerhetsfunktioner utöver det som krävs av ställda säkerhetskrav.

För att uppnå mätbara, entydiga och kompletta säkerhetskrav kan ramverk och standarder, såsom Common Criteria (Common Criteria, 2004) och ISO/IEC 27002 (ISO/IEC, 2005), nyttjas.



Figur 4: Aktiviteter och artefakter som ingår i framtagandet av säkerhetskrav.

3.4.2 Sårbarhetsanalys

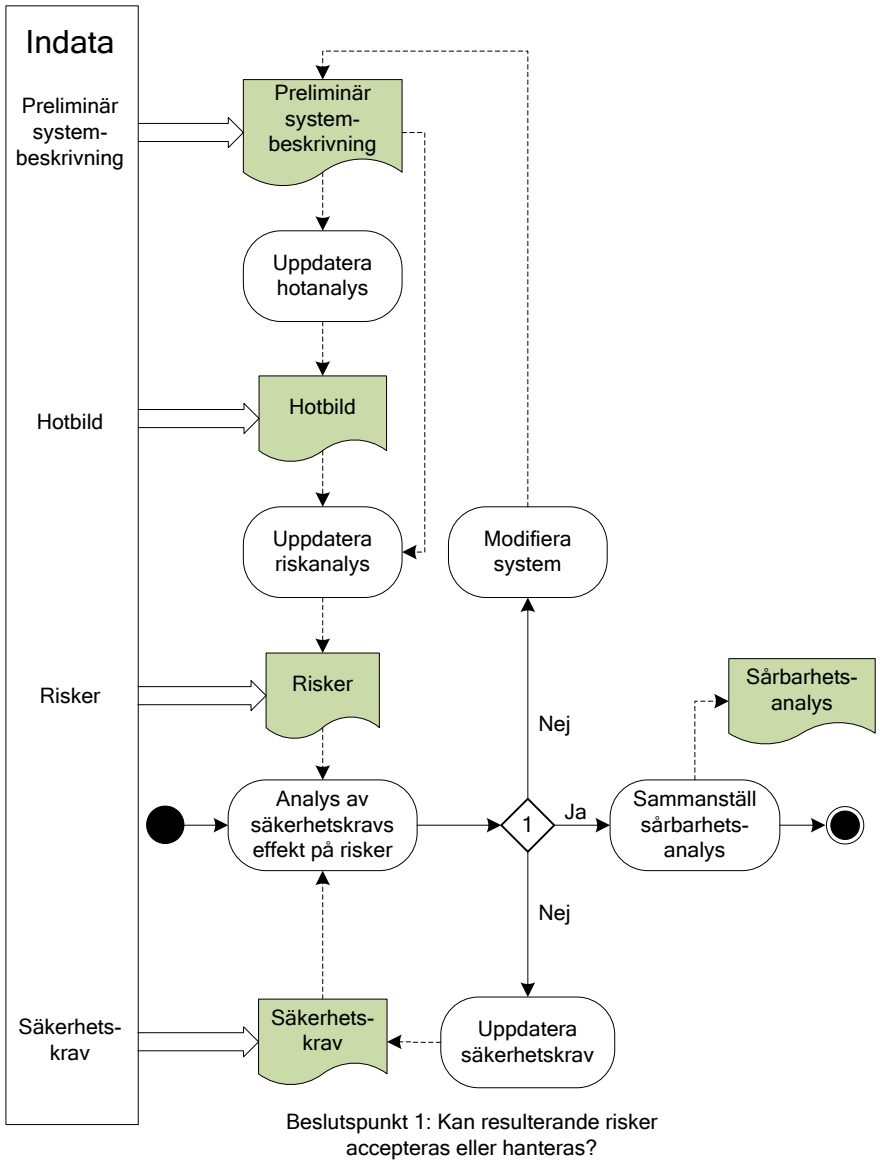
Sårbarhetsanalysen utgår ifrån hotbilden och riskanalysen som erhålls ur hot- och riskanalyserna. Vidare utgörs underlaget för sårbarhetsanalysen av de säkerhets-krav som hittills framtagits under arbetet med underlaget för auktorisationsbeslut B2. För att kunna modifiera systemet, om det är nödvändigt för att begränsa riskerna, krävs också en preliminär systembeskrivning.

De identifierade hoten och riskerna jämförs med säkerhetskraven för att bedöma till vilken grad de, av säkerhetskraven resulterande säkerhetslösningarna, kommer att eliminera eller reducera förekommande riskvärden. Samtliga risker prövas för att slutligen erhålla resulterande riskvärden. De resulterande riskvärdena benämns som förekommande sårbarheter.

Om de identifierade sårbarheterna är acceptabla eller kan riskhanteras[1] är sårbarhetsanalysen slutförd. I annat fall måste antingen säkerhetskraven omformuleras för att bättre kunna reducera de förekommande riskerna, eller IT-systemet modifieras genom att funktionalitet relaterad till de kvarvarande sårbarheterna tas bort. Detta bildar en iterativ process som pågår tills de

[1] Denna användning av termen riskhantering är olycklig då den insinuerar att innebörden av riskhantering är att de aktuella riskerna måste accepteras.

kvarvarande riskerna är tillräckligt begränsade för att kunna accepteras eller hanteras (Figur 5).



Figur 5: Aktiviteter, artefakter och beslutspunkter som ingår i eller relaterar till processen för sårbarhetsanalys.

4 Test av identifierade värderingsmetoder

I detta kapitel genomförs tester av relevans och validitet avseende värdering av IT-säkerhet hos de två utvalda studieobjekten *framtagande av säkerhetskrav* samt *sårbarhetsanalys*. Genomförandet involverar de sex steg som presenteras i avsnitt 2.4.3.

4.1 Framtagande av säkerhetskrav

Aktivitet 1 – Identifiera användarbehov

Användarbehoven tas fram av eller i dialog med användare alternativt, i de fall då användare utgörs av en process, baseras på specificeringar av vilka indata processen behöver. I detta fall kan de generella behoven utläsas från den omgivande processen, dvs. *ta fram underlag för auktorisationsbeslut B2* (Figur 3).

