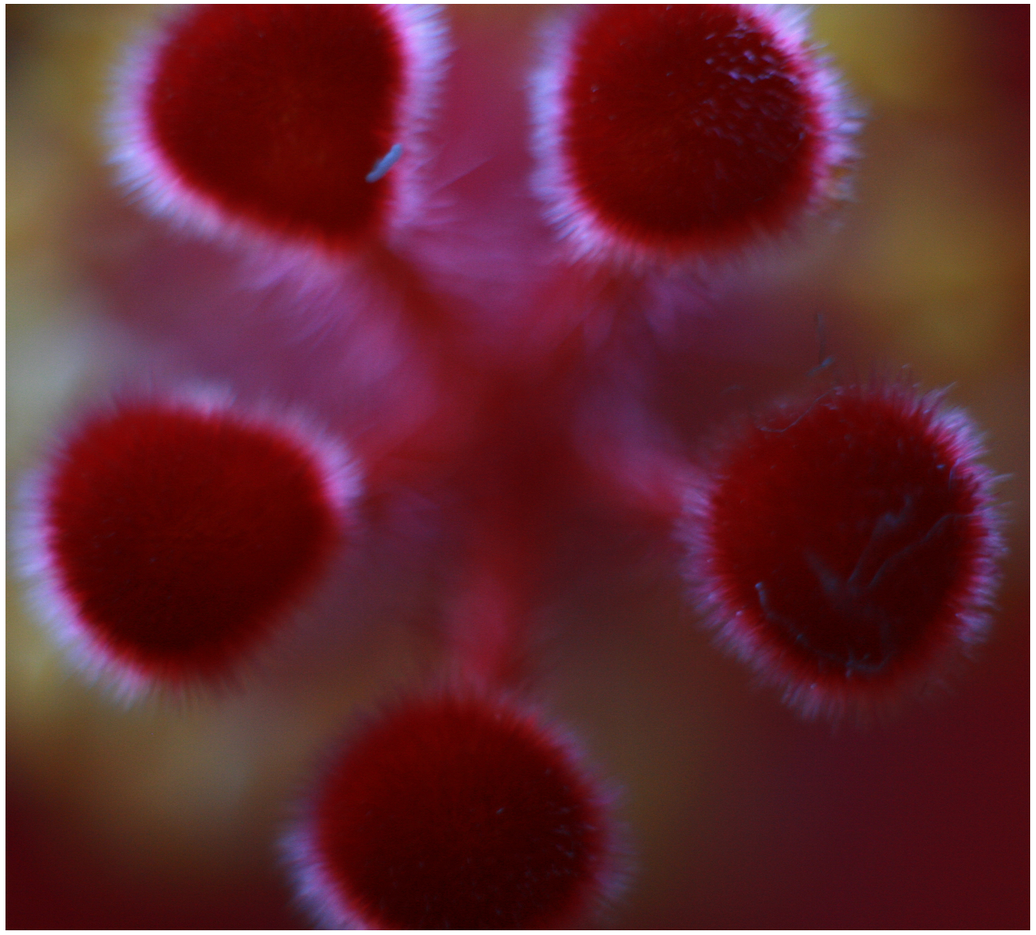
Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete

JOHAN BENGTSSON, JONAS HALLBERG



FOI
Totalförsvarets forskningsinstitut
Ledningssystem
Box 1165
581 11 Linköping

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

www.foi.se

FOI-R--2531--SE Underlagsrapport **Ledningssystem**
ISSN 1650-1942 Juni 2008

Johan Bengtsson, Jonas Hallberg

Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete

Titel	Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete
Title	Assessment aspects within the Swedish Armed Forces regarding IT security
Rapportnr/Report no	FOI-R--2531--SE
Rapporttyp Report Type	Underlagsrapport Base data report
Sidor/Pages	51 p
Månad/Month	Juni/June
Utgivningsår/Year	2008
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten
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	

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

FOI , Swedish Defence Research Agency
Command and Control Systems
SE-581 11 Linköping

Sammanfattning

Informationssäkerhet är verksamhetskritiskt för Försvarsmakten, varför de IT-system som stödjer verksamheten måste ha adekvat IT-säkerhetsnivå. Därmed är Försvarsmaktens arbete med ackrediteringsprocessen av stor betydelse. Som en konsekvens av detta är det av stor vikt att kunna sätta värden på vilken IT-säkerhet olika IT-system har. Om effekterna av olika lösningar, såväl organisatoriska och användarinriktade som tekniska, är kända blir det tydligare hur eventuella brister kan hanteras. Därmed ökar möjligheterna att nyttja IT för att effektivisera verksamheten.

I denna rapport presenteras underlag vars syfte är att skapa förståelse för hur IT-säkerhet i dagsläget värderas inom Försvarsmakten. Baserat på detta underlag kan Totalförsvarets forskningsinstitut (FOI) inrikta sitt arbete med utveckling av metoder för värdering av IT-säkerhet så att största möjliga stöd kan ges till Försvarsmaktens IT-säkerhetsarbete.

I denna rapport presenteras 49 värderingsaspekter med 150 tillhörande frågeställningar. Utgående från de centrala värderingsaspekterna inom området ackreditering beskrivs tre processer rörande ackrediteringsbeslut, framtagande av ackrediteringsunderlag samt sårbarhetsanalys. I vidare arbete behöver frågeställningarna tillhörande värderingsaspekterna beaktas för att erhålla bra underlag för testning av metoder för värdering av IT-säkerhet samt inriktning av FOIs utveckling av metoder och verktyg för IT-säkerhetsvärdering.

Nyckelord: IT-säkerhet, Ackreditering, Värdering

Innehåll

Figurer

1 Inledning

Informationssäkerhet är verksamhetskritiskt för Försvarsmakten. Detta kan uttryckas som att ”Ett IT-system som skall kunna användas som ett stöd i verksamheten måste åtnjuta ett tillräckligt skydd.” (Försvarsmakten, 2006b). Väsentligt för en effektiv informationshantering är att informationssäkerhet är adekvat, inte bara tillräcklig. Detta genomsyrar Försvarsmaktens arbete med ackrediteringsprocessen (Försvarsmakten, 2004; Försvarsmakten, 2006b). Följaktligen är det av stor vikt att kunna sätta värden på vilken IT-säkerhet olika IT-system har och hur det påverkar organisationens informationssäkerhet. Om effekterna av olika lösningar, såväl organisatoriska och användarinriktade som tekniska, är kända blir det tydligare hur eventuella brister kan hanteras. Därmed ökar möjligheterna att nyttja IT för att effektivisera verksamheten.

1.1 Syfte

I denna rapport presenteras underlag vars syfte är att skapa förståelse för hur IT-säkerhet i dagsläget värderas inom Försvarsmakten. Baserat på detta underlag kan Totalförsvarets forskningsinstitut (FOI) inrikta sitt arbete med utveckling av metoder för värdering av IT-säkerhet så att största möjliga stöd kan ges till Försvarsmaktens IT-säkerhetsarbete.

1.2 Metod

För att ta fram ett underlag som kan skapa förståelse för hur frågor som relaterar till värdering av IT-säkerhet i dagsläget hanteras inom Försvarsmakten har följande metod nyttjats.

- Utsagor som relaterar till värdering samlas in från Försvarsmaktsdokument samt i dialog med representanter från Försvarsmakten och andra organisationer som arbetar för Försvarsmakten.
- Insamlade utsagor grupperas för att identifiera värderingsaspekter. Värderingsaspekter baseras på aktiviteter, beslut eller resultat som indikerar behov av att värdera IT-säkerhet.
- Till de identifierade värderingsaspekterna kopplas frågeställningar som behöver klargöras i dialog med Försvarsmakten för att metoder för att hantera värderingsaspekterna skall kunna specificeras.
- Processer som inkluderar några av de centrala värderingsaspekterna specificeras översiktligt.

Baserat på den specificerade metoden har bland annat ett antal utsagor relaterade till genomförandet av sårbarhetsanalyser identifierats i H SÄK IT (Försvarsmakten, 2006b). När dessa utsagor grupperats framstod de beslut som måste fattas baserat på sårbarhetsanalysen som en värderingsaspekt eftersom det krävs värdering av IT-säkerhet för att kunna avgöra, till exempel, hur begränsade de sårbarheter som återstår är med hänsyn till de säkerhetskrav som påförts systemet. Värderingsaspekten leder till flera frågeställningar, till exempel ”Hur avgörs säkerhetskravens förmåga att eliminera risker?” (avsnitt 3.2.8). Utgående från den information som finns i de samlade utsagorna har processen för sårbarhetsanalys formulerats översiktlig (avsnitt 4.3).

1.3 Bidrag

Arbetet som presenteras i denna rapport har resulterat i 49 värderingsaspekter med 150 tillhörande frågeställningar. Utgående från de centrala värderingsaspekterna inom området ackreditering beskrivs tre processer rörande ackrediteringsbeslut, framtagande av ackrediteringsunderlag samt sårbarhetsanalys.

Underlaget som presenteras i denna rapport kan tjäna som underlag för vidare kartläggning av praxis för värdering av informationssäkerhet inom Försvarsmakten. Därmed fyller rapporten sitt syfte och kan utgöra en bas för FOIs vidare arbete med metoder för värdering av informationssäkerhet.

2 Bakgrund

I detta kapitel redogörs kortfattat för begreppen informations- och IT-säkerhet samt området värdering av informations- och IT-säkerhet.

2.1 Informations- och IT-säkerhet

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.

Termen **informationssystem** avser system som samlar in, bearbetar, lagrar och distribuerar information. Innebörden är allmän, men oftast, liksom i denna rapport, avses datorstödda informationssystem[1]. För att undvika otydligheter avseende vad informationssystem faktiskt inkluderar kan termen IT-system nyttjas.

Med **IT-system** avses system med teknik som hanterar och utbyter information med omgivningen (Försvarsmakten, 2006b; Försvarsmakten, 2004). 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.

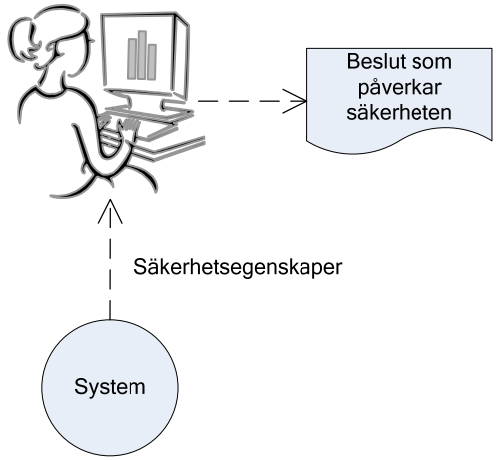
I denna rapport används delvis det mer generella begreppet säkerhet istället för IT-säkerhet. Det skall dock, om inte annat anges, inte tolkas i vidare mening än IT-säkerhet.

2.2 Värdering av IT-säkerhet

Värdering av IT-säkerhet syftar till att öka kunskapen om kvaliteter avseende IT-säkerhet hos system, detta genom att fastställa nivåer för relevanta säkerhetsegenskaper. Värdering har inget självändamål. Därför skall all värdering av säkerhet motsvara behov av kunskap. En typisk situation illustreras i Figur 1, där en beslutsfattare behöver underlag för att kunna fatta ett välinformerat beslut. Detta kan avse till exempel:

- vilken policy för val av lösenord som skall gälla för ett specifikt system,
- vilka säkerhetskrav som skall formuleras för ett system,
- vilka säkerhetslösningar som skall nyttjas för att möta specificerade säkerhetskrav, eller
- vilka säkerhetslösningar som skall utvecklas för att tillse att framtida system kommer att kunna erhålla adekvata säkerhetsnivåer.

[1] Nationalencyclopedin. Artikel om informationssystem. www.ne.se. Besökt 2008-06-10.

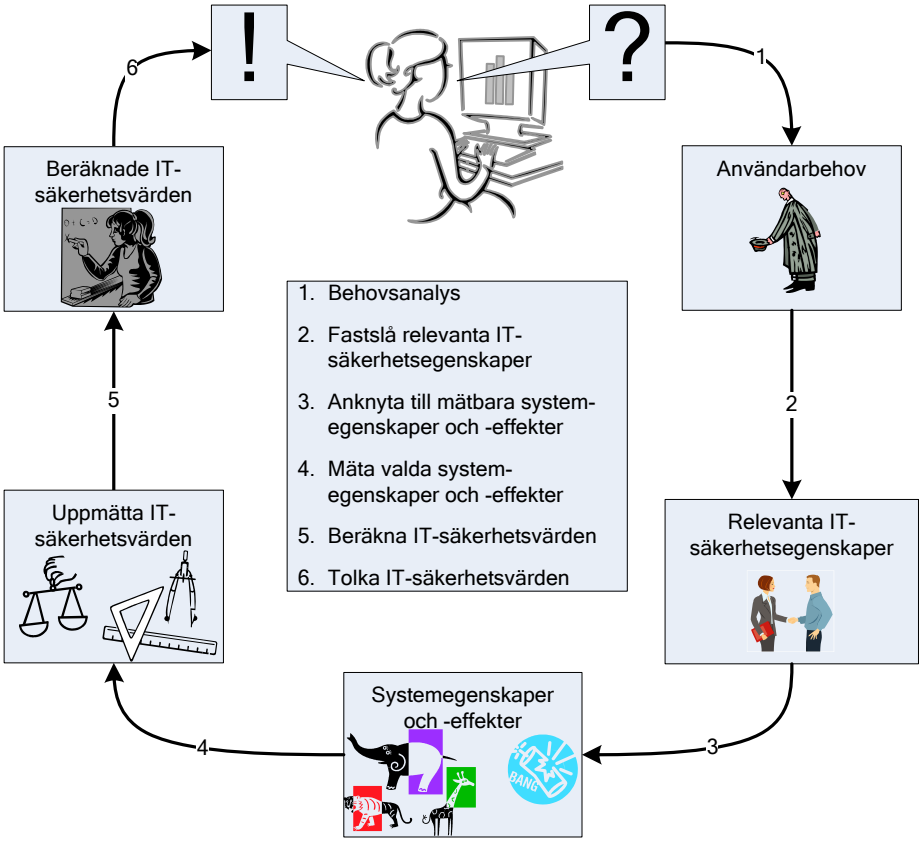


Figur 1: Beslut som påverkar säkerheten i system fordrar värdering av säkerheten för att vara välgrundade.

I samband med värdering relateras ibland till systemegenskaper, vilka karaktäriserar system. Säkerhetsrelevanta systemegenskaper kan användas för att beskriva säkerheten hos system. Systemeffekter utgörs av skeenden som orsakas av system. Systemeffekter, som beror på säkerheten hos system, kan användas för att beskriva denna säkerhet hos systemen. För att beskrivningar av systems säkerhet utgående från systemeffekter skall bli ändamålsenliga behöver systemeffekterna knytas till säkerhetsrelevanta systemegenskaper. Till exempel kan antalet otillbörliga åtkomster till dokument utgöra ett mått på förmågan att reglera åtkomsten till system. Då är den otillbörliga åtkomsten en systemeffekt och förmågan att reglera åtkomsten till system en säkerhetsegenskap.

2.2.1 Processmodell för IT-säkerhetsvärdering

Med syfte att klargöra vilka deluppgifter som måste lösas vid värdering av IT-säkerhet har en processmodell för IT-säkerhetsvärdering tagits fram (Hallberg et al., 2007). Processmodellen består av sex aktiviteter (Figur 2).



Figur 2: Processmodell för IT-säkerhetsvärdering (Hallberg et al., 2007).

Värderingsprocesser skall inte formuleras utifrån vilka metoder och verktyg som finns att tillgå. Värderingsprocesser måste istället utgå ifrån vilka behov som de aktuella intressenterna (beslutsfattare, systemanvändare, etc.) har. Behoven formuleras utifrån att det finns en brist på kunskap om systems IT-säkerhet.