Användarnas generella behov är att kunna formulera listor med kompletta, konsistenta, mätbara och entydiga säkerhetskrav (J. Hallberg, N. Hallberg, Hunstad, & Ölvander, 2006). För att kunna göra detta behövs förmåga att avgöra hur enskilda säkerhetskrav kan påverka säkerhetsnivån, hos det system som ska utvecklas. Kravmängden baseras på KSF samt eventuella tillkommande krav härledda från på den specifika hotbilden samt verksamhetens informations-säkerhetsmål. Säkerhetsvärderingen syftar till att avgöra om den framtagna kravmängden ger tillräcklig hög säkerhetsnivå. Alltså ska de säkerhetskrav som erhålls från KSF värderas utifrån den specifika hotbilden och verksamhetens informationssäkerhetsmål.

Aktivitet 2 – Välj relevanta attribut

Användarbehoven som identifierats i den första aktiviteten måste omvandlas till attribut. Med attribut avses de egenskaper hos en säkerhetsvärderingsmetod som man ämnar mäta. Attributen väljs bland de relevansrelaterade egenskaperna i TSAR-tabellerna. Den resulterande uppsättningen av relevansrelaterade attribut återges i Tabell 2.

Tabell 2: Relevansrelaterade attribut.

ID	Attributnamn
1.1.1	Requirements engineering
1.1.5	Accreditation
1.2.1.1	Technical
1.2.1.2	Organizational
1.2.1.4	Operational
1.2.1.5	Contextual
1.2.3.3	Entity characteristics
1.2.3.4	System-wide characteristics
1.2.3.5	Structural characteristics
1.3.1.1	Computer components
1.3.1.2	Computers
1.3.1.3	Networked systems
1.3.1.4	Humans
1.3.1.5	Organizational units
1.3.1.6	System processes
1.3.1.7	System characteristics
1.3.2	System entity inter-relations
1.3.3	Multiple abstraction levels
1.3.4	Hierarchical models
1.3.5	Established modeling technique/language
1.4.1	Atomic security values
1.4.2	Aggregated security values
1.4.3	Security values inter-relations
1.5.1	Related to system modeling
1.5.2	Related to computations modeling
1.5.3	Related to security values computation
1.5.4	Related to measurements
1.8	Interpret security values
1.9.1	Reuse produced data from previous assessments of the same system
1.9.2	Reuse produced data from previous assessment of other systems
1.9.3	Need of consulting experts to prepare the input to the security assessment method
1.9.4	Need of consulting experts to perform the security assessment

Aktivitet 3 – Tilldela vikter till de relevansrelaterade attributen

Enligt beskrivningen i avsnitt 2.4.3 tilldelas vikter till de valda relevansrelaterade attributen genom att de delas in i två ungefär lika stora grupper av viktiga och mindre viktiga attribut. De viktiga attributen får vikter som är dubbelt så stora

som de mindre viktiga och den totala summan av alla vikter ska vara 1. Resultatet av viktningen återges i Tabell 4 nedan.

Aktivitet 4 – Mätning av attribut

Mätningen av relevans- och validitetsrelaterade attribut baseras på den skiss av metod för framtagande av säkerhetskrav som återges i avsnitt 3.4.1. Resultaten avseende relevans återges i Tabell 4 nedan, medan resultaten avseende validitet återfinns i Tabell 3.

Tabell 3: Resultat från mätning av validitetsattribut.

ID	Attributnamn	Värde
2.1.1	Temporal aspects	0
2.2.1	System entity inter-relations	0
2.3.1	Security values inter-relation	0
2.4.1	Implementation of the computational model	0
2.4.2	Objective measurement	0
2.5	Security assessment results	1
2.6.1	Specification of relevant security characteristics	1
2.6.2	Specification of system extent	1
2.7.1	System modeling regarding system entities	0
2.7.2	Identification of system characteristics and effects	1
2.7.3	System modeling regarding measurable system characteristics and effects	0
2.7.4	Specification of a computational model	0
2.8.1	Review of the quality of associated values	0
2.8.2	Association of values with measurable system characteristics and effects	0
2.9.1	Adding information to computations	0
2.9.2	Detecting relevant information	0
2.9.3	Handling system context factors	0

Aktivitet 5 – Beräkna kvalitetsvärden

Kvalitetsvärdena för relevans och validitet avseende framtagande av säkerhetskrav erhålls genom att multiplicera de framtagna attributvärdena med de satta vikterna och summera dessa viktade värden. Resultaten avseende relevans och validitet återfinns i Tabell 4 respektive Tabell 5.

Tabell 4: Framtagande av relevansvärde.

ID	Värde	Vikt	Viktat värde
1.1.1	1	1/48	1/48
1.1.5	1	1/48	1/48
1.2.1.1	1	1/24	1/24
1.2.1.2	0	1/48	0
1.2.1.4	0	1/24	0
1.2.1.5	1	1/48	1/48
1.2.3.3	0	1/48	0
1.2.3.4	1	1/24	1/24
1.2.3.5	0	1/48	0
1.3.1.1	0	1/48	0
1.3.1.2	0	1/48	0
1.3.1.3	0	1/48	0
1.3.1.4	0	1/48	0
1.3.1.5	0	1/48	0
1.3.1.6	1	1/48	1/48
1.3.1.7	1	1/24	1/24
1.3.2	0	1/48	0
1.3.3	0	1/48	0
1.3.4	0	1/48	0
1.3.5	0	1/24	0
1.4.1	0	1/24	0
1.4.2	0	1/24	0
1.4.3	0	1/24	0
1.5.1	0	1/24	0
1.5.2	0	1/24	0
1.5.3	0	1/24	0
1.5.4	0	1/24	0
1.8	0	1/24	0
1.9.1	0	1/48	0
1.9.2	0	1/24	0
1.9.3	0	1/24	0
1.9.4	0	1/24	0
	Relevansvärde		**0,21**

Tabell 5: Framtagande av validitetsvärde.

ID	Värde	Vikt	Viktat värde
2.1.1	0	1/26	0
2.2.1	0	1/13	0
2.3.1	0	1/13	0
2.4.1	0	1/26	0
2.4.2	0	1/13	0
2.5	1	1/13	1/13
2.6.1	1	1/26	1/26
2.6.2	1	1/26	1/26
2.7.1	0	1/13	0
2.7.2	1	1/13	1/13
2.7.3	0	1/13	0
2.7.4	0	1/13	0
2.8.1	0	1/26	0
2.8.2	0	1/13	0
2.9.1	0	1/26	0
2.9.2	0	1/26	0
2.9.3	0	1/26	0
	Validitetsvärde		**0,23**

Aktivitet 6 – Tolka och diskutera resultatet

Resultaten av testerna diskuteras i kapitel 5.