För att uppfylla de fastslagna behoven och göra det möjligt att beskriva systemets IT-säkerhetsnivå på ett för intressenterna meningsfullt sätt, måste relevanta IT-säkerhetsegenskaper formuleras. Detta är väsentligt eftersom IT-säkerhet är ett vittomfattande och abstrakt område och att värdera IT-säkerhet i generell bemärkelse därmed endast kan ge intetsägande resultat. De relevanta IT-säkerhetsegenskaperna måste därmed vara konkreta och anpassade till behoven hos dem som skall nyttja resultaten. Värderingen av de relevanta IT-säkerhetsegenskaperna skall besvara de frågor som intressenterna har.

Ofta är inte de IT-säkerhetsegenskaper som bedömts som relevanta möjliga att mäta direkt, istället måste deras värdering baseras på andra systemegenskaper och -effekter som är mätbara. Följaktligen krävs sammanställningar av säkerhetsvärden som motsvarar olika systemegenskaper och -effekter. Formuleringar av hur sådana sammanställningar skall gå till väga resulterar i så kallade beräkningsmodeller.

Hur själva mätningarna skall gå till beror på vilka egenskaper och -effekter som adresseras. Baseras värderingen på analys av systemets inre, ger detta ett markant annorlunda mätförfarande än vad en värdering baserad på analys av in- och utsignaler till och från systemet ger.

När nödvändiga mätvärden har tagits fram skall dessa sammanställas till säkerhetsvärden för de relevanta IT-säkerhetsegenskaperna. Beroende på beräkningsmodellen kan beräkningarna vara så pass rättframma att de kan utföras manuellt alternativt kräva

speciellt stöd för beräkningar eller simuleringar. Sammanställning av värden innebär en minskning av mängden data, vilket kan leda till förlust av relevant information. Då säkerhet är komplext, abstrakt och beroende av många systemegenskaper och -effekter, är det väsentligt att kunna sammanställa data så att väsentliga parametrar framträder tydligt medan andra parametrar undertrycks.

För att uppmätta och beräknade säkerhetsvärden skall innebära något måste dessa tolkas. Detta leder till värderingsprocessens slutresultat i form av värderade relevanta säkerhetsegenskaper. Tolkningen avser de relevanta säkerhetsegenskaperna i den kontext det studerade systemet utgör, vilket innebär att tolkningen av ett och samma säkerhetsvärde kan vara olika för olika system.

3 Värderingsaspekter

I detta kapitel beskrivs ett antal värderingsaspekter. Värderingsaspekter lyfter fram delar av sammanhang, det vill säga aspekter, som indikerar behov av att värdera IT-säkerheten i 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 IT-säkerhetsnivåer i system, eller delar av system. Resultat, ur vilka värderingsaspekter kan härledas, innehåller element av IT-säkerhetsvärderingar.

Syftet med kapitlet är att beskriva värderingsaspekterna utifrån deras sammanhang, det vill säga

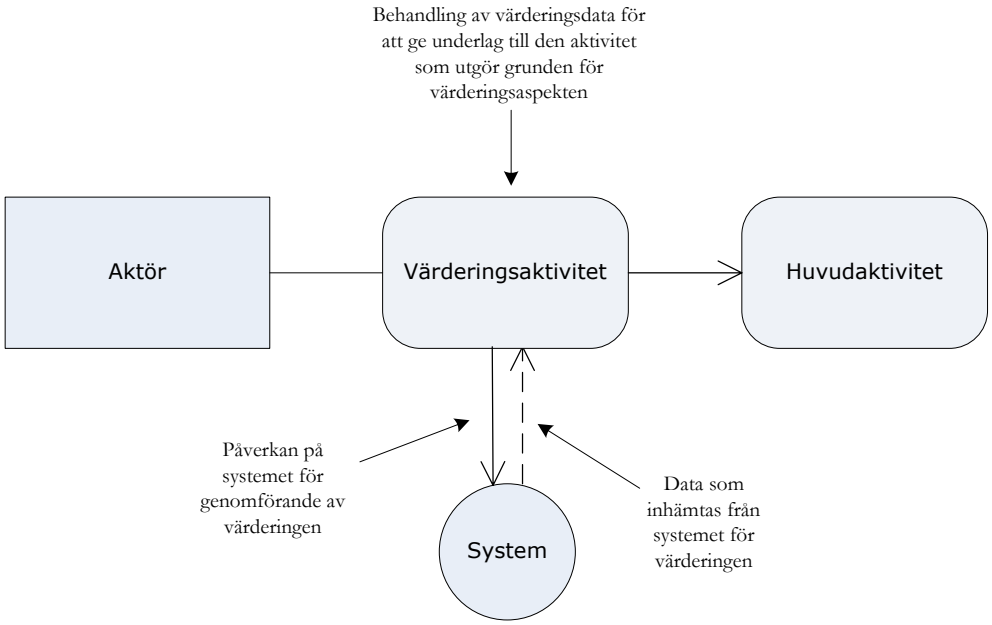
- vilka aktörer som skall genomföra aktuella aktiviteter,
- vilka aktiviteter det är som innehåller värdering,
- vilka beslut som explicit skall fattas baserat på genomförda värderingar och
- vilka resultat som skall levereras.

Detekterade värderingsaspekter och deras kontext illustreras i figurer enligt de alternativa formaten i Figur 3, Figur 4 och Figur 5.

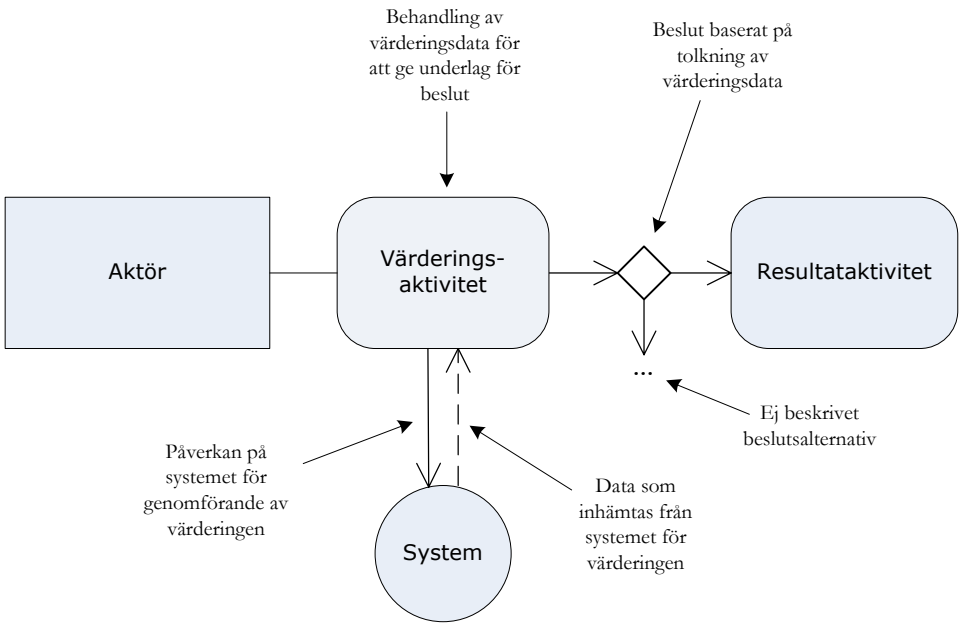
Formatet i Figur 3 används då underlaget från värderingen utgör indata till den aktivitet som utgör grunden för värderingsaspekten, dvs. för aktivitetsbaserade värderingsaspekter. Ett exempel på detta är genomförande av sårbarhetsanalys, vilket bland annat kräver underlag i form av IT-säkerhetsvärderingar.

Formatet i Figur 4 används då beslut explicit skall fattas baserat på värderingen, dvs. för beslutsbaserade värderingsaspekter. Ett exempel på detta är att användningen av system där erforderligt skydd inte kan uppnås skall begränsas. Därmed finns behov av att bedöma skyddsnivå. Baserat på denna värdering skall beslut om begränsning av användning fattas.

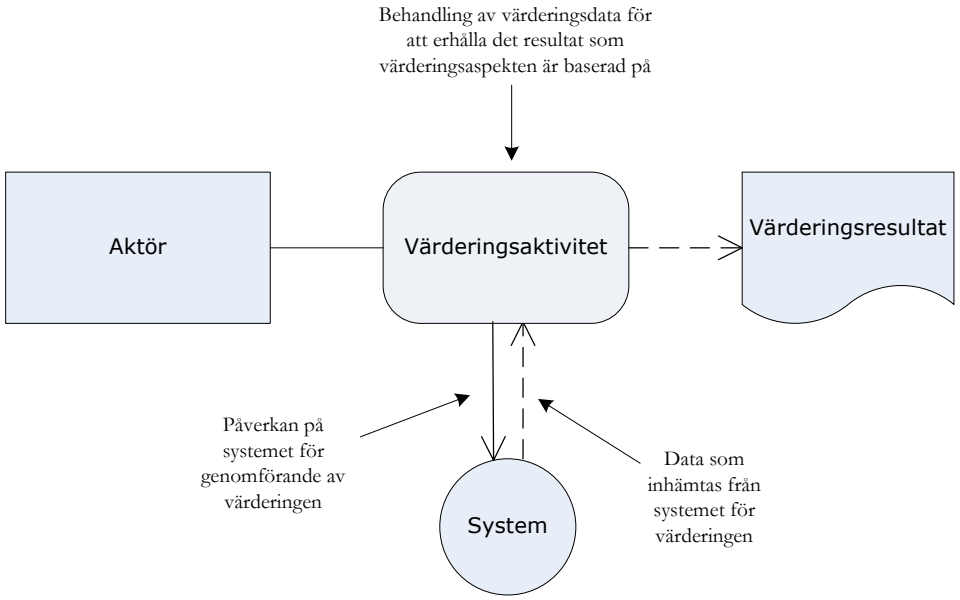
Formatet i Figur 5 används då underlaget från värderingen utgör slutresultat, dvs. för resultatbaserade värderingsaspekter. Ett exempel på detta är skapandet av lägesbilder över IT-säkerheten i system.



Figur 3: Format för figurer vilka illustrerar aktivitetsbaserade värderingsaspekter, där underlaget från värderingen utgör indata till en annan aktivitet.



Figur 4: Format för figurer vilka illustrerar beslutsbaserade värderingsaspekter, där beslut baserade på värderingsresultatet explicit ingår.



Figur 5: Format för figurer vilka illustrerar resultatbaserade värderingsaspekter, där underlaget från värderingen utgör slutresultat.

Värderingsaspekterna har strukturerats i de övergripande kategorierna utveckling, ackreditering och drift. Kopplat till värderingsaspekterna finns ett antal frågeställningar. Genom vidare arbete som ger svar till dessa frågeställningar kan mer detaljerade beskrivningar av värderingsaspekterna tas fram.

Värderingsaspekterna har hämtats från följande dokument:

- Direktiv för Försvarsmaktens informationsteknikverksamhet, DIT, (Försvarsmakten, 2004)
- Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik, H SÄK IT, (Försvarsmakten, 2006b)
- Försvarsmaktens interna bestämmelser, FIB 2006:2, (Försvarsmakten, 2006a)
- Mall Spårbarhet, krav-säkerhetsmål (Försvarsmakten, 2006c)
- Mall Säkerhetsmålsättning (Försvarsmakten, 2007)

För att öka läsbarheten refereras dessa dokument med kortformen av deras namn, istället för med korrekt hänvisning till referenslistan. I nästa kapitel beskrivs processer med aktiviteter avseende IT-säkerhetsvärdering utgående från de värderingsaspekter som identifieras i detta kapitel.

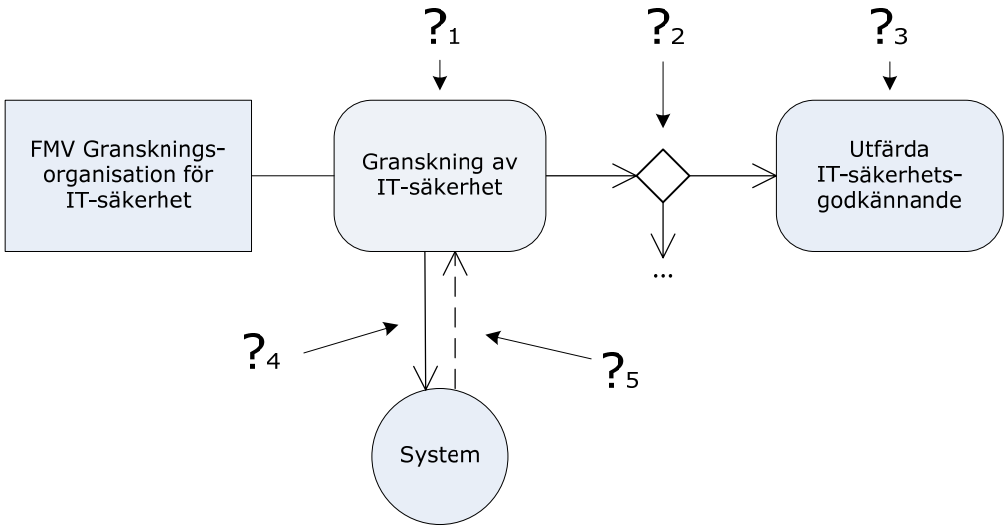
3.1 Utveckling

I denna kategori ingår värderingsaspekter som är kopplade till utvecklingen av system.

3.1.1 Beslut om IT-säkerhetsgodkännande

I DIT (kapitel 1) anges att Försvarets materielverk (FMV) skall ”bygga upp en av materielsystemen oberoende granskningsorganisation för IT-säkerhet”. Syftet är att FMV med sina leveranser skall bifoga ett ”IT-säkerhetsgodkännande” och, enligt DIT (avsnitt 5.1.1), ”utföra huvuddelen av IT-säkerhetsarbetet inom ramen för sina beställningar”.

Detta utgör en beslutsbaserad värderingsaspekt, då beslut om IT-säkerhetsgodkännande måste fattas baserat på granskningen av IT-säkerhet (Figur 6).



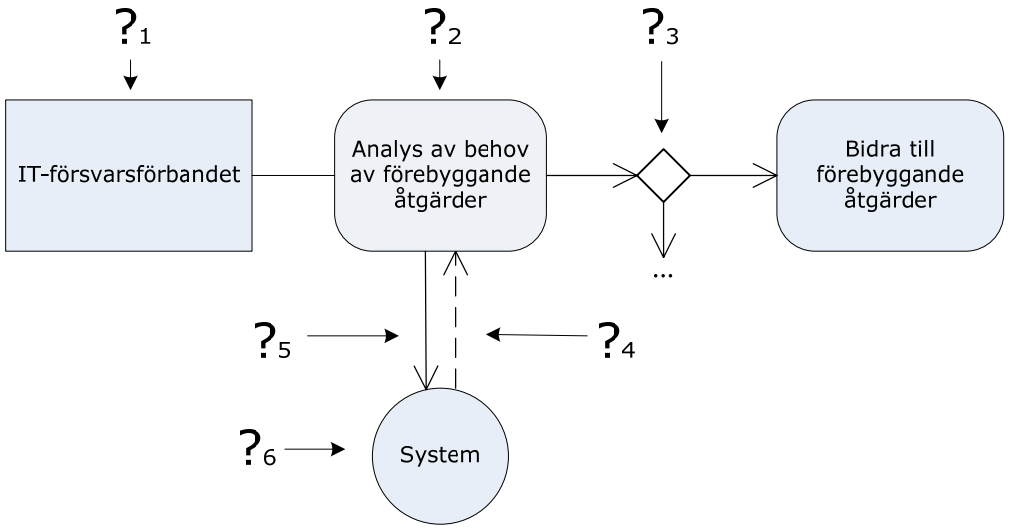
Figur 6: Värderingsaspekten Beslut om IT-säkerhetsgodkännande.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilka arbetsprocesser har utformats för framtagande av underlag för beslut om att utfärda IT-säkerhetsgodkännande?
2. Hur fattas beslut om att utfärda IT-säkerhetsgodkännande?
3. Vad innehåller beslut om IT-säkerhetsgodkännande?
4. Hur påverkas det studerade systemet för att erhålla nödvändiga data?
5. Hur sker återkoppling från det studerade systemet till granskningsorganisationen?

3.1.2 Bidrag till förebyggande åtgärder inom IT-försvarsområdet

Enligt DIT (avsnitt 4.1.10) är ett av syftena med IT-försvarsförbanden att de skall ”bidra till förebyggande åtgärder inom IT-försvarsområdet”. Detta utgör en beslutsbaserad värderingsaspekt, då förebyggande åtgärder kräver beslut om vilka bidrag till förebyggande åtgärder som skall tas fram (Figur 7).



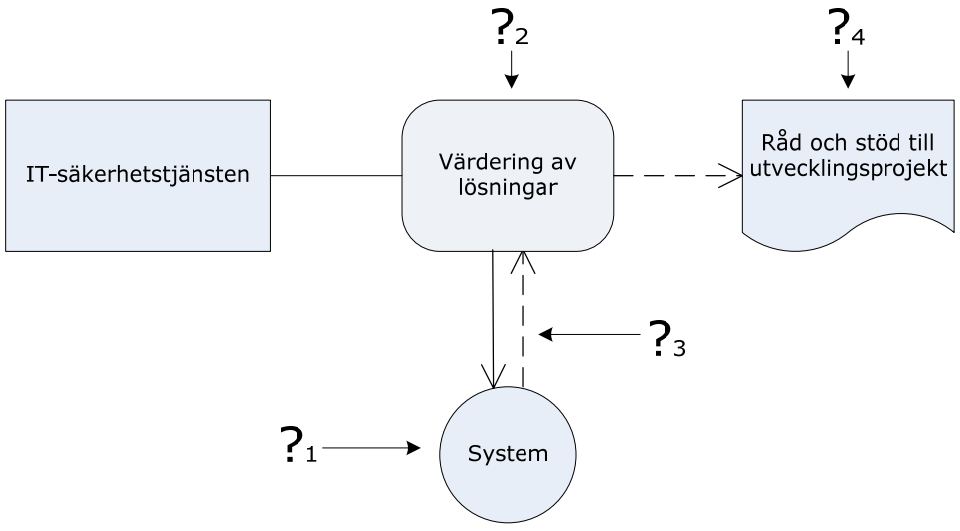
Figur 7: Värderingsaspekten Beslut om vilka bidrag till förebyggande åtgärder inom IT-försvarsområdet som skall tas fram.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Finns det en organisation inom IT-försvarsförbandet för att hantera denna värdering?
2. Vilka arbetsprocesser har utformats för att identifiera behov av att anpassa IT-försvaret?
3. Hur avgörs vilka bidrag till förebyggande åtgärder som skall tas fram?
4. Hur sker återkoppling från det studerade systemet till IT-försvarsförbandet?
5. Hur påverkas det studerade systemet för att erhålla nödvändiga data?
6. Vilka typer av system studeras inom IT-försvarsområdet?

3.1.3 Råd och stöd till utvecklingsprojekt

Enligt DIT (avsnitt 5.5.1) skall IT-säkerhetstjänsten tillhandahålla ”råd och stöd till utvecklingsprojekt vid deras utformning av lösningar”. Om detta gäller IT-säkerhetslösningar, utgör resultatet en resultatbaserad värderingsaspekt vilken kräver värderingar av lösningar (Figur 8).



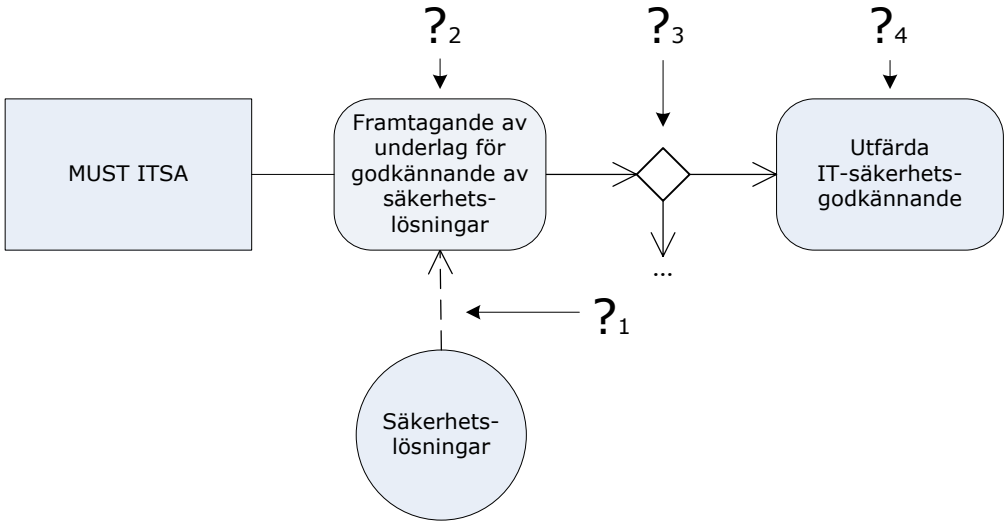
Figur 8: Värderingsaspekten Råd och stöd till utvecklingsprojekt.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Syftar ”lösningar” på IT-säkerhetslösningar i det som utvecklas?
2. Hur värderas vilken säkerhetsnivå som fås med de valda lösningarna?
3. Vilka data behövs från utvecklingsprojektet för att kunna ge råd och stöd?
4. I vilken form erbjuds råd och stöd?

3.1.4 Godkännande av säkerhetslösningar

Enligt DIT (avsnitt 5.5.1) skall MUST ITSA godkänna ”säkerhetslösningar som kan användas av flera projekt och system avseende signalskyddssystem”. Beslut om godkännande av säkerhetslösningar kräver fastställande av vilka säkerhetsnivåer dessa lösningar ger, vilket leder till en beslutsbaserad värderingsaspekt (Figur 9).



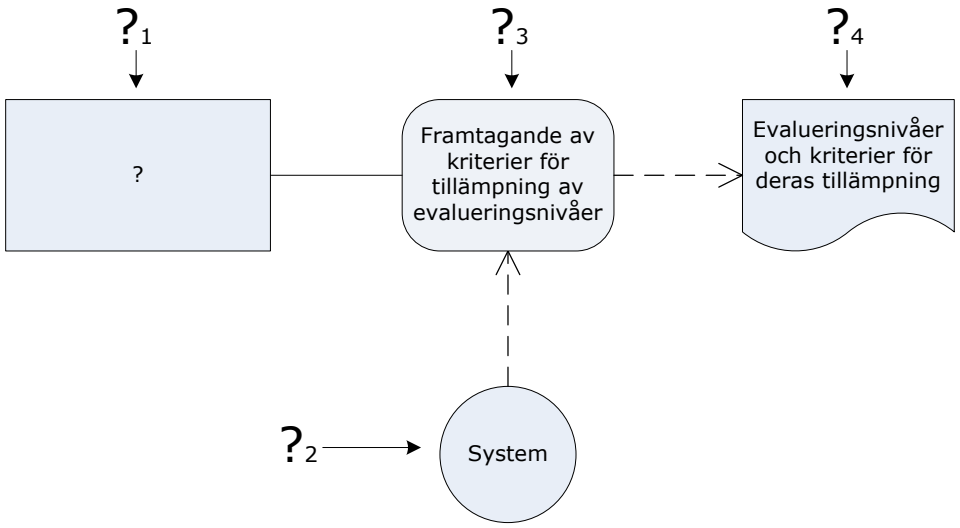
Figur 9: Värderingsaspekten Godkännande av säkerhetslösningar.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilka data samlas in gällande säkerhetslösningarna?
2. Hur avgörs vilken säkerhetsnivå som erhålls med de valda lösningarna?
3. Vad krävs för att en säkerhetslösning skall bli godkänd?
4. Vad innehåller ett IT-säkerhetsgodkännande?

3.1.5 Kriterier för tillämpning av evalueringsnivåer

Enligt DIT (avsnitt 5.5.2) gäller att ”Försvarsmakten skall verka för etablering av en struktur för evaluering och certifiering av informationssäkerhet i IT-system. Eventuella krav på evaluering och certifiering beslutas i förekommande fall genom **Auktorisations beslut**. Kriterier för tillämpning av olika evalueringsnivåer tas fram”. Detta ger upphov till en resultatbaserad värderingsaspekt avseende de kriterier för tillämpning av evalueringsnivåer som skall tas fram (Figur 10).



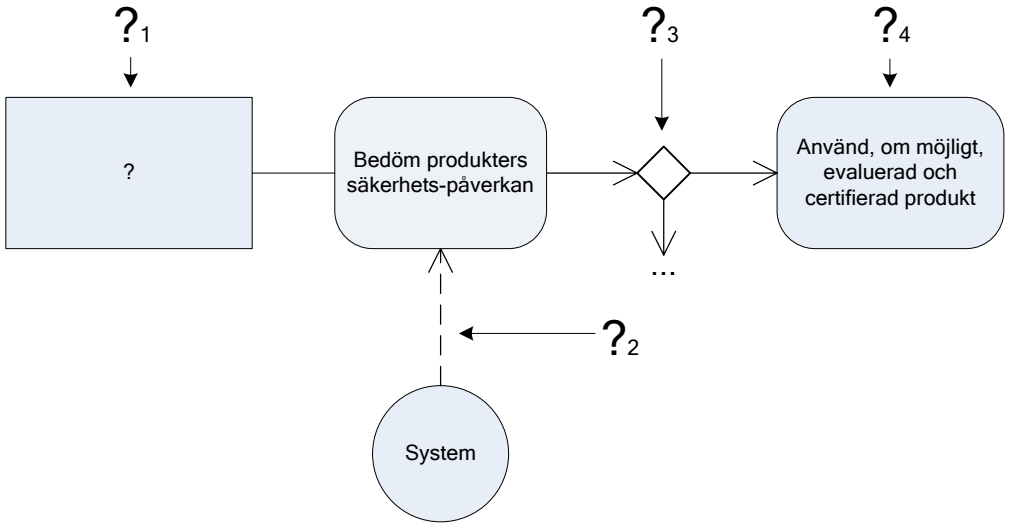
Figur 10: Värderingsaspekten Kriterier för tillämpning av evalueringsnivåer.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vem ansvarar för framtagande av de nämnda kriterierna för tillämpning av evalueringsnivåer?
2. Vilka system, eller typer av system, ligger till grund för utarbetningen av kriterierna?
3. Hur går framtagandet av kriterier för tillämpning av evalueringsnivåer tillväga?
4. Vilka evalueringsnivåer och kriterier för deras tillämpning finns?

3.1.6 Avgöra produkters säkerhetspåverkan

Enligt DIT (avsnitt 5.5.2) skall det gå att avgöra vilka produkter som påverkar säkerheten i Försvarsmaktens system. De produkter som påverkar säkerheten ska, om möjligt, vara evaluerade och certifierade. Detta kräver beslut avseende vilka produkter som påverkar säkerheten i system, vilket utgör en beslutsbaserad värderingsaspekt (Figur 11). I förlängningen är detta ett grundläggande IT-säkerhetsvärderingsproblem: att avgöra vilka faktorer som påverkar säkerhetsnivåer i system .



Figur 11: Värderingsaspekten Avgöra produkters säkerhetspåverkan.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

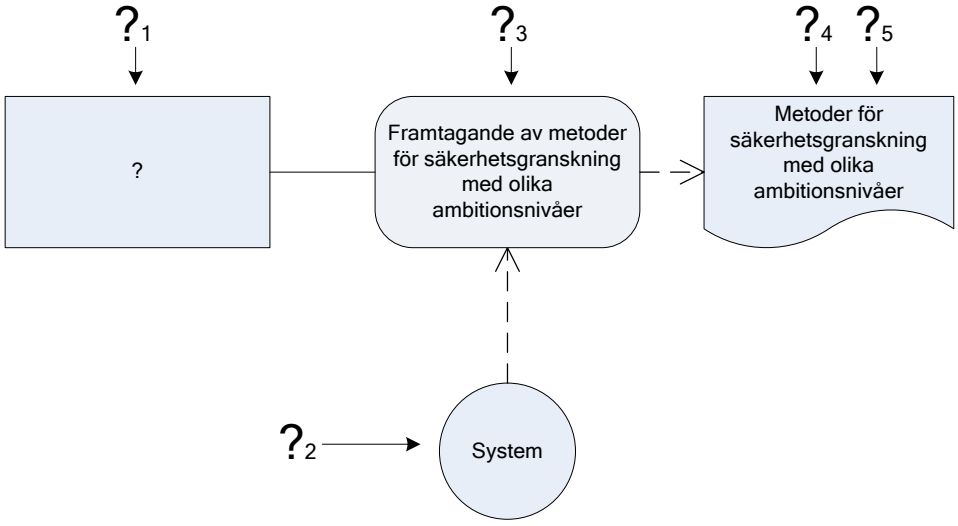
1. Vem skall genomföra de nämnda bedömningarna av produkters säkerhetspåverkan?
2. Vilka data samlas in från system för att kunna avgöra produkters säkerhetspåverkan?
3. Hur avgörs det om en produkt påverkar säkerheten?
4. Vilka kriterier ligger till grund för att avgöra om produkter skall vara evaluerade och certifierade, eller ej?

3.2 Ackreditering

I denna kategori ingår värderingsaspekter som är kopplade till ackreditering av IT-system.

3.2.1 Metoder för säkerhetsgranskning med olika ambitionsnivåer

Enligt DIT (avsnitt 5.5.5) gäller att ”Evaluering och ackreditering av IT-system skall kunna ske med olika ambitionsnivåer. Beslut om ambitionsnivå tas i Auktorisationsbeslut”. Enligt DIT (avsnitt 6.1.2) pågår arbetet med ”Metoder för säkerhetsgranskning enligt olika ambitionsnivåer”. Detta uttrycker såväl behov av som arbete med metoder som kan generera säkerhetsgranskningar med olika ambitionsnivåer, vilket leder till en resultatbaserad värderingsaspekt (Figur 12).



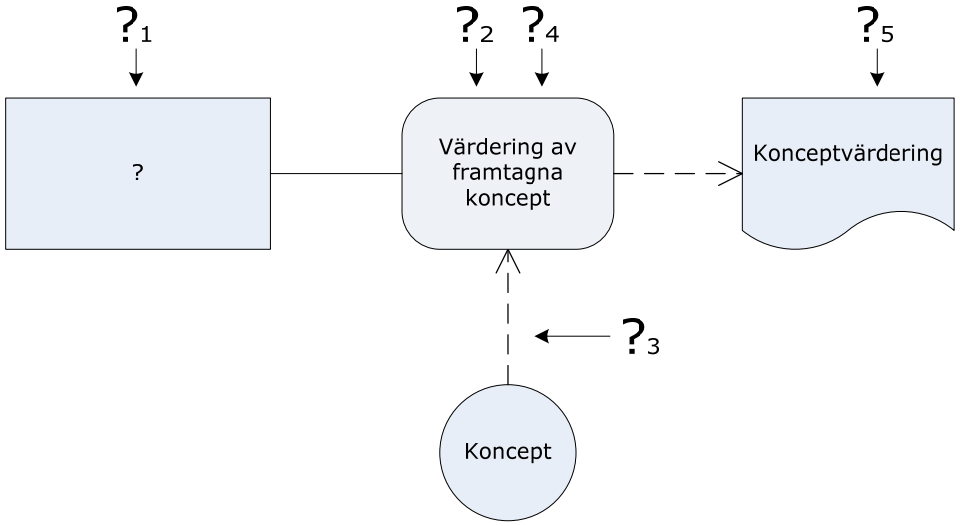
Figur 12: Värderingsaspekten Metoder för säkerhetsgranskning med olika ambitionsnivåer.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vem arbetar med framtagning av nämnda metoder för säkerhetsgranskning med olika ambitionsnivåer?
2. Vilka system, eller typer av system, har legat till grund för utarbetningen av nämnda metoder för säkerhetsgranskning med olika ambitionsnivåer?
3. Hur har framtagningen av metoderna för säkerhetsgranskning gått till väga?
4. Vilka metoder för säkerhetsgranskning har tagits fram?
5. Vilka kriterier finns för tillämpning av de olika ambitionsnivåerna för säkerhetsgranskning?

3.2.2 Konceptvärdering

Enligt avsnitt 6.1.1 (steg P2b) skall framtagna koncept för realisering värderas ”utifrån exempelvis perspektiven personal, organisation, verksamhet, arkitektur, infrastruktur, teknik, underhåll, arvet, ekonomi och industri- och marknadsförutsättningar”. Om värderingen inkluderar säkerhet, utgör detta en resultatbaserad värderingsaspekt (Figur 13).