4.2 Sårbarhetsanalys

Aktivitet 1 – Identifiera användarbehov

Användarbehoven tas fram av eller i dialog med användare alternativt, i de fall då användare utgörs av en process, baseras på specificeringar av vilka indata processen behöver. I detta fall kan de generella behoven utläsas från den omgivande processen, dvs. *ta fram underlag för auktorisationsbeslut B2* (Figur 3).

Avseende sårbarhetsanalys är användarnas initiala behov att avgöra till vilken grad säkerhetskraven sänker de identifierade riskerna. Säkerhetsvärderingar stödjer bedömning av effekter avseende sannolikheter för realisering av hot. Vidare uppstår det, då riskerna inte kan reduceras till en acceptabel nivå eller

hanteras, behov av att kunna avgöra vilka effekter modifiering av systemet eller säkerhetskraven får. Vid uppdatering av säkerhetskrav uppstår samma problematik avseende säkerhetsvärdering som vid framtagande av säkerhetskrav (avsnitt 4.1).

Aktivitet 2 – Välj relevanta attribut

Användarbehoven som identifierats i den första aktiviteten måste omvandlas till attribut. Med attribut avses de egenskaper hos en säkerhetsvärderingsmetod som man ämnar mäta. Attributen väljs bland de relevansrelaterade egenskaperna i TSAR-tabellerna. Den resulterande uppsättningen av relevansrelaterade attribut återges i Tabell 6.

Tabell 6: Relevansrelaterade attribut.

ID	Attributnamn
1.1.1	Requirements engineering
1.1.3	Risk management
1.1.5	Accreditation
1.2.1.1	Technical
1.2.1.2	Organizational
1.2.1.4	Operational
1.2.1.5	Contextual
1.2.3.3	Entity characteristics
1.2.3.4	System-wide characteristics
1.2.3.5	Structural characteristics
1.3.1.1	Computer components
1.3.1.2	Computers
1.3.1.3	Networked systems
1.3.1.4	Humans
1.3.1.5	Organizational units
1.3.1.6	System processes
1.3.1.7	System characteristics
1.3.2	System entity inter-relations
1.3.3	Multiple abstraction levels
1.3.4	Hierarchical models
1.3.5	Established modeling technique/language
1.4.1	Atomic security values
1.4.2	Aggregated security values
1.4.3	Security values inter-relations
1.5.1	Related to system modeling
1.5.2	Related to computations modeling
1.5.3	Related to security values computation

ID	Attributnamn
1.5.4	Related to measurements
1.8	Interpret security values
1.9.1	Reuse produced data from previous assessments of the same system
1.9.2	Reuse produced data from previous assessment of other systems
1.9.3	Need of consulting experts to prepare the input to the security assessment method
1.9.4	Need of consulting experts to perform the security assessment

Aktivitet 3 – Tilldela vikter till de relevansrelaterade attributen

Enligt beskrivningen i avsnitt 2.4.3 tilldelas vikter till de valda relevansrelaterade attributen genom att de delas in i två ungefär lika stora grupper av viktiga och mindre viktiga attribut. De viktiga attributen får vikter som är dubbelt så stora som de mindre viktiga och den totala summan av alla vikter ska vara 1. Resultatet av viktningen återfinns i Tabell 8 nedan.

Aktivitet 4 – Mätning av attribut

Mätningen av relevans- och validitetsrelaterade attribut baseras på den skiss av metod för sårbarhetsanalys som återges i avsnitt 3.4.1. Resultaten avseende relevans återges i Tabell 8 nedan, medan resultaten avseende validitet återfinns i Tabell 7.

Tabell 7: Resultat från mätning av validitetsattribut.

ID	Attributnamn	Värde
2.1.1	Temporal aspects	0
2.2.1	System entity inter-relations	0
2.3.1	Security values inter-relation	0
2.4.1	Implementation of the computational model	0
2.4.2	Objective measurement	0
2.5	Security assessment results	1
2.6.1	Specification of relevant security characteristics	1
2.6.2	Specification of system extent	1
2.7.1	System modeling regarding system entities	0
2.7.2	Identification of system characteristics and effects	1
2.7.3	System modeling regarding measurable system characteristics and effects	0
2.7.4	Specification of a computational model	0
2.8.1	Review of the quality of associated values	0

ID	Attributnamn	Värde
2.8.2	Association of values with measurable system characteristics and effects	0
2.9.1	Adding information to computations	0
2.9.2	Detecting relevant information	0
2.9.3	Handling system context factors	0

Aktivitet 5 – Beräkna kvalitetsvärden

Kvalitetsvärdena för relevans och validitet avseende säkerhetsvärdering inom ramen för sårbarhetsanalys erhålls genom att multiplicera de framtagna attributvärdena med de satta vikterna och summera dessa viktade värden. Resultaten avseende relevans och validitet återfinns i Tabell 8 respektive Tabell 9.

Tabell 8: Framtagande av relevansvärde.

ID	Värde	Vikt	Viktat värde
1.1.1	1	1/50	1/50
1.1.3	1	1/25	1/25
1.1.5	1	1/50	1/50
1.2.1.1	1	1/25	1/25
1.2.1.2	0	1/50	0
1.2.1.4	0	1/25	0
1.2.1.5	0	1/50	0
1.2.3.3	0	1/50	0
1.2.3.4	1	1/25	1/25
1.2.3.5	0	1/50	0
1.3.1.1	0	1/50	0
1.3.1.2	0	1/50	0
1.3.1.3	0	1/50	0
1.3.1.4	0	1/50	0
1.3.1.5	0	1/50	0
1.3.1.6	0	1/50	0
1.3.1.7	0	1/25	0
1.3.2	0	1/50	0
1.3.3	0	1/50	0
1.3.4	0	1/50	0
1.3.5	0	1/25	0
1.4.1	1	1/25	1/25
1.4.2	0	1/25	0
1.4.3	0	1/25	0

ID	Värde	Vikt	Viktat värde
1.5.1	0	1/25	0
1.5.2	0	1/25	0
1.5.3	0	1/25	0
1.5.4	0	1/25	0
1.8	0	1/25	0
1.9.1	1	1/50	1/50
1.9.2	1	1/25	1/25
1.9.3	0	1/25	0
1.9.4	0	1/25	0
	Relevansvärde		**0,26**

Tabell 9: Framtagande av validitetsvärde.