Figur 13: Värderingsaspekten Konceptvärdering.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vem utför värderingen av koncept?
2. Utifrån vilka olika perspektiv görs vanligen en konceptvärdering?
3. Vilka konceptdata är nödvändiga för värderingen?
4. Hur genomförs värderingen?
5. Vad skall resultatet av värderingen innehålla?

3.2.3 Centralt ackrediteringsbeslut

Det centrala ackrediteringsbeslutet ger upphov till flera värderingsaspekter, vilka lyfts fram i texten nedan samt i Figur 14.

Enligt DIT (avsnitt B.3) gäller att ”Produktägaren beslutar om central ackreditering så att ett balanserat skydd kan erhållas. Som underlag för beslutet skall bland annat MUST yttrande framgå”. Att avgöra att villkoren för att kunna uppnå ”ett balanserat skydd” är uppfyllda utgör en beslutsbaserad värderingsaspekt.

1. Vad avses med ”balanserat skydd”?
2. Hur skapas förutsättningar för ”ett balanserat skydd”?

Enligt H SÄK IT (avsnitt 23.4) gäller att ”I ett centralt ackrediteringsunderlag bör – förutom att auktorisationsbeslut, avtal eller överenskommelser redovisas – produktägaren ange krav på lokala åtgärder (lokal checklista) som systemägaren måste hantera i det lokala ackrediteringsarbetet, eventuellt tillsammans med driftansvariga.” Att avgöra vilka lokala åtgärder som krävs utgör en beslutsbaserad värderingsaspekt.

3. Hur avgörs vilka lokala åtgärder som är nödvändiga?

Enligt H SÄK IT (avsnitt 23.3) gäller att ”När ett IT-system godkänns från säkerhetssynpunkt skall beslutet naturligtvis dokumenteras. Anledningen till detta är bl a att det skall gå att spåra på vilka grunder ett IT-system har godkänts från säkerhetssynpunkt.” Själva ackrediteringsbeslutet är en värderingsaspekt. Vad som utgör grunden för detta beslut är centralt.

4. Hur dokumenteras vad som utgör grunden för ackrediteringsbeslut?

Enligt H SÄK IT (avsnitt 8.1) gäller att ”Säkerhetsmålsättningen används i ackrediteringsarbetet […] genom att granskningen utgår från målsättningen för att kunna bedöma om den framtagna säkerhetslösningen tillgodoser de uppställda förväntningarna. Utifrån detta kan slutsatser dras om säkerheten i och kring IT-systemet är godtagbar, eller inte.” Bedömning av framtagna säkerhetslösningar utgör en beslutsbaserad värderingsaspekt. Indirekt måste även säkerhetsmålsättningen bedömas.

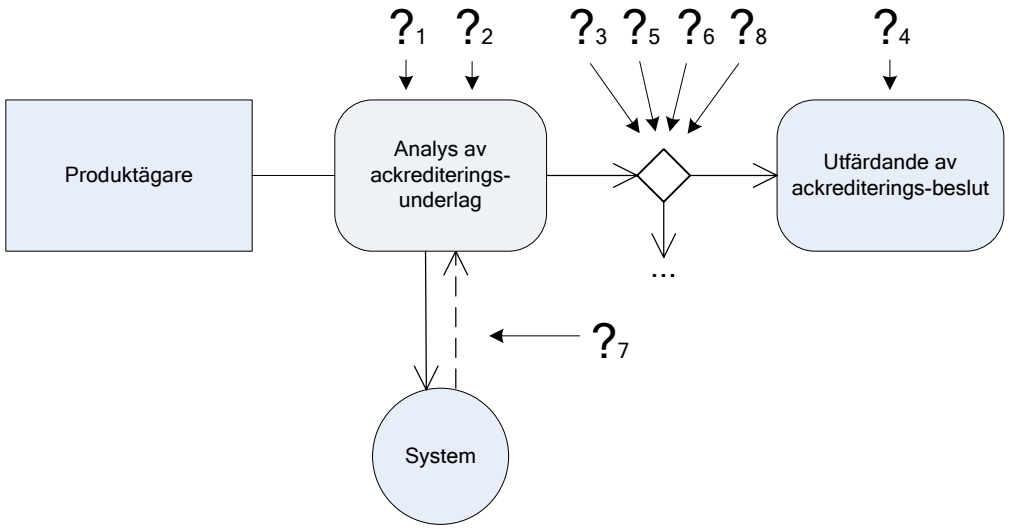
5. Hur avgörs om säkerhetsmålsättningen är tillräcklig för ackreditering av systemet?
6. Hur avgörs om framtagna säkerhetslösningar tillgodoser de uppställda förväntningarna?

Enligt H SÄK IT (avsnitt 23.2) gäller att ”En säkerhetsgranskning i och kring ett IT-system föregår alltid och skall ligga till grund för ett beslut i fråga om ackreditering. Föreskrifternas syfte är att säkerställa att IT-systemet erbjuder ett tillräckligt skydd för de uppgifter som skall kunna behandlas i IT-systemet.” Att säkerställa tillräckligt skydd utgör en beslutsbaserad värderingsaspekt.

7. Vilka egenskaper hos IT-system och deras kontext beaktas för att säkerställa att skyddsnivån är tillräcklig med tanke på de uppgifter som kan komma att hanteras?

Enligt H SÄK IT (avsnitt 23.2) gäller att ”Syftet med en säkerhetsgranskning är att säkerställa att säkerhetsmålsättningen möts av relevanta och tillräckliga säkerhetsmekanismer.” Att avgöra vad som är ”relevanta och tillräckliga säkerhetsmekanismer” utgör en beslutsbaserad värderingsaspekt.

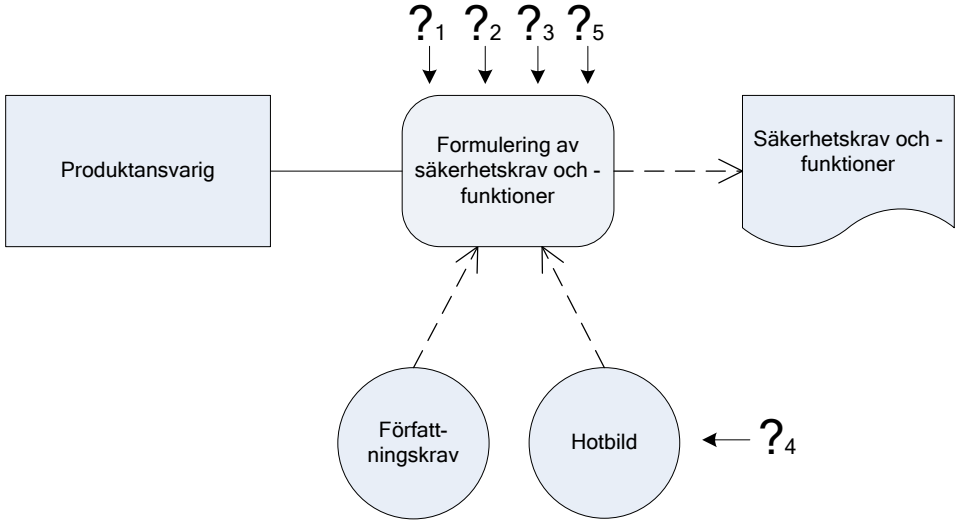
8. Hur avgörs vilka säkerhetsmekanismer som är ”relevanta och tillräckliga”?



Figur 14: Värderingsaspekter relaterade till centrala ackrediteringsbeslut.

3.2.4 Säkerhetskrav och -funktioner

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). Enligt Mall Säkerhetsmålsättning (avsnitt 5) gäller att ”Tillsammans med författningskraven utgör hotbilden grunden för säkerhetsskyddskraven. […] För en mer detaljerad hotbild inkluderat risk- och sårbarhetsanalys kan hänvisas till för verksamheten genomförd hot-, risk- och sårbarhetsanalys”. Vidare gäller enligt Mall Säkerhetsmålsättning (avsnitt 7) att ”Om verksamhetens krav kommer i konflikt med säkerhetsmålen måste man göra en bedömning av vilket som skall ha prioritet: informationssäkerhet eller verksamhet. […] Härleds säkerhetsmålet till Försvarsmaktens handböcker, eller till hot som kommit fram under en hot-, risk- och sårbarhetsanalys görs en avvägning mellan nyttan av verksamhetskravet och hotet mot informationssäkerheten” Krav på adekvat specificering av säkerhetskrav och säkerhetsfunktioner gör detta till en resultatbaserad värderingsaspekt (Figur 15).



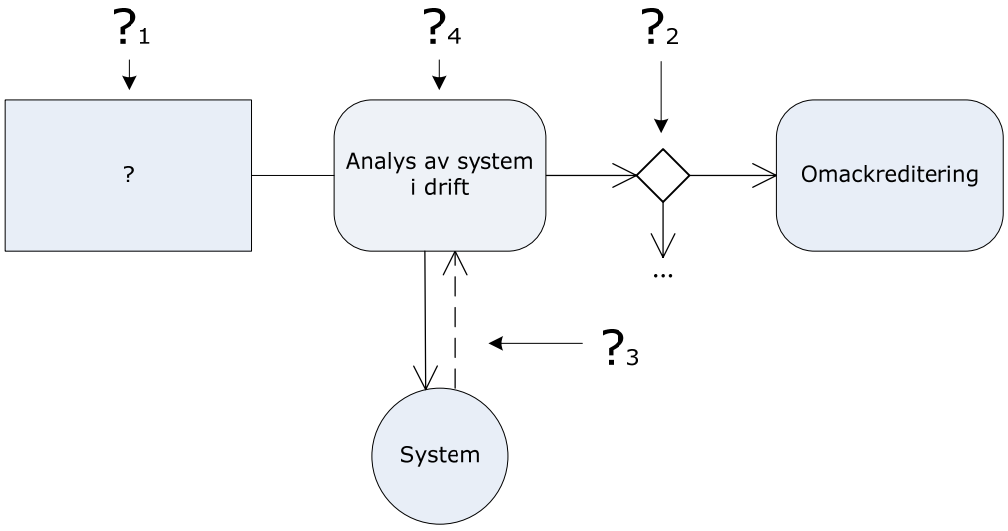
Figur 15: Värderingsaspekten Säkerhetskrav och -funktioner.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Hur specificeras säkerhetskrav så att de är mätbara, entydiga och kompletta?
2. Hur specificeras krav på avgränsningar mot omgivningen?
3. Hur specificeras tillhörande risk, tillämplighet, förslag på alternativa åtgärder, icke tillämpade krav samt skyddsnivåer för säkerhetsfunktioner?
4. Inkluderar begreppet hotbild risk- och sårbarhetsanalys?
5. Hur genomförs avvägningar mellan ”nyttan av verksamhetskravet och hotet mot informationssäkerheten”?

3.2.5 Beslut om omackreditering

Enligt FIB 2006:2 (11 kap. 6 §) gäller att befintliga IT-system skall ackrediteras ”om det sker förändringar i eller kring systemet som kan påverka dess säkerhet.” Detta behov av att kunna besluta om omackreditering ger upphov till en beslutsbaserad värderingsaspekt (Figur 16).



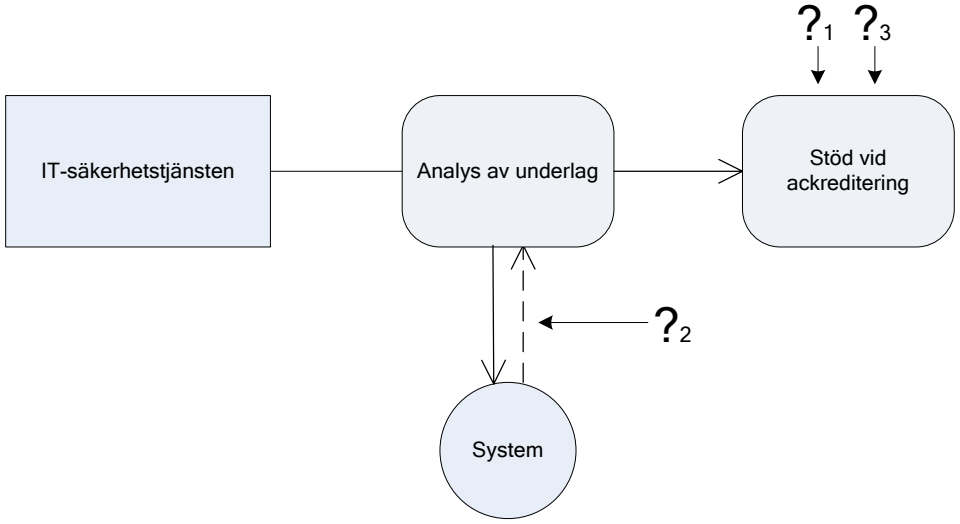
Figur 16: Värderingsaspekten Beslut om omackreditering.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vem tar beslut om omackreditering?
2. Hur avgörs när villkoret ”förändringar i eller kring systemet som kan påverka dess säkerhet” är uppfyllt?
3. Vilka data samlas in från systemet för att kunna bedöma ifall omackreditering skall ske?
4. Hur analyseras insamlade data för att ge erforderligt beslutsunderlag?

3.2.6 Stöd vid ackreditering

Enligt DIT (avsnitt 5.5.1) skall IT-säkerhetstjänsten tillhandahålla ”stöd vid säkerhetsgodkännande (ackreditering) av IT-system”. Detta stöd utgör en aktivitetsbaserad värderingsaspekt (Figur 17).



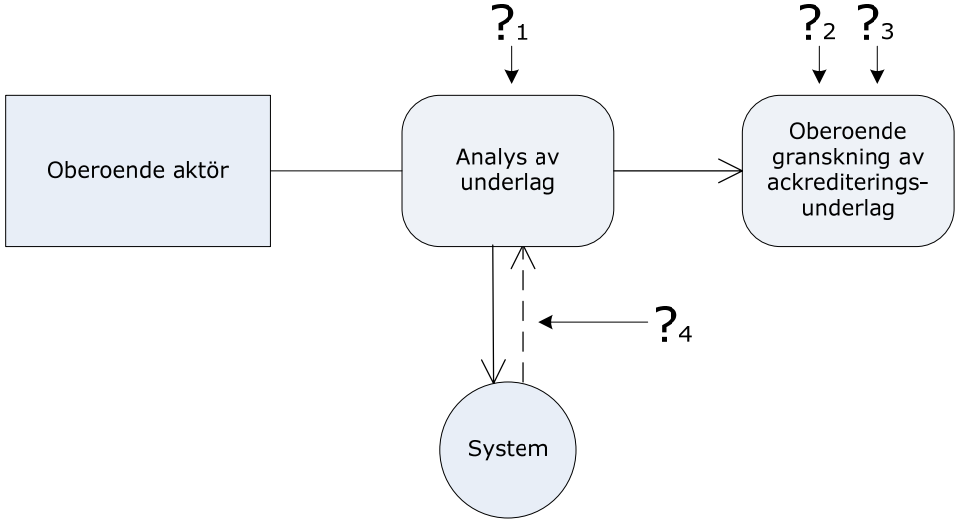
Figur 17: Värderingsaspekten Stöd vid ackreditering.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. I vilka former erbjuder IT-säkerhetstjänsten stöd vid ackreditering av IT-system?
2. Vilka data utgår de olika formerna av stöd ifrån (systemet självt, ackrediteringsunderlag etc.)?
3. Vilka resultat tillhandahåller de olika formerna av stöd?

3.2.7 Oberoende granskning

Enligt DIT (avsnitt B.3) skall det ”vid behov som bestäms genom Auktorisationsbeslut” genomföras ”oberoende granskning av IT-säkerhetsarbetet”. Syftet är att ”stödja leverantören och underlätta MUST granskning” samt att ”stödja produktägaren genom kvalitetssäkring av underlaget och genom att ge en bild av underlagets och IT-systemets svagheter och styrkor”. Eftersom analysen av underlaget måste hantera värderingsfrågor, utgör oberoende granskning en aktivitetsbaserad värderingsaspekt (Figur 18).