ID	Värde	Vikt	Viktat värde
2.1.1	0	1/26	0
2.2.1	0	1/13	0
2.3.1	0	1/13	0
2.4.1	0	1/26	0
2.4.2	0	1/13	0
2.5	1	1/13	1/13
2.6.1	1	1/26	1/26
2.6.2	1	1/26	1/26
2.7.1	0	1/13	0
2.7.2	1	1/13	1/13
2.7.3	0	1/13	0
2.7.4	0	1/13	0
2.8.1	0	1/26	0
2.8.2	0	1/13	0
2.9.1	0	1/26	0
2.9.2	0	1/26	0
2.9.3	0	1/26	0
	Validitetsvärde		**0,23**

Aktivitet 6 – Tolka och diskutera resultatet

Resultaten av testerna diskuteras i kapitel 5.

5 Diskussion

Syftet med arbetet som presenteras i denna rapport har varit att beskriva befintliga metoder för värdering av säkerhet i Försvarsmaktens IT-system. För detta ändamål har testproceduren TSAR formulerats (Bengtsson et al., 2008), vilken utgår från de två kvaliteterna relevans och validitet för att beskriva säkerhetsvärderingsmetoder.

För att genomföra testerna är TSAR-proceduren beroende av metodbeskrivningar. Den studie som genomförts under arbetet med denna rapport har inte resulterat i vare sig kompletta eller korrekta beskrivningar av de identifierade processerna. Detta beror delvis på att motstridiga uppgifter framkommit i analysen av svaren på ställda frågor (Appendix A och B) samt dokumentation. Konsekvensen av detta är att kompletta och korrekta metodbeskrivningar saknas för de identifierade processerna för *framtagande av säkerhetskrav* och *sårbarhetsanalys*. Detta leder till att:

- De genomförda testerna utgår från ofullständigt underlag.
- Resultaten inte nödvändigtvis är rättvisande utgående från att enskilda individer mycket väl kan använda sig av mer strukturerade, men inte beskrivna, metoder för säkerhetsvärdering.
- De mer avancerade tillvägagångssätten i TSAR-proceduren för viktning och mätning av validitets- och relevansattribut har inte varit tillämpbara.

De genomförda testerna resulterade i väldigt låga relevans- och validitetsvärden för de testade värderingsmetoderna. För att uppnå högre relevans- och validitetsvärden måste tydligare formulering och dokumentation tas fram för processerna med tillhörande metoder. Det som nu finns beskrivet svarar på *vad* som ska göras, men inte *hur*. MAACK ger inte mycket stöd, då det i grund och botten är en samling dokumentmallar innehållande sammanfattningar av *vad*-beskrivningarna i H SÄK IT och DIT 04.

Vid formulering av grund för säkerhetskrav verkar den gängse metoden vara att utifrån identifierade informationssäkerhetsklasser välja tillämpliga delar av KSF (Försvarsmakten, 2004b). Författningskraven verkar endast indirekt påverka formuleringen av grund för säkerhetskrav som indata vid framtagande av KSF. Då den specifika hotbilden endast kan höja kravnivån har den sannolikt ringa inverkan på formulering av grund för säkerhetskrav, om aktuella handläggare inte vill försvåra en redan komplex process.

En delmängd av underlaget för denna studie har inhämtats via intervjuer och diskussioner med personer med anknytning till auktorisations- och

ackrediteringsprocessen. Detta har lett till att det har framkommit information som inte har direkt anknytning till de formulerade frågeställningarna. Av intresse för det fortsatta arbetet återges även följande observationer.

- Det har framkommit att auktorisations- och ackrediteringsprocessen inte stämmer med de förutsättningar som gäller inom FM. Ofta är en beställning av ett system lagd redan innan auktorisationsprocessen initieras. Tanken med auktorisationsprocessen är att rationalisera systemutvecklingen inom FM genom att öka återanvändningen och endast utveckla system då det finns behov därav. Då beslut om att system ska utvecklas finns, har behov av systemet redan fastslagits. Framtagandet av B1- till B4-underlagen blir då en efterhandskonstruktion.
- Auktorisations- och ackrediteringsprocessen är anpassad för avgränsade mindre produkter, ej för hela system, vilket leder till brist på helhetssyn och kontraproduktiva krav.
- Systembilden är väldigt vag då B2-underlaget tas fram. Orsaken är att det är först senare i livscykeln som det finns resurser att ta fram mer än övergripande beskrivningar av systemet, även på en hög abstraktionsnivå.
- Det är inte alltid den säkerhetsmässigt bästa lösningen som väljs utan den som kommer att godkännas i ackrediteringsprocessen. Ett typfall är att en äldre teknik som tidigare har godkänts kan väljas istället för en nyare som ej tidigare har godkänts.

Referenser

Bengtsson, J., & Hallberg, J. (2008). *Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete*. Underlagsrapport, Totalförsvarets forskningsinstitut, FOI.

Bengtsson, J., Hallberg, J., Hunstad, A., & Löfvenberg, J. (2008). *The TSAR procedure – Test of Security Assessment Relevance and validity*. Scientific report, Swedish Defence Research Agency, FOI.

Common Criteria. (2004). Common Criteria for Information Technology Security Evaluation, version 2.2 - Part 1: Introduction and general model. . Retrieved August 18, 2008, from http://www.commoncriteriaportal.org/thecc.html.

Försvarsmakten. (2004a). *Direktiv för Försvarsmaktens informationsteknikverksamhet*.

Försvarsmakten. (2004b). *Krav på säkerhetsfunktioner - Grunder*. 10 750: 78976, Högkvarteret.

Försvarsmakten. (2006a). *Försvarsmaktens interna bestämmelser om IT-säkerhet, FIB 2006:2*.

Försvarsmakten. (2006b). *Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik (H SÄK IT)*.

Försvarsmakten. (2007). *Metodik Ansökan om auktorisation, version 1.8. Bilaga till MAACK – Metod- & utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten*.

Hallberg, J., Hallberg, N., Hunstad, A., & Ölvander, C. (2006). *Kravanalys avseende värdering av IT-säkerhet*. FOI Memo 1760, Totalförsvarets forskningsinstitut, FOI.

ISO/IEC. (2005). *ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management*.

Kulak, D., & Guiney, E. (2000). *Use Cases: Requirements in Context* (1st ed., p. 329). Addison-Wesley Professional.

Nationalencyklopedin. (2008a). Informationssystem. In *Nationalencyklopedin*. Retrieved December 2, 2008, from http://www.ne.se/artikel/211494.