Figur 18: Värderingsaspekten Oberoende granskning.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Hur analyseras tillhandahållet underlag vid en ”oberoende granskning av IT-säkerhetsarbetet”?
2. Hur ser ”en bild av underlagets och IT-systemets svagheter och styrkor” ut?
3. Hur säkerställs kvalitén hos den oberoende granskningen?
4. Vad, utöver ackrediteringsunderlaget, utgör grunden för analysen?

3.2.8 Hot-, risk- och sårbarhetsanalys

Enligt H SÄK IT (avsnitt 8.6) gäller att organisationsenheter skall genomföra hot-, risk- och sårbarhetsanalyser för IT-system. Dessa analysaktiviteter resulterar i flera aktivitetsbaserade värderingsaspekter (Figur 19).

Analysernas omfattning antyds i H SÄK IT (avsnitt 8.1): ”Beroende på hur omfattande och komplext ett IT-system är, kan det vara nödvändigt att genomföra och dokumentera analyserna samt kravformuleringen stegvis. I många fall är dock IT-systemen och den verksamhet som de ska stödja så pass överblickbar att de olika analyserna och kravformuleringen kan göras och dokumenteras i ett steg.” Bedömningar av komplexiteten hos kommande hot-, risk- och sårbarhetsanalyser utgör en värderingsaspekt.

1. Hur avgörs när system och verksamhet är ”så pass överblickbar” att hot-, risk- och sårbarhetsanalyser för IT-system kan genomföras som en analys?

Enligt H SÄK IT (avsnitt 8.6) gäller att ”För att kunna genomföra en risk- och sårbarhetsanalys, måste en hotbild mot verksamheten och IT-systemet vara framtagen (hotanalys). Idéer och förslag på hot framgår av H SÄK Hot och H SÄK IT hot.” Enligt H SÄK IT (avsnitt 8.6) gäller att ”De hot som identifieras (genom t ex [eng. brainstorming]) kvantifieras avseende den konsekvens som ett inträffat hot medför samt sannolikheten för att hotet skall inträffa.” Bedömningar av sannolikheter för att hot skall inträffa utgör en värderingsaspekt.

2. Hur begränsas de möjliga hoten, riskerna och sårbarheterna?
3. Hur kvantifieras konsekvensen som ett inträffat hot medför?
4. Hur tas sannolikheten för att ett hot skall inträffa fram?

Enligt H SÄK IT (avsnitt 8.6) gäller att ”Riskanalysen kan genomföras med stöd av SBA Scenario, för vilket Försvarsmakten har licens.” Enligt *Mall Säkerhetsmålsättning* (avsnitt 5) gäller att ”För hot-, risk- och sårbarhetsanalys rekommenderas FM-Scenario.” Hur riskanalyser genomförs med hjälp av ett verktyg utgör en metodikfråga och värderingsaspekt.

5. Vilka verktyg används för hot-, risk- och sårbarhetsanalyser?
6. Vilket metodikstöd tillhandahålls för att möjliggöra effektiva analyser?

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. 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.” Genomförande av sårbarhetsanalys utgör en värderingsaspekt.

7. Hur avgörs säkerhetskravens förmåga att eliminera risker?
8. Vilka indata krävs från systemet för genomförandet av sårbarhetsanalysen?
9. Är det vanligt att sårbarhetsanalysen är iterativ?
10. Hur avgörs det när ”de bedömda resulterande riskvärdena hos sårbarheterna har nått tillräckligt låga och acceptabla nivåer”?

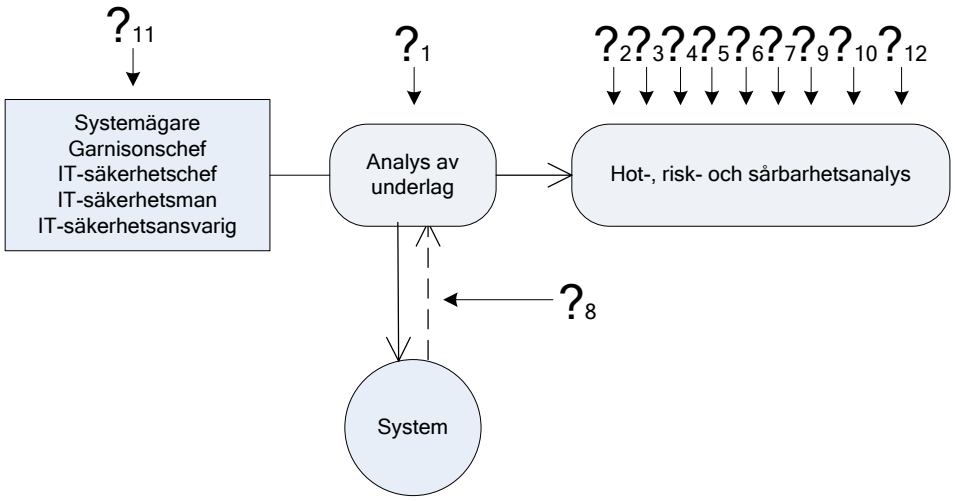
Många olika aktörer kan vara inblandade i framtagandet av hot-, risk- och sårbarhetsanalyser.

- 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-säkerhetsmans uppgifter kan, bl a, innefatta att ”Medverka vid genomförandet av IT-säkerhetsanalyser.” (H SÄK IT, avsnitt 7.6.2)
- 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)
- ”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 §)
- Deltagande analys skall genomföras, med användarrepresentanter, chefer och andra berörda (H SÄK IT, avsnitt 8.6).

11. Vilka olika aktörer genomför i praktiken hot-, risk- och sårbarhetsanalyser för IT-system?

Enligt H SÄK IT (avsnitt 8.6) resulterar hot-, risk- och sårbarhetsanalyser i konsekvensanalyser. Kopplingen mellan konsekvensanalyser respektive hot-, risk- och sårbarhetsanalyser utgör en värderingsaspekt.

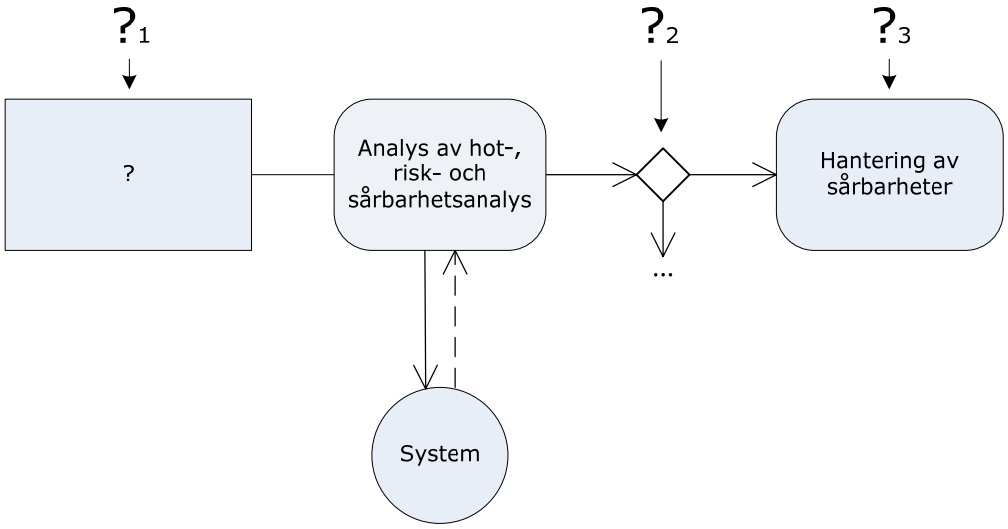
12. På vilket sätt erhålls konsekvensanalyser ur hot-, risk- och sårbarhetsanalyser?



Figur 19: Värderingsaspekter resulterande från hot-, risk-, och sårbarhetsanalys.

3.2.9 Beslut avseende hantering av sårbarheter

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. Beslut avseende hantering av sårbarheter utgör en beslutsbaserad värderingsaspekt (Figur 20).



Figur 20: Värderingsaspekten Beslut avseende hantering av sårbarheter.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilka olika aktörer tar beslut om hur sårbarheter skall behandlas?
2. Vilka kriterier ligger till grund för beslut om hur sårbarheter skall behandlas?
3. Vad avses med riskhantering?

3.2.10 Fastslå kravställning och realisering av säkerhetsfunktioner

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.”

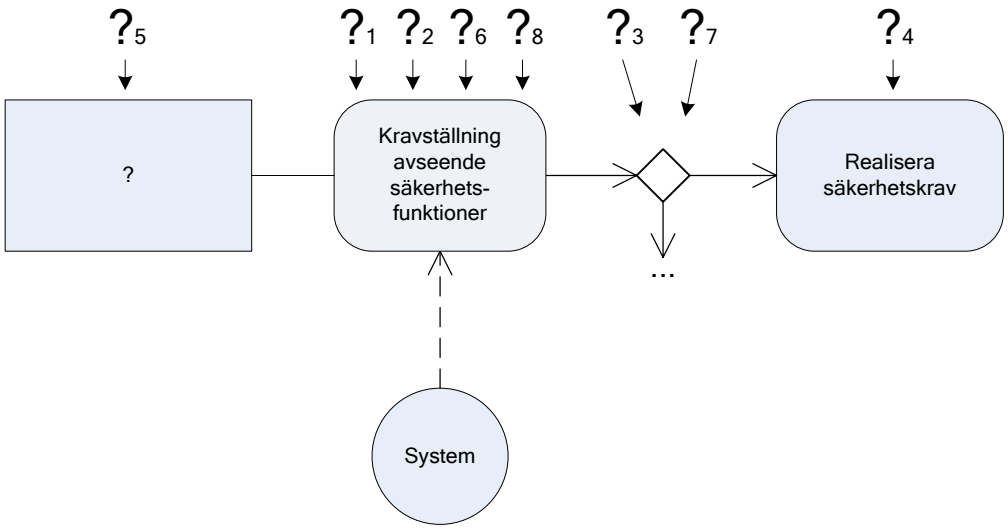
Detta ger upphov till de två beslutsbaserade värderingsaspekterna fastslå kravställning och realisering av säkerhetsfunktioner (Figur 21). Följande frågeställningar är relaterade till dessa värderingsaspekter.

1. Hur visas att uppfyllelse av KSF leder till system med ”godtagbar IT-säkerhet”?
2. Hur anpassas KSF för en specifik hotbild?
3. Hur avgörs om KSF, anpassad för en specifik hotbild, uppfyller miniminivån för IT-säkerhet inom FM?
4. Hur avgörs om implementerade säkerhetsmekanismer uppfyller kraven?

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.” Detta relaterar till värderingsaspekten fastslå kravställning av säkerhetsfunktioner.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

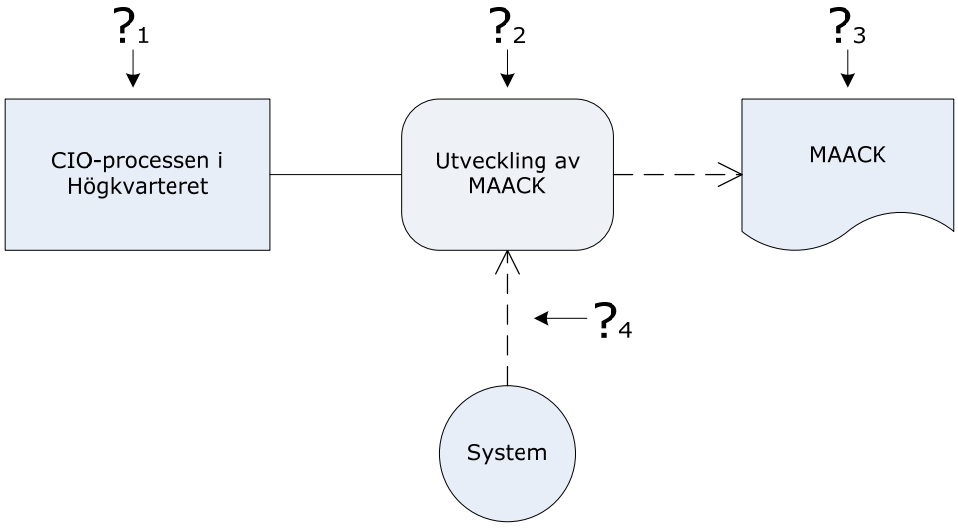
5. Vilka aktörer ansvarar för, respektive genomför aktiviteten kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen?
6. Vilken är relationen mellan kravställning avseende säkerhetsfunktioner i säkerhetsmålsättningen och sårbarhetsanalysen?
7. Hur avgörs vilka alternativa åtgärder som kan nyttjas?
8. I vilka fall är det aktuellt att kravställa säkerhetsmekanismer i säkerhetsmålsättningen?



Figur 21: Värderingsaspekten Fastslå kravställning och realisering av säkerhetsfunktioner.

3.2.11 MAACK

Enligt H SÄK IT (avsnitt 8.6) innehåller Metod och utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten (MAACK) metodik för att ta fram hot-, risk- och sårbarhetsanalyser. Enligt H SÄK IT (avsnitt 23.1) gäller att ”Stödprocessen CIO-processen i Högkvarteret ansvarar för Försvarsmaktens ackrediteringsprocess med tillhörande metodstöd (MAACK).” Själva innehållet i MAACK utgör en resultatbaserad värderingsaspekt (Figur 22).



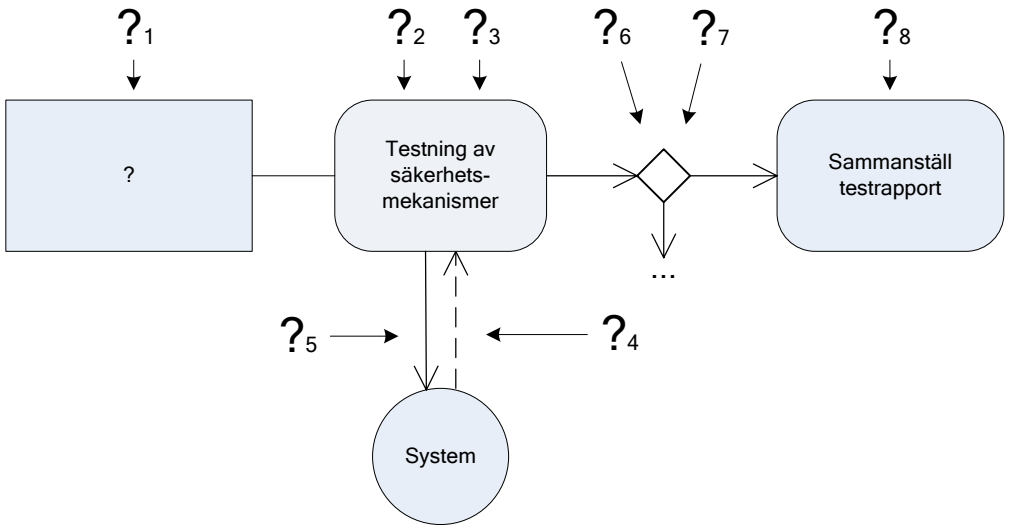
Figur 22: Värderingsaspekten MAACK.

Följande frågeställningar är relaterade till de identifierade värderingsaspekterna.

1. Är det CIO-processen i Högkvarteret som driver utvecklingen av MAACK?
2. Hur utvecklas MAACK?
3. Vilken metodik för att ta fram hot-, risk- och sårbarhetsanalyser innehåller MAACK?
4. Vilka typer av system utgår utvecklingen av MAACK från?

3.2.12 Testgodkännande

Enligt H SÄK IT (avsnitt 11.1) gäller ”Att de valda och implementerade säkerhetsmekanismerna fungerar på avsett sätt säkerställs genom tester. För att slutligen kunna ackreditera ett IT-system är det viktigt att testresultaten visar att säkerhetsmålsättningen är uppfylld.” Detta resulterar i den beslutsbaserade värderingsaspekten testgodkännande (Figur 23).