Nationalencyklopedin. (2008b). Metod. In *Nationalencyklopedin (Kort)*. Retrieved November 18, 2008, from http://www.ne.se/artikel/1403918.

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

Appendix A – Underlag utskick 1

Frågeställningar relaterade till framtagande av underlag för auktorisationsbeslut B2

Johan Bengtsson & Jonas Hallberg
Totalförsvarets forskningsinstitut, Olaus Magnus väg 42, SE-583 30, Linköping
{johan.bengtsson, jonas.hallberg}@foi.se

1 Inledning

Framtagandet av ackrediteringsunderlag är centralt för att skapa förutsättningar för adekvat informationssäkerheten inom Försvarsmaktens IT-system. Inom ramen för FoT-projektet Testning av metoder och verktyg för värdering av informationssäkerhet pågår ett arbete med att modellera praxis för hur informationssäkerhet värderas vid framtagandet av ackrediteringsunderlag för IT-system.

I avsnitt 1.1 ges en övergripande beskrivning av processen för framtagande av underlag för auktorisationsbeslut B2. Denna beskrivning baseras på den befintliga dokumentationen i H SÄK IT [1], DIT 04 [2], FIB 2006:2 [3] och MAACK [4] (Figur 1). Syftet med denna översiktliga beskrivning är att ge ett sammanhang för två av de ingående delprocesserna: formulera säkerhetskrav samt sårbarhetsanalys. De frågeställningar som återfinns i kapitel 2 och 3 relaterar till dessa delprocesser.

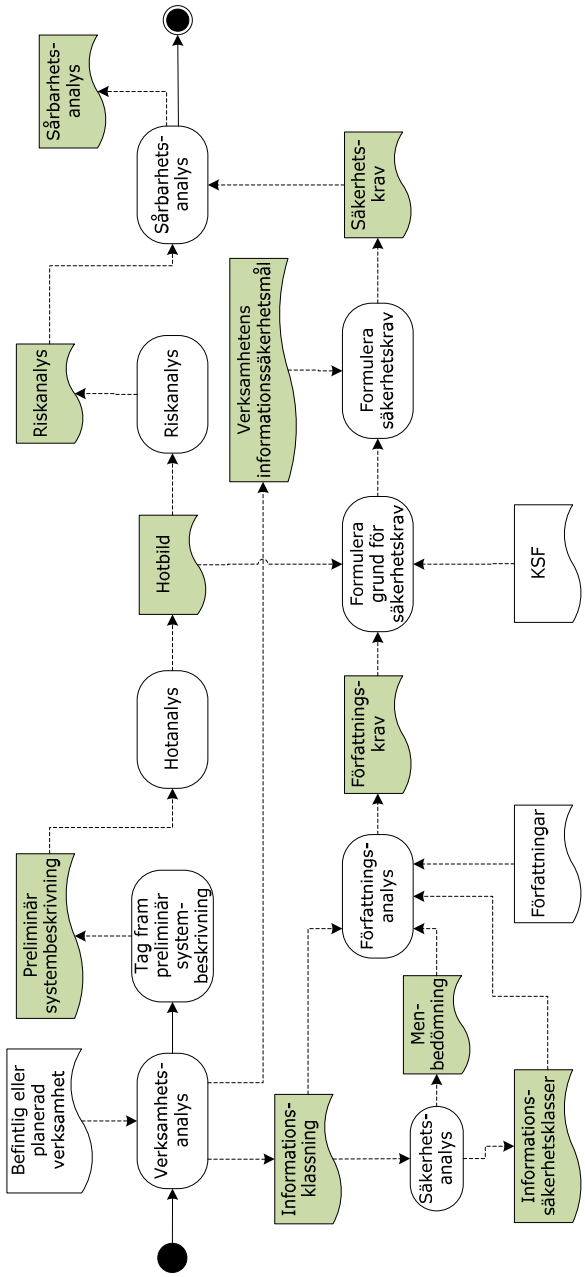
Alla frågeställningarna är numrerade. Därmed kan svar skrivas i separat dokument eller direkt i ett email med referens till aktuell fråga.

1.1 Framtagande av underlag för auktorisationsbeslut B2

Framtagandet av underlag för auktorisationsbeslut B2 (Figur 1) inleds med genomförandet av en verksamhetsanalys. Verksamhetsanalysen syftar till att, genom en övergripande beskrivning, analysera den befintliga eller önskade verksamheten. Verksamhetsanalysen inkluderar även en informationsklassning som bedömer säkerhetsklassen hos den information som skall behandlas. Denna informationsklassning ligger till grund för säkerhetsanalysen vars syfte är att bedöma om några av de uppgifter som det angivna IT-systemet är avsett att behandla, är hemliga.

Produktägaren ansvarar för att en författningsanalys genomförs. Författningsanalysen syftar till att se över vilka lagar, förordningar, föreskrifter och bestämmelser som måste beaktas för det aktuella IT-systemet. Resultatet av analysen är en uppsättning författningskrav.

För att avgöra vad som kan påverka en myndighets säkerhetskritiska verksamhet genomförs hot-, risk- och sårbarhetsanalyser. Dessa analyser skall egentligen genomföras som tre separata analyser, men för många IT-system så är detta samlat till en gemensam analys. Först genomförs hotanalysen, vilken har för avsikt att identifiera de hot IT-systemet exponeras för. Hotanalysen resulterar i en hotbild. Vidare genomförs riskanalysen för att identifiera de befintliga riskerna med avseende på den framtagna hotbilden. För att kunna genomföra en sårbarhetsanalys måste säkerhetskrav tas fram, varvid nästa aktivitet i processen är att formulera en grund för säkerhetskrav.



Figur 1: Framtagande av underlag för auktorisationsbeslut B2.

Utifrån de tidigare framtagna författningskraven, Försvarsmaktens krav på godkända säkerhetsfunktioner (KSF) samt den aktuella hotbilden formuleras grund för säkerhetskrav. Denna grund används tillsammans med verksamhetens informationssäkerhetsmål för att formulera de säkerhetskrav som ställs på det framtagna IT-systemet.