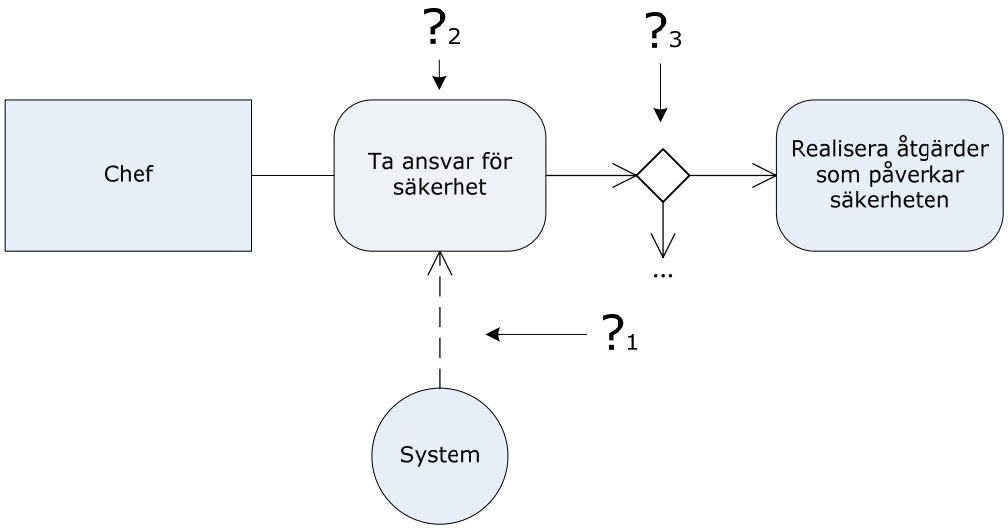
Figur 23: Värderingsaspekten Testgodkännande.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vem genomför testerna?
2. Hur avgörs det om testernas omfång är tillräckligt?
3. Hur dokumenteras testerna och erhållna data?
4. Vilka data samlas in från de testade säkerhetsmekanismerna?
5. Vilken påverkan nyttjas för att erhålla önskade data från de testade säkerhetsmekanismerna?
6. Hur avgörs att ”säkerhetsmekanismerna fungerar på avsett sätt”?
7. Vem avgör att ”säkerhetsmekanismerna fungerar på avsett sätt”?
8. Vad innehåller testrapporten för att bidra till att visa att säkerhetsmålsättningen är uppfylld?

3.2.13 Åtgärdsbeslut

Enligt H SÄK IT (avsnitt 8.6) gäller att ”chefer på alla nivåer vid en organisationsenhet har genom sitt verksamhetsansvar ansvar för säkerheten i och kring IT-systemen”. Ansvar medför behov av kunskap, vilket medför att ansvar för säkerhet blir en beslutsbaserad värderingsaspekt (Figur 24).



Figur 24: Värderingsaspekten Åtgärdsbeslut.

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilket stöd får chefer för att kunna ta sitt ”ansvar för säkerheten i och kring IT-systemen”?
2. Hur skall chefer analysera tillhandahållet underlag för att kunna ta sitt ansvar?
3. Hur skall chefer avgöra vad som behöver åtgärdas för att de skall fullgöra sitt ansvar?

3.3 Drift

I denna kategori ingår värderingsaspekter som är kopplade till driften av IT-system.

3.3.1 Kontroll

3.3.1.1 Tillse att skydd är erforderligt

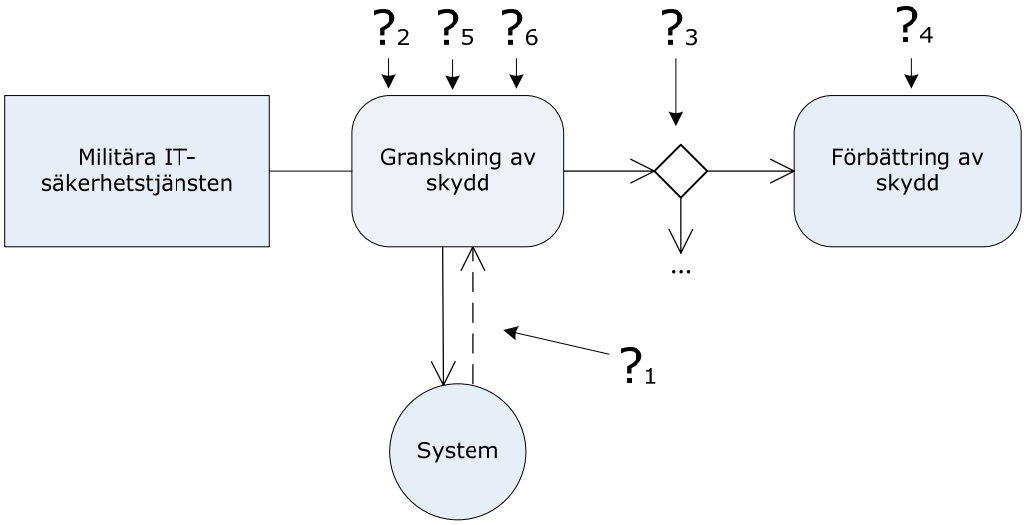
Enligt DIT (avsnitt 5.5.1) är det ett mål inom informationssäkerhetsområdet att militära IT-säkerhetstjänsten skall ”tillse att IT-infrastruktur, IT-system, information och anläggningar såväl inom som utom landet har erforderligt skydd”, samt ”tillgodose kraven på skydd av IT-infrastruktur, IT-system och information avseende tillgänglighet, riktighet, spårbarhet och sekretess” (DIT, avsnitt 5.5.2). Detta utgör en beslutsbaserad värderingsaspekt då det krävs förmågan att avgöra om ett befintligt skydd är adekvat (Figur 25). Följande frågeställningar är relaterade till denna värderingsaspekt.

1. Hur återkopplas skyddsnivån till militära IT-säkerhetstjänsten?
2. Hur genomförs granskningen av befintligt skydd?
3. Hur avgörs vad som är ”erforderligt skydd”?
4. Hur avgörs vilka åtgärder som skall genomföras för att erhålla ”erforderligt skydd”?

Enligt DIT (avsnitt 5.5.1) skall militära IT-säkerhetstjänsten utveckla ”förmågan att genomföra administrativa kontroller av efterlevnad av regelverket vad avser signalskydd och IT-säkerhet” samt tillhandahålla ”aktiva och tekniska kontroller”. Att avgöra om regelverket efterlevs utgör en beslutsbaserad värderingsaspekt (Figur 25).

Följande frågeställningar är relaterade till denna värderingsaspekt.

5. Hur avgörs om regelverket efterlevs?
6. Hur genomförs de tekniska IT-säkerhetskontrollerna?



Figur 25: Värderingsaspekten Tillse att skydd är erforderligt

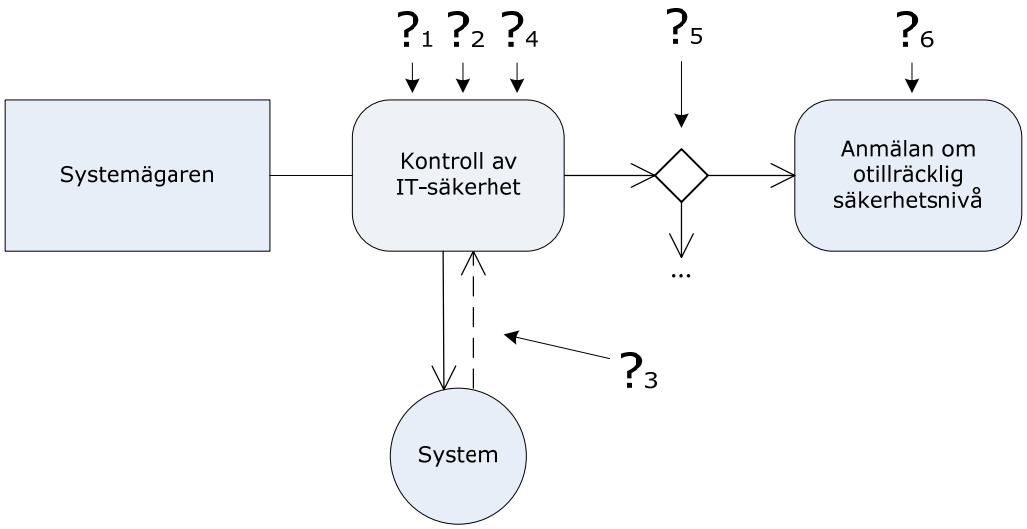
3.3.1.2 Avgöra tillräcklighet hos säkerheten i och kring IT-system

Enligt H SÄK IT (avsnitt 7.4) gäller att ”Systemägaren skall genomföra kontroller av säkerheten i och kring sådana IT-system inom enheten som inte är avsedda för behandling av hemliga uppgifter.” Att avgöra ifall nivån på säkerheten i och kring ett IT-system är tillräcklig utgör en beslutsbaserad värderingsaspekt. (Figur 26). Följande frågeställningar är relaterade till denna värderingsaspekt.

1. Hur kontrolleras säkerheten ”kring” ett IT-system?
2. Innebär kontroll av säkerheten ”kring” ett IT-system att varje Systemägare skall värdera säkerheten i alla IT-system inom enheten?
3. Vilka data samlas in för att genomföra kontrollen?

Enligt DIT (avsnitt 3.9) skall systemägare anmäla ”otillräcklig säkerhetsnivå till militärdistriktet/MUST ITSA och produktägaren”. Att avgöra ifall ett system har en otillräcklig säkerhetsnivå utgör en beslutsbaserad värderingsaspekt (Figur 26). Följande frågeställningar är relaterade till denna värderingsaspekt.

4. Hur specificeras systemets säkerhetsnivå?
5. Hur detekteras ”otillräcklig säkerhetsnivå”?
6. Hur avgörs vilka åtgärder en anmälan leder till?



Figur 26: Värderingsaspekten Avgöra tillräcklighet hos säkerheten i och kring IT-system

3.3.1.3 Beslut om tillräcklig skyddsnivå

Enligt H SÄK IT (avsnitt 24.1) gäller att ”kontrollera att skyddsnivån är anpassad till aktuell hotbild. Detta innebär att kontroller genomförs för att verifiera att de skyddsåtgärder som finns fyller sitt syfte och att de sårbarheter (resulterande risker) som accepterats, hanteras på ett säkert sätt.” Att avgöra ifall skyddet är tillräckligt utgör en beslutsbaserad värderingsaspekt (Figur 27). Följande frågeställningar är relaterade till denna värderingsaspekt.

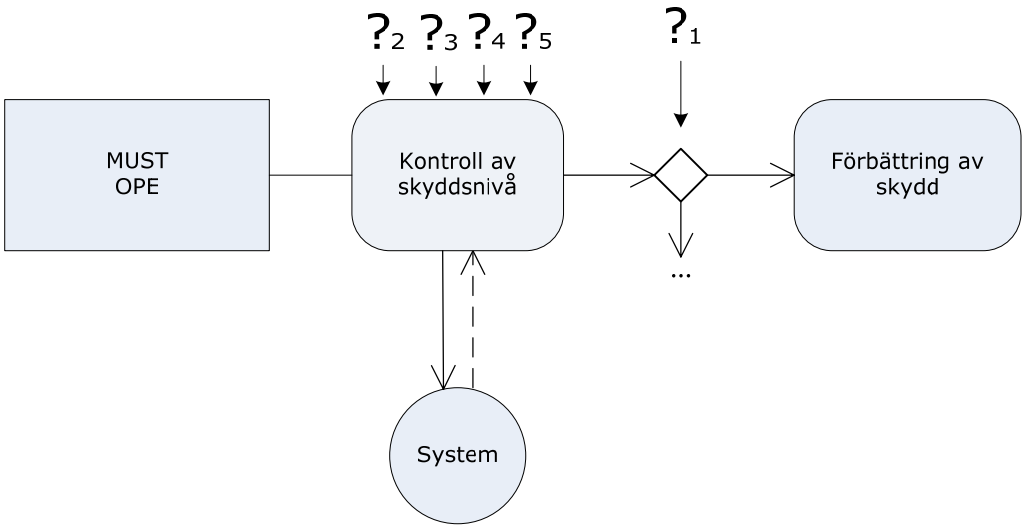
1. Hur avgörs om ”skyddsnivån är anpassad till aktuell hotbild”?
2. Hur verifieras att skyddsåtgärderna ”fyller sitt syfte”?
3. Hur avgörs om sårbarheter ”hanteras på ett säkert sätt”?

Enligt H SÄK IT (avsnitt 24.1) gäller att ”En IT-säkerhetskontroll måste även eftersträva att identifiera och medvetandegöra förbisedda brister i skyddet.” Att avgöra vad som är brister i skyddet utgör en beslutsbaserad värderingsaspekt (Figur 27) med följande frågeställning.

4. Hur går man tillväga för att ”identifiera och medvetandegöra förbisedda brister”?

Enligt H SÄK IT (avsnitt 24.2) gäller att ”Militära underrättelse- och säkerhetstjänsten (MUST) genomför IT-säkerhetskontroll vid Högkvarteret (där säkerhets- och samverkanssektionerna ingår i den operativa enheten [OPE]), FMLOG, utlandsstyrkan m fl.” Enligt H SÄK IT (avsnitt 24.2) gäller att ”Varje säkerhets- och samverkanssektion vid OPE genomför IT-säkerhetskontroller vid övriga organisationsenheter inom sina respektive ansvarsområden.” Att avgöra om ett system är säkert eller ej utgör en beslutsbaserad värderingsaspekt. Följande frågeställning är relaterad till denna värderingsaspekt (Figur 27).

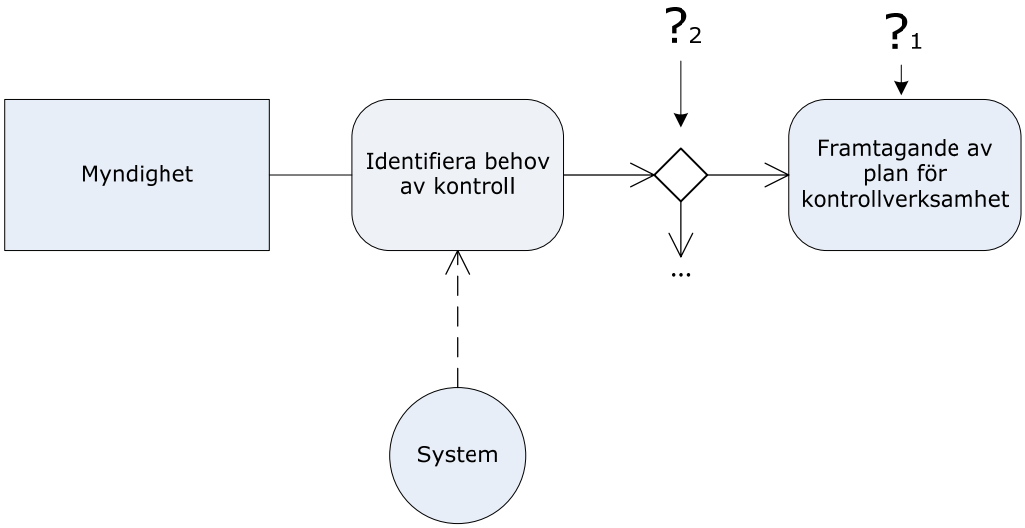
5. Vad innefattar IT-säkerhetskontrollen som MUST/OPE genomför?



Figur 27: Värderingsaspekten Beslut om tillräcklig skyddsnivå

3.3.1.4 Avgöra behov av kontroll

Enligt H SÄK IT (avsnitt 24.3) gäller att ”En plan för kontroll av IT-säkerhetsskyddet skall finnas. I denna redovisas vad som skall kontrolleras och när det skall ske.” Att avgöra vad som skall kontrolleras är en beslutsbaserad värderingsaspekt (Figur 28).



Figur 28: Värderingsaspekten Avgöra behov av kontroll

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Uppdateras kontrollplanen då nytt behov uppstår, eller sker detta med ett bestämt intervall (t.ex. årligen)?
2. Hur säkerställs att alla relevanta faktorer finns med i kontrollplanen?

3.3.1.5 Beslut om åtgärdande av identifierade brister

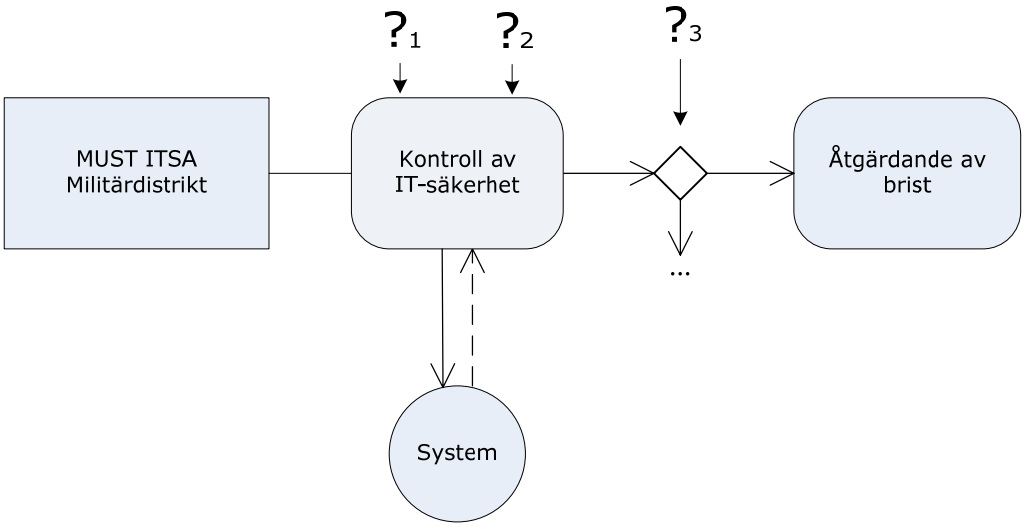
Enligt DIT (avsnitt 3.9) skall föranmälda och oanmälda kontroller av IT-säkerhet genomföras för alla organisationsenheter av MUST ITSA samt för varje militärdistrikts

organisationsenheter av respektive Militärdistrikt. Att avgöra vilken nivå ett systems IT-säkerhet har är en beslutsbaserad värderingsaspekt (Figur 29). Följande frågeställningar är relaterade till denna värderingsaspekt.

1. Genomförs kontrollerna på alla system hos en organisationsenhet, eller görs stickprov på utvalda system?
2. Innebär kontrollen att det säkerställs att den i ackrediteringsbeslutet angivna nivån upprätthålls?

Enligt H SÄK IT (avsnitt 24.4) gäller att ”Direkt efter kontrollen delges den kontrollerade muntligen en sammanfattning av gjorda iakttagelser. […] Den muntliga återredovisningen omfattar även förslag på omedelbara åtgärder.” Att avgöra vilka ”omedelbara åtgärder” som måste genomföras utgör en beslutsbaserad värderingsaspekt (Figur 29). Följande frågeställning är relaterad till denna värderingsaspekt.

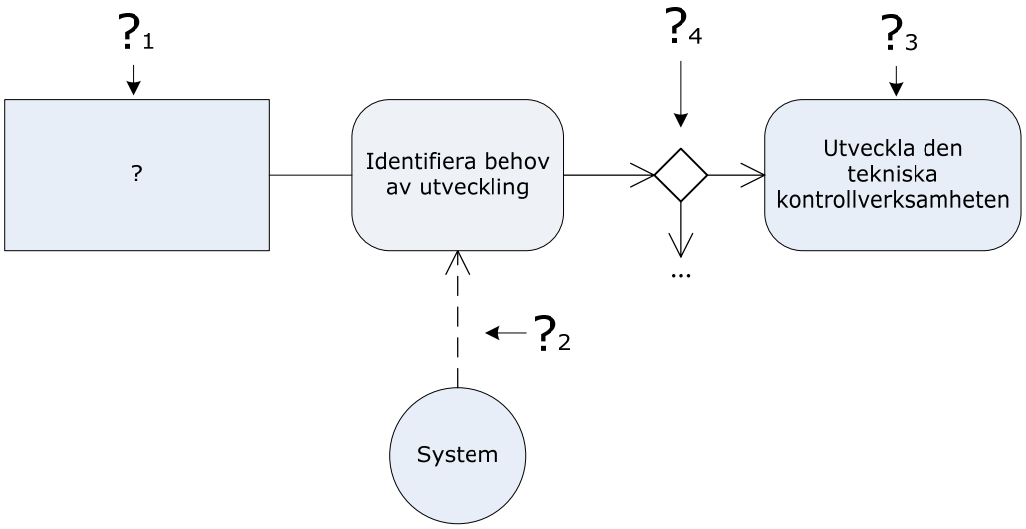
3. Hur avgörs vilka åtgärder som skall genomföras för att åtgärda identifierade brister?



Figur 29: Värderingsaspekten Beslut om åtgärdande av identifierade brister

3.3.1.6 Avgöra behov av utveckling av den tekniska kontrollverksamheten

Enligt DIT (avsnitt 5.5.2) gäller att ”Tekniska kontrollverksamheten skall utvecklas och förbättras både vad avser signalskydd och vad avser IT-system och IT-infrastruktur. Förbättringar skall ske både vad avser processer och verktyg/metoder”. Att avgöra hur den tekniska kontrollverksamheten skall utvecklas och förbättras är en beslutsbaserad värderingsaspekt (Figur 30).



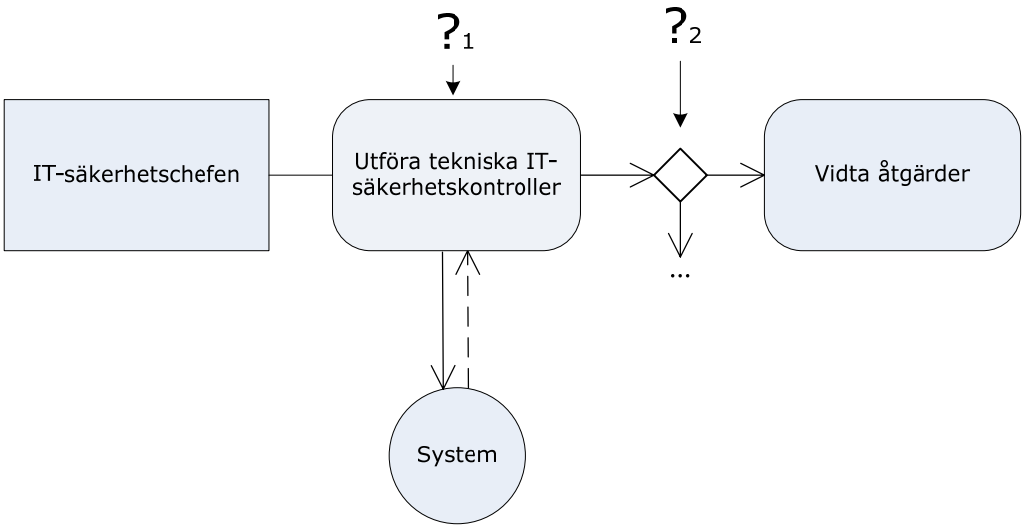
Figur 30: Värderingsaspekten Avgöra behov av utveckling av den tekniska kontrollverksamheten

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilken aktör utvecklar och förbättrar kontrollverksamheten?
2. Vilka data används för att identifiera behov av utveckling och förbättring?
3. Hur utvecklas och förbättras kontrollverksamheten?
4. Hur avgörs vilka identifierade utvecklingar och förbättringar som skall genomföras?

3.3.1.7 Beslut om åtgärder baserat på tekniska IT-säkerhetskontroller

Enligt H SÄK IT (avsnitt 24.4.2) gäller att ”Tekniska IT-säkerhetskontroller genomförs för att säkerställa att uppgifter i IT-system inte görs tillgängliga eller röjs för obehöriga, att uppgifterna är riktiga, spårbara samt tillgängliga för behöriga användare. Vid sådana kontroller har en IT-säkerhetschef ett antal verktyg till sin hjälp, vilka är godkända för användning inom Försvarsmakten, den s k kontrollplattformen”. Att avgöra huruvida ett IT-system uppfyller de nämnda kraven utgör en beslutsbaserad värderingsaspekt (Figur 31).



Figur 31: Värderingsaspekten Beslut om åtgärder baserat på tekniska IT-säkerhetskontroller

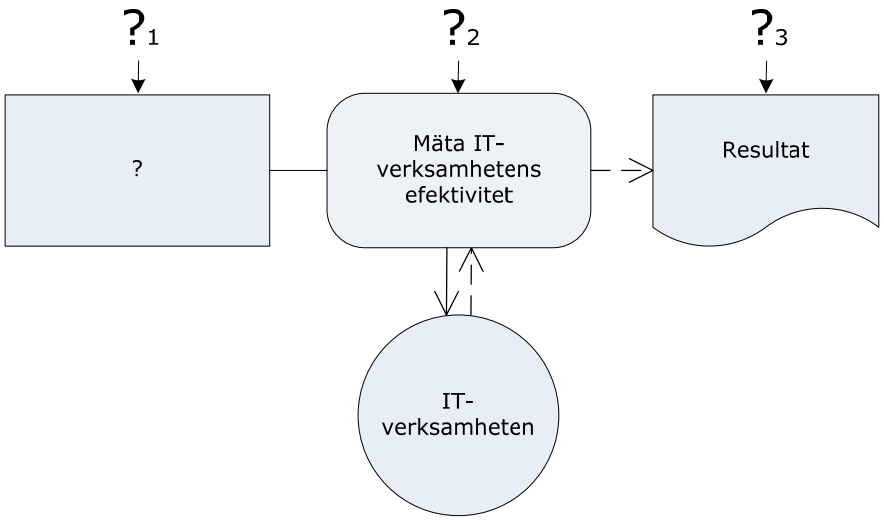
Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilka rutiner finns för hur plattformen skall användas?
2. Hur avgörs om plattformens verktyg och de genomförda kontrollerna beaktar relevanta faktorer för att ”säkerställa att uppgifter i IT-system inte görs tillgängliga eller röjs för obehöriga, att uppgifterna är riktiga, spårbara samt tillgängliga för behöriga användare”?

3.3.2 Informationssäkerhetsverksamhet

3.3.2.1 IT-säkerhetsarbetets effektivitet

Enligt DIT (avsnitt 5.3.3) är det ett mål att ”IT-verksamhetens effektivitet skall mätas”. Enligt den tillhörande handlingsplanen skall IT-säkerhetsarbetet kunna särredovisas. En koppling från IT-verksamhet till IT-säkerhetsarbete ger den resultatbaserade värderingsaspekten IT-säkerhetsarbetets effektivitet (Figur 32).



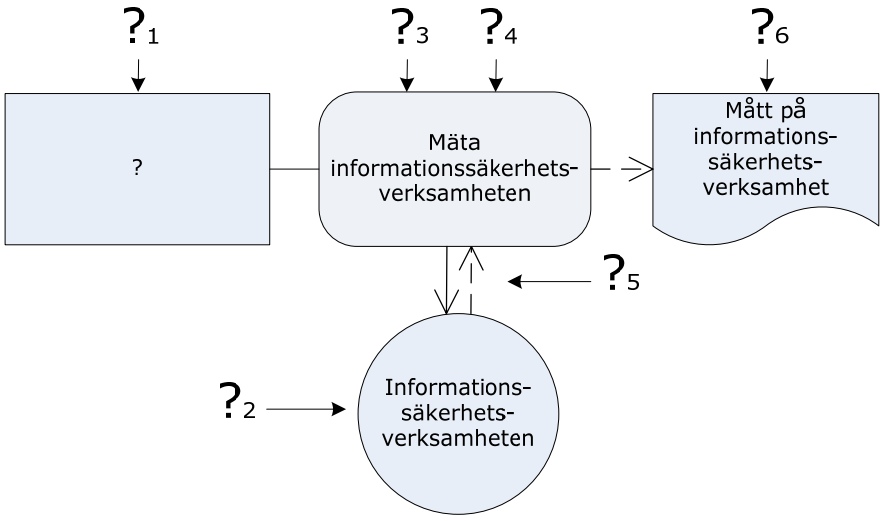
Figur 32: Värderingsaspekten IT-säkerhetsarbetets effektivitet

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilka aktörer skall mäta IT-verksamhetens effektivitet?
2. Innebär detta att IT-säkerhetsarbetets effektivitet skall mätas och i så fall hur?
3. Vad utgör resultatet av mätningen?

3.3.2.2 Mått på informationssäkerhetsverksamheten

Enligt DIT (avsnitt 5.5.5) är det ett mål att ”Informationssäkerhetsverksamheten skall vara mätbar och bedrivas på ett rationellt och kostnadseffektivt sätt” samt att ”Informationssäkerhetsverksamhet inom produktägarens ansvarsområde skall budgeteras och följas upp”. Detta ger upphov till den resultatbaserade värderingsaspekten mått på informationssäkerhetsverksamheten (Figur 33).



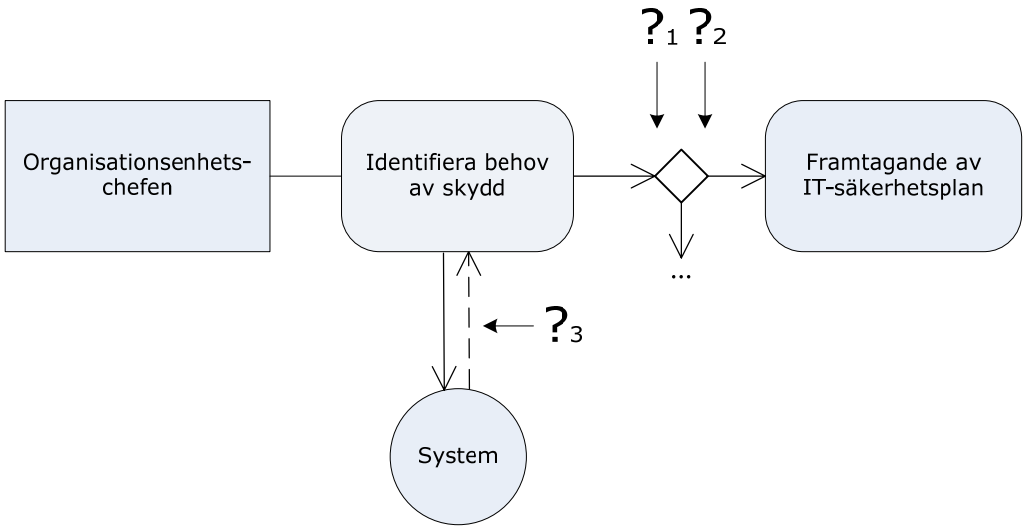
Figur 33: Värderingsaspekten Mått på informationssäkerhetsverksamheten

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vilka aktörer skall mäta?
2. Vad innefattar informationssäkerhetsverksamheten?
3. Vad skall mätas för att profilera verksamheten?
4. Hur säkerställs mätbarheten?
5. Hur följs informationssäkerhetsverksamheten upp?
6. Leder handlingsplanen (DIT, avsnitt 5.5.5) till att målet om mätbarhet uppfylls?

3.3.2.3 Organisationsenhetschefen: beslut om innehåll i IT-säkerhetsplan

Enligt avsnitt H SÄK IT (avsnitt 8.9) gäller att ”en IT-säkerhetsplan skall ta upp sådana omständigheter som måste åtgärdas av någon ansvarig inom en viss angiven tidsrymd givet vissa resurser för att skyddet för berört IT-system skall kunna sägas vara tillräckligt.” Att avgöra vilka omständigheter som måste åtgärdas utgör en beslutsbaserad värderingsaspekt (Figur 34).



Figur 34: Värderingsaspekten Beslut om innehåll i IT-säkerhetsplan

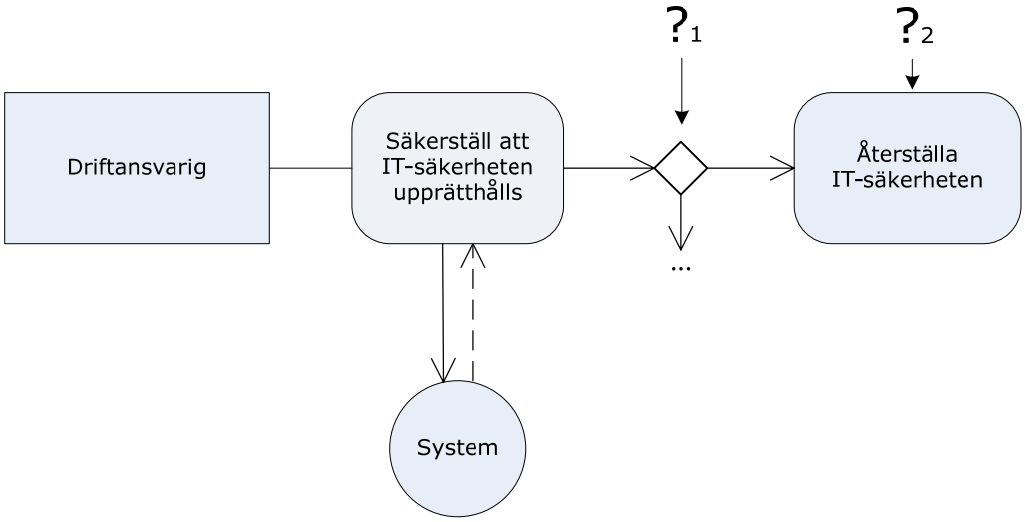
Följande frågeställning är relaterad till den identifierade värderingsaspekten.