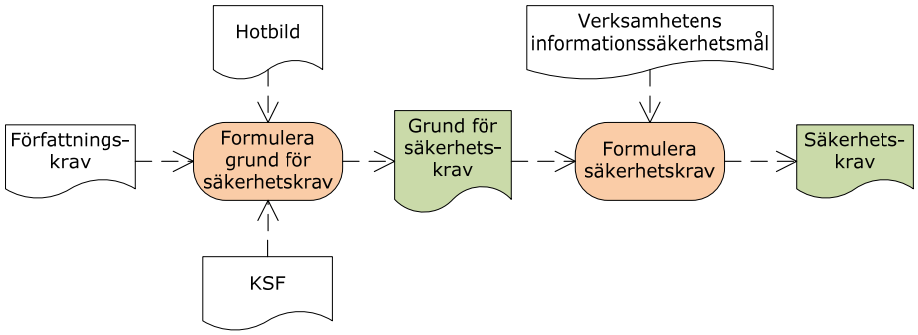
Den avslutande aktiviteten är sårbarhetsanalysen, som vidare beskrivs i avsnitt 3.

Fråga 1: Stämmer den övergripande beskrivningen av processen för framtagande av underlag för auktorisationsbeslut B2 som återges i Figur 1 med verkligheten?

2 Säkerhetskrav

2.1 Beskrivning

Utgående ifrån de identifierade författningskraven, den aktuella hotbilden, samt Försvarsmaktens krav på godkända säkerhetsfunktioner (KSF) formuleras en grund för säkerhetskrav. Denna grund för säkerhetskrav används sedan tillsammans med verksamhetens informationssäkerhetsmål för att formulera de säkerhetskrav som ställs på det framtagna IT-systemet. En illustration av processen för att formulera säkerhetskrav återfinns i Figur 2.



Figur 2: Aktiviteter och artefakter som ingår i framtagandet av säkerhetskrav.

2.2 Frågeställningar

För att förbättra och fördjupa beskrivningen av processen för framtagande av säkerhetskrav behöver följande frågor besvaras. En del av frågorna är nya, medan andra är hämtade ifrån rapporten Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete [5]. För att förtydliga vissa frågor redovisas

en kontext till dessa. Referenser till källorna som listas i slutet av detta dokument ges inom hakparenteser.

2.2.1 Frågeställningar avseende formulering av grund för säkerhetskrav

Fråga 2: I vilken omfattning påverkar hotbild och författningskrav för aktuellt IT-system i realiteten formuleringen av grund för säkerhetskrav?

Enligt H SÄK IT (avsnitt 23.4) gäller att ”De av C MUST beslutade kraven på godkända säkerhetsfunktioner […] är formulerade utifrån en generell hotbild […] och skall användas för att uppnå en godtagbar IT-säkerhet.” Enligt H SÄK IT (avsnitt 16.5.3) gäller att ”Syftet med KSF är således att säkerställa en miniminivå vad avser IT-säkerhet för IT-system som används inom Försvarsmakten. Miniminivån styrs av aktuellt systems informationssäkerhetsklass. […] Respektive produktägare har därefter frihet att beroende på t ex aktuell hot-, risk- och sårbarhetsanalys skärpa i KSF angivna krav.” Enligt H SÄK IT (avsnitt 16.2) gäller att ”Beroende på de miljöer som IT-system verkar i kan hotbilden variera mellan IT-system, vilket i sin tur kan medföra mer eller mindre omfattande krav på säkerhetsfunktioner. Detta är en viktig aspekt som måste tas i beaktande vid framtagande av säkerhetsmekanismer.” [5] (avsnitt 3.2.10)

Fråga 3: Hur visas att uppfyllelse av KSF leder till system med ”godtagbar IT-säkerhet”?

Fråga 4: Hur anpassas KSF för en specifik hotbild?

Fråga 5: Hur avgörs om KSF, anpassad för en specifik hotbild, uppfyller miniminivån för IT-säkerhet inom FM?

Fråga 6: Vilken status har KSFen? D.v.s. utgör de i KSFen specificerade kraven för aktuell informationsklassning:

- en utgångspunkt för att formulera grund för säkerhetskrav,
- hela grund för säkerhetskrav, eller
- direkt de säkerhetskrav som utgör indata till sårbarhetsanalysen?

Enligt DIT (avsnitt 5.5.1) skall IT-säkerhetstjänsten tillhandahålla ”stöd vid säkerhetsgodkännande (ackreditering) av IT-system”. [5] (avsnitt 3.2.6)

Fråga 7: Erbjuder IT-säkerhetstjänsten även stöd vid framtagande av underlag för auktorisationsbeslut B2, och i så fall i vilka former?

2.2.2 Frågeställningar avseende formulering av säkerhetskrav

Fråga 8: Hur påverkas säkerhetskraven av verksamhetens informationssäkerhetsmål?

Avseende framtagande av ackrediteringsunderlag lyfts, bland annat, följande fram i H SÄK IT (avsnitt 23.4) som viktigt att inkludera: säkerhetskrav (mätbara, entydiga och kompletta), krav på avgränsningar mot omgivning (t ex andra IT-system) och säkerhetsfunktioner (med t ex tillhörande risk, tillämplighet, förslag på alternativa åtgärder, icke tillämpade krav samt skyddsnivåer). [5] (avsnitt 3.2.4)

Fråga 9: Hur specificeras säkerhetskrav så att de är mätbara, entydiga och kompletta?

Fråga 10: Hur specificeras krav på avgränsningar mot omgivningen?

Fråga 11: Hur specificeras tillhörande risk, tillämplighet, förslag på alternativa åtgärder, icke tillämpade krav samt skyddsnivåer för säkerhetsfunktioner?

Enligt H SÄK IT (avsnitt 8.7) gäller att ”En viktig del i säkerhetsmålsättningen är redogörelsen för vilka krav på godkända säkerhetsfunktioner som ett IT-system måste uppfylla. Det är även här som eventuella alternativa åtgärder redovisas. Kravställning på säkerhetsmekanismnivå ingår normalt inte i säkerhetsmålsättningsdokumentet.” Enligt H SÄK IT (avsnitt 16.5.3) gäller att ”Eftersom HKV MUST har beslutat vilka krav som ska gälla för de godkända säkerhetsfunktionerna bör HKV MUST rådfrågas innan alternativa åtgärder tas fram. Vidare är det HKV MUST som avgör om en föreslagen alternativ åtgärd ger erforderlig säkerhetsfunktionalitet.” [5] (avsnitt 3.2.10)

Fråga 12: Vilka aktörer ansvarar för, respektive genomför aktiviteten kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen?

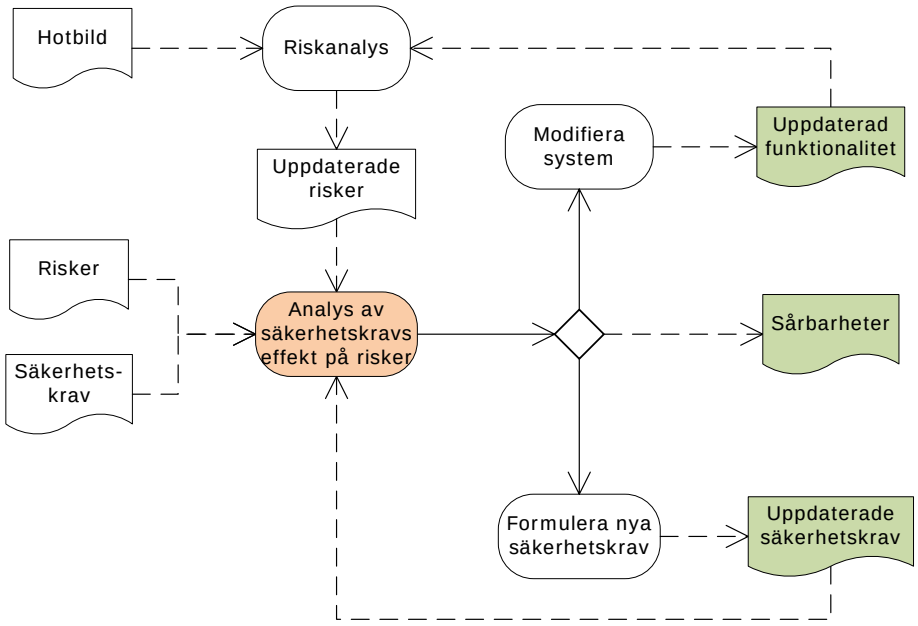
Fråga 13: I vilka fall är det aktuellt att kravställa säkerhetsmekanismer i säkerhetsmålsättningen?

Fråga 14: Vilken är relationen mellan kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen och sårbarhetsanalysen?

3 Sårbarhetsanalys

3.1 Beskrivning

Sårbarhetsanalysen utgår ifrån hotbilden, riskanalysen samt de säkerhetskrav som hittills framtagits under arbetet med underlaget för auktorisationsbeslut B2. De identifierade hoten och riskerna jämförs med säkerhetskraven för att bedöma till vilken grad de, av säkerhetskraven resulterande säkerhetslösningarna, kommer att eliminera eller reducera förekommande riskvärden. Samtliga risker prövas för att slutligen erhålla resulterande riskvärden. De resulterande riskvärdena benämns som förekommande sårbarheter. Om de identifierade sårbarheterna kan riskhanteras är sårbarhetsanalysen slutförd. I annat fall måste antingen säkerhetskraven omformuleras för att bättre kunna reducera de förekommande riskerna, eller IT-systemet modifieras genom att funktionalitet relaterad till de kvarvarande sårbarheterna tas bort. Detta bildar en iterativ process som pågår tills de kvarvarande riskerna är tillräckligt begränsade för att kunna hanteras (Figur 3).



Figur 3: Aktiviteter, artefakter och beslutspunkter som ingår i eller relaterar till processen för sårbarhetsanalys.

3.2 Frågeställningar

För att förbättra och fördjupa beskrivningen av processen för sårbarhetsanalys behöver frågeställningarna i detta avsnitt besvaras. En del av frågorna är nya medan andra är hämtade ifrån rapporten Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete [5]. För att förtydliga vissa frågor redovisas en kontext till dessa. Referenser, till källorna som listas i slutet av detta dokument, ges inom hakparenteser.

3.2.1 Frågeställningar avseende förutsättningar för sårbarhetsanalys

Fråga 15: Var i FMs livscykelmodell befinner sig sårbarhetsanalysen?

Fråga 16: Enligt [6] (s. 8) ingår sårbarhetsanalysen som underlag till B2, men är det endast där?

Enligt [6] (s. 7) avgörs i Auktorisationsbeslut B1 ifall en teknisk produktspecifikation ska ingå i underlaget för B2-B3. Den tekniska produktspecifikationen ska beskriva vilken maskin- och/eller programvara, inklusive versionsnummer, som produkten är uppbyggd av.

Fråga 17: Utgör den tekniska produktspecifikationen underlag för sårbarhetsanalysen?

Fråga 18: Hur beskrivs systemets funktionalitet, som underlag för sårbarhetsanalysen?

Enligt H SÄK IT (avsnitt 8.7) gäller att ”En viktig del i säkerhetsmålsättningen är redogörelsen för vilka krav på godkända säkerhetsfunktioner som ett IT-system måste uppfylla. Det är även här som eventuella alternativa åtgärder redovisas.” [5] (avsnitt 3.2.10)

Fråga 19: Vilken är relationen mellan kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen och sårbarhetsanalysen?

3.2.2 Frågeställningar avseende genomförande av sårbarhetsanalys

Enligt [7] (kap. 5) gäller att ”För hot-, risk- och sårbarhetsanalys rekommenderas FM-Scenario.” [5] (avsnitt 3.2.8)

Fråga 20: Vilka verktyg (dokumentmallar, mjukvara, etc.) används för att genomföra sårbarhetsanalyser?

Fråga 21: Hur stödjer MAACK genomförandet av sårbarhetsanalyser?

Fråga 22: Vilket metodikstöd (specifikationer av arbetsprocesser) tillhandahålls som stöd för genomförandet av sårbarhetsanalyser?

Enligt H SÄK IT (avsnitt 8.1 och 8.6) genomförs, utgående från hot- och riskanalyser, en sårbarhetsanalys där ställda säkerhetskravs förmåga att eliminera risker bedöms. Resultaten kan illustreras översiktligt i figurer där risker markeras baserat på uppskattad sannolikhet och konsekvens och säkerhetskravs förmåga att minska risker illustreras. [5] (avsnitt 3.2.8)

Fråga 23: Hur avgörs säkerhetskravens förmåga att eliminera risker?

Fråga 24: Vilka indata krävs från systemet för genomförandet av sårbarhetsanalysen?

Enligt H SÄK IT (avsnitt 8.1) gäller att ”Eventuellt måste analysen genomlöpas ett antal gånger. För varje ny analysomgång kan det vara nödvändigt att formulera nya säkerhetskrav tills de bedömda resulterande riskvärdena hos sårbarheterna har nått tillräckligt låga och acceptabla nivåer.” [5] (avsnitt 3.2.8)

Fråga 25: Är det vanligt att sårbarhetsanalysen är iterativ?

Fråga 26: Hur avgörs det när ”de bedömda resulterande riskvärdena hos sårbarheterna har nått tillräckligt låga och acceptabla nivåer”?

Många olika aktörer kan vara inblandade i framtagandet av sårbarhetsanalyser. Ur den tillgängliga dokumentationen kan följande aktörer identifieras:

- IT-säkerhetschefen

IT-säkerhetschefens uppgifter kan, bl a, innefatta att ”Stödja genomförandet av analyser som t ex hot-, risk och sårbarhetsanalyser.” (H SÄK IT, avsnitt 7.6.1)

- IT-säkerhetsman

IT-säkerhetsmans uppgifter kan, bl a, innefatta att ”Medverka vid genomförandet av IT-säkerhetsanalyser.” (H SÄK IT, avsnitt 7.6.2)

- IT-säkerhetsansvarig

IT-säkerhetsansvarigs uppgifter kan, bl a, innefatta att ”Stödja genomförandet av analyser som t ex hot-, risk och sårbarhetsanalyser.” (H SÄK IT, avsnitt 7.8)

- Garnisonschef

”Varje garnisonschef eller den han bestämmer skall genomföra och dokumentera hot-, risk- och sårbarhetsanalyser i fråga om ett IT-system som skall användas gemensamt inom garnisonen och utifrån analyserna vidta lämpliga skyddsåtgärder.” (FIB 2006:2, 3 kap. 2 §)

- Användarrepresentanter, chefer och andra berörda

Deltagande analys skall genomföras, med användarrepresentanter, chefer och andra berörda (H SÄK IT, avsnitt 8.6).

Fråga 27: Vilka aktörer genomför i praktiken sårbarhetsanalyser för IT-system?

Enligt H SÄK IT (avsnitt 8.6) gäller att kvarstående risker, vars nivå är för hög för att de skall bedömas som acceptabla, är sårbarheter och anses vara brister i systemet. För att hantera kvarstående risker måste antingen funktionalitet tas bort från systemet eller riskhantering nyttjas. [5] (avsnitt 3.2.9)

Fråga 28: Vilka kriterier ligger till grund för beslut om hur sårbarheter skall behandlas?

Fråga 29: Vad avses med riskhantering?

3.2.3 Frågeställningar avseende sårbarhetsanalysers resultat

Enligt H SÄK IT (avsnitt 8.6) resulterar hot-, risk- och sårbarhetsanalyser i konsekvensanalyser. [5] (avsnitt 3.2.8)

Fråga 30: På vilket sätt erhålls konsekvensanalyser ur sårbarhetsanalyser?

Fråga 31: Hur används resultat från genomförda sårbarhetsanalyser, förutom att de ingår som en del i säkerhetsmålsättningen?

Referenser

[1] Försvarsmakten, Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik Hotbeskrivning (H SÄK IT Hot), 2001.

[2] Försvarsmakten, Direktiv för Försvarsmaktens informationsteknikverksamhet, 2004.

[3] Försvarsmakten, Försvarsmaktens interna bestämmelser om IT-säkerhet, FIB 2006:2, 2006.

[4] Försvarsmakten, MAACK – Metod- & utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten, 2008.

[5] J. Bengtsson and J. Hallberg, Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete, Swedish Defence Research Agency, 2008.

[6] Försvarsmakten, Metodik Ansökan om auktorisation, version 1.8, 2007.

[7] Försvarsmakten, Mall Säkerhetsmålsättning, 2007.

Appendix B – Underlag utskick 2

Vi har fått in en del svar på det tidigare email gällande auktorisationsbeslut B2, som skickades 2008-11-10, men en del frågetecken kvarstår. Vi har kortat listan och återger nedan de kvarvarande frågorna. Precis som förra gången gäller, hellre ett kort och snabbt svar på någon fråga än inget svar alls.

Enligt DIT (avsnitt 5.5.1) skall IT-säkerhetstjänsten tillhandahålla ”stöd vid säkerhetsgodkännande (ackreditering) av IT-system”.

Fråga 1: Erbjuder IT-säkerhetstjänsten även stöd vid framtagande av underlag för auktorisationsbeslut B2, och i så fall i vilka former?

Enligt H SÄK IT (avsnitt 8.7) gäller att ”En viktig del i säkerhetsmålsättningen är redogörelsen för vilka krav på godkända säkerhetsfunktioner som ett IT-system måste uppfylla. Det är även här som eventuella alternativa åtgärder redovisas. Kravställning på säkerhetsmekanismnivå ingår normalt inte i säkerhetsmålsättningsdokumentet.”

Fråga 2: Vilka aktörer ansvarar för, respektive genomför aktiviteten kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen?

Fråga 3: Finns det något typfall (exempel) då det är aktuellt att kravställa säkerhetsmekanismer i säkerhetsmålsättningen?

Enligt dokumentet *Metodik Ansökan om auktorisation*, version 1.8 (s. 7) avgörs i Auktorisationsbeslut B1 ifall en *Preliminär systembeskrivning* ska tas fram.

Fråga 4: Behöver *Preliminär systembeskrivning* tas fram för majoriteten av de system som ska genomgå ackrediteringsprocessen?

Fråga 5: Inför vilket auktorisationsbeslut (B2-B4) ska en eventuell *Preliminär systembeskrivning* tas fram?

Fråga 6: Hur stödjer MAACK genomförandet av sårbarhetsanalyser?

Fråga 7: Vilket metodikstöd (specifikationer av arbetsprocesser) tillhandahålls som stöd för genomförandet av sårbarhetsanalyser?

Enligt H SÄK IT (avsnitt 8.6) gäller att kvarstående risker, vars nivå är för hög för att de skall bedömas som acceptabla, är sårbarheter och anses vara brister i systemet. För att hantera kvarstående risker måste antingen funktionalitet tas bort från systemet eller riskhantering nyttjas.

Fråga 8: Vilka kriterier ligger till grund för beslut om hur sårbarheter (kvarvarande risker) ska behandlas, dvs. om funktionalitet ska tas bort, kraven ska uppdateras eller sårbarheterna ska riskhanteras?

Fråga 9: Sårbarheter är risker vars nivåer är för höga för att kunna accepteras. Vad innebär det, i realiteten, att sårbarheter riskhanteras (dvs. vad gör man)?

Fråga 10: Hur används resultat från genomförda sårbarhetsanalyser, förutom att de ingår som en del i säkerhetsmålsättningen?