1. Hur avgörs vilka ”omständigheter” som måste åtgärdas?
2. Hur avgörs inom vilken tidsrymd som ”omständigheter” måste åtgärdas?
3. Vilka data behöver samlas in från system?

3.3.3 Lägesbild

3.3.3.1 Avgöra om IT-säkerheten upprätthålls

Enligt H SÄK IT (avsnitt 9.1) gäller att ”Den som ansvarar för driften av ett IT-system har också ett ansvar att säkerställa att IT-säkerheten upprätthålls. Detta ansvar utgår från krav i ackrediteringsbeslut eller beslut om driftförutsättningar, eller båda. Det åligger härmed också driftägaren att hantera, det vill säga åtgärda fel och brister som uppstår vid incidenter samt återställa systemets IT-säkerhetsnivå vid händelse av en incident.” Att avgöra huruvida IT-säkerheten upprätthålls utgör en beslutsbaserad värderingsaspekt (Figur 35).



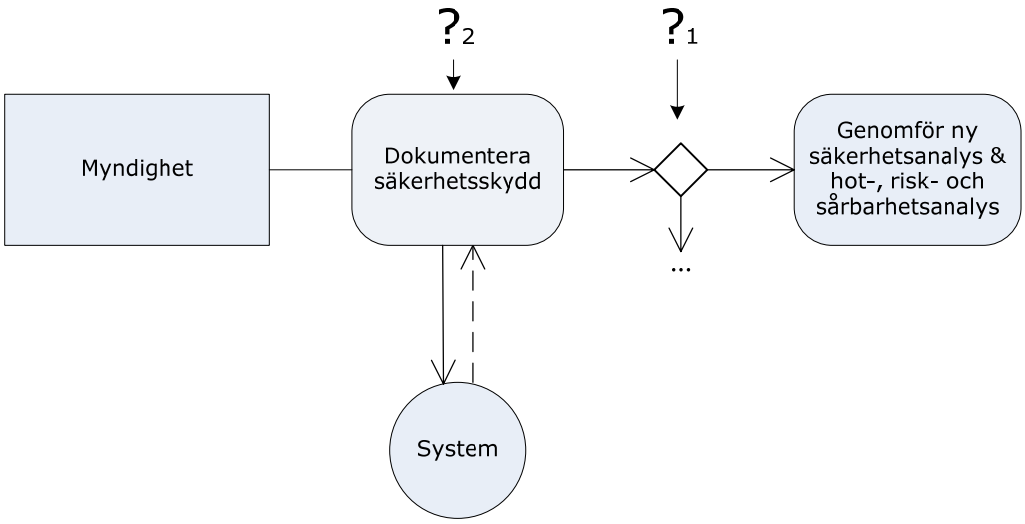
Figur 35: Värderingsaspekten Avgöra om IT-säkerheten upprätthålls

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Hur avgörs om IT-säkerheten upprätthålls?
2. Hur avgörs om IT-säkerheten återställts?

3.3.3.2 Beslut om förnyade analyser

Enligt H SÄK IT (avsnitt 11.1) gäller att ”För att ett IT-systems skydd skall kunna upprätthållas under systemets livslängd är det nödvändigt att kontinuerligt dokumentera det skydd som gäller för IT-systemet. För att kontrollera att säkerhetsskyddet är tillräckligt kan det finnas behov av att genomföra en ny säkerhetsanalys, hot-, risk- och sårbarhetsanalys över systemet”. Detta ger upphov till värderingsaspekten beslut om förnyade analyser (Figur 36).



Figur 36: Värderingsaspekten Beslut om förnyade analyser

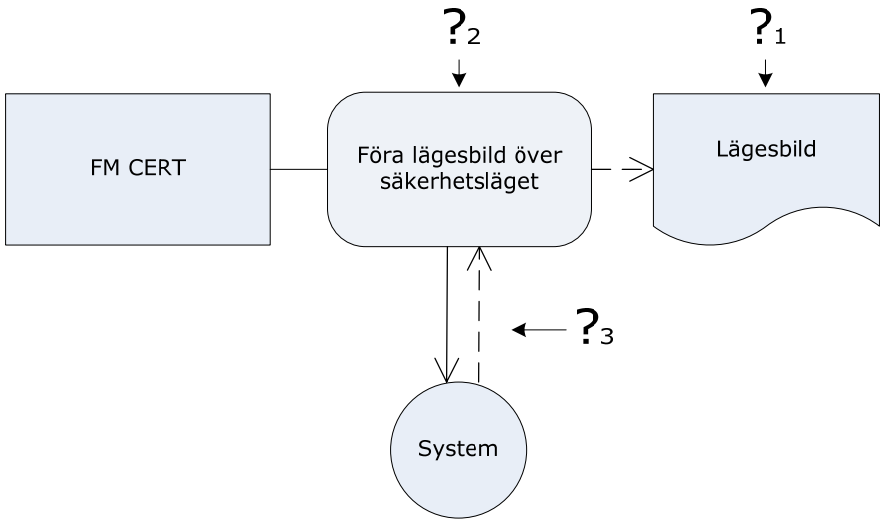
Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Hur avgörs om nya analyser behöver genomföras?

2. Hur avgörs vad som skall ingå i dokumentationen?

3.3.3.3 Lägesbild över säkerhetsläget

Enligt H SÄK IT (avsnitt 9) gäller att ”FM CERT har till huvuduppgift att föra en lägesbild över säkerhetsläget i Försvarsmaktens IT-system. Med säkerhetsläge avses de faktorer som påverkar sekretess, tillgänglighet, riktighet och spårbarhet i de uppgifter som behandlas i myndighetens IT-system. Mottagare av dessa uppgifter är bland andra operativa enheten i Högkvarteret, driftägare, produktägare och säkerhetsorganisationen.” Lägesbilder avseende säkerheten i IT-system utgör en resultatbaserad värderingsaspekt (Figur 37).



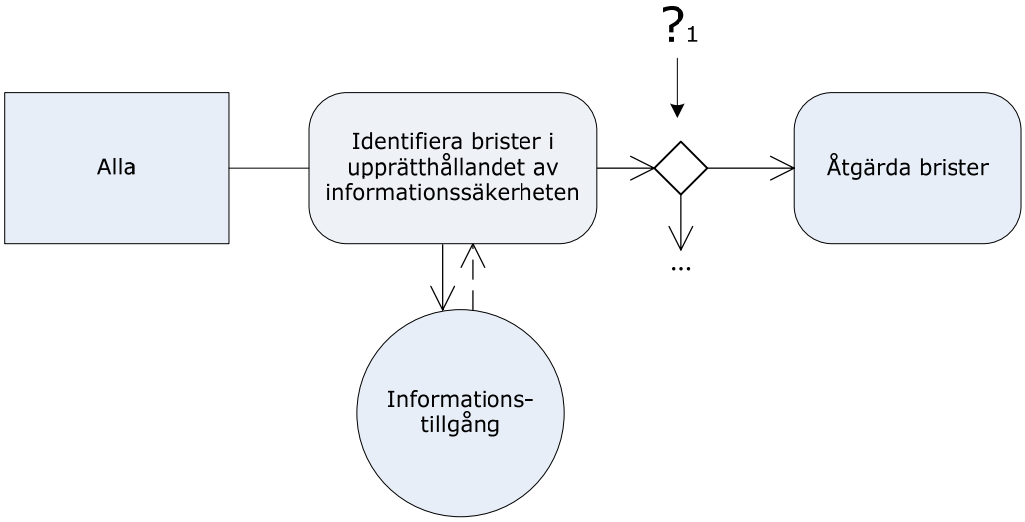
Figur 37: Värderingsaspekten Lägesbild över säkerhetsläget

Följande frågeställningar är relaterade till den identifierade värderingsaspekten.

1. Vad innebär en ”lägesbild över säkerhetsläget”?
2. Hur anpassas en ”lägesbild över säkerhetsläget” till mottagarens behov?
3. Vilka data behövs för en ”lägesbild över säkerhetsläget”?

3.3.4 Avgöra ifall informationssäkerheten upprätthålls

Enligt H SÄK IT (Bilaga 1) gäller att ”Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten.” Att avgöra om informationssäkerheten upprätthålls utgör en beslutsbaserad värderingsaspekt (Figur 38).



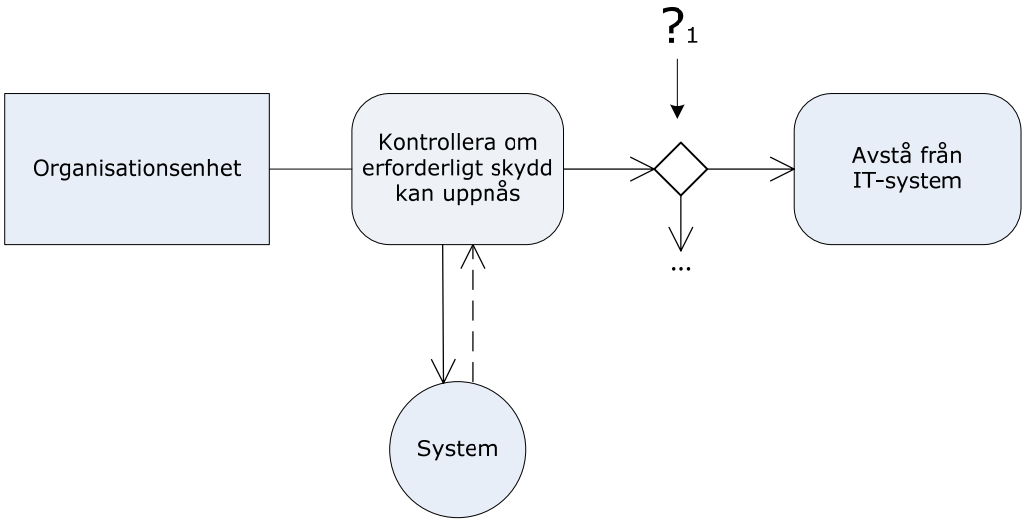
Figur 38: Värderingsaspekten Avgöra ifall informationssäkerheten upprätthålls

Följande frågeställning är relaterad till den identifierade värderingsaspekten.

1. Hur avgörs ifall informationssäkerheten upprätthålls?

3.3.5 Beslut om begränsning av användning

Enligt FIB 2006:2 (3 kap. 5 §) gäller att ”varje organisationsenhet skall av säkerhetsskäl avstå från ett IT-system som inte är avsett för behandling av hemliga uppgifter eller begränsa dess innehåll, om erforderligt skydd inte kan uppnås eller upprätthållas. Med erforderligt skydd avses att uppgifter inte görs tillgängliga eller röjs för obehöriga personer, samt att uppgifterna är riktiga och spårbara samt tillgängliga för behöriga användare.”. Att avgöra huruvida erforderligt skydd kan uppnås eller ej innebär en beslutsbaserad värderingsaspekt (Figur 39).



Figur 39: Värderingsaspekten Beslut om begränsning av användning.

Följande frågeställning är relaterad till den identifierade värderingsaspekten.

1. Hur avgörs ifall ”erforderligt skydd inte kan uppnås eller upprätthållas”?

4 Processer innehållande värderingsaspekter

Utgående från i föregående kapitel presenterade värderingsaspekter, beskrivs i detta kapitel ett antal identifierade processer.

4.1 Ackrediteringsbeslut

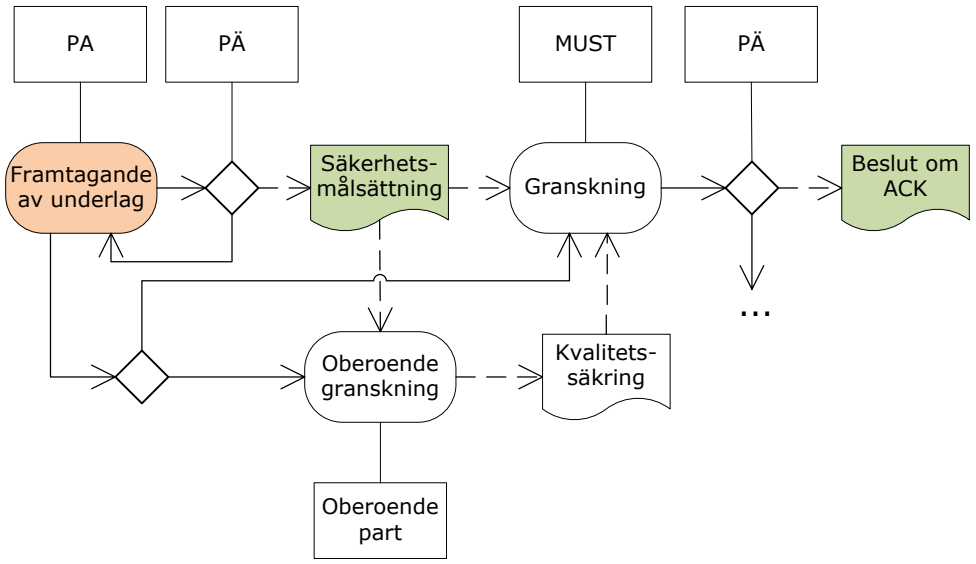
Ett beslut om ackreditering innebär att ett system godkänns ur säkerhetssynpunkt för användning inom Försvarsmakten. Syftet med ackreditering är att säkerställa att ett IT-system har ett tillräckligt IT-säkerhetsskydd, samt att det inte påverkar befintliga IT-system negativt.

Processen för beslut om ackreditering (Figur 40) inleds med att den produktansvarige (PA) tar fram ett ackrediteringsunderlag, vilket består av en säkerhetsmålsättning. Produktägaren (PÄ) fastställer säkerhetsmålsättningen. Säkerhetsmålsättningens innehåll, samt hur innehållet tas fram beskrivs mer ingående i avsnitt 4.2.

I Auktorisationsbeslut avgörs om en oberoende granskning av IT-säkerhetsarbetet skall genomföras av en oberoende part. Syftet med en oberoende granskning är att underlätta granskningsarbetet för MUST, samt att kvalitetssäkra det framtagna ackrediteringsunderlaget.

MUST genomför, då så beslutats i Auktorisationsbeslut, en granskning av ackrediteringsunderlaget. I de fall en oberoende granskning genomförts använder MUST rapporten från den oberoende granskningen som underlag. Resultatet av MUST granskning är ett yttrande över säkerheten i och kring det specifika IT-systemet. Detta yttrande är en del i ackrediteringsunderlaget som ligger till grund för beslut om ackreditering.

Produktägaren ansvarar för att säkerheten i och kring IT-systemet granskas. Syftet med de tidigare angivna granskningarna är att säkerställa att alla specificerade säkerhetskrav möts av säkerhetsmekanismer som är både relevanta och tillräckliga. Det är särskilt viktigt att vid en säkerhetsgranskning tillse att IT-systemet inte påverkar andra IT-system negativt. Det är produktägaren som slutligen avgör om säkerhetsmålsättningen uppfylls och därmed beslutar om systemet skall ackrediteras eller ej.



Figur 40: Process för ackrediteringsbeslut.

4.2 Framtagande av ackrediteringsunderlag

Framtagandet av ackrediteringsunderlag är en central process för att skapa förutsättningar för och vidmakthålla adekvata nivåer av informationssäkerheten inom FM. I detta avsnitt modelleras denna process översiktligt (Figur 41).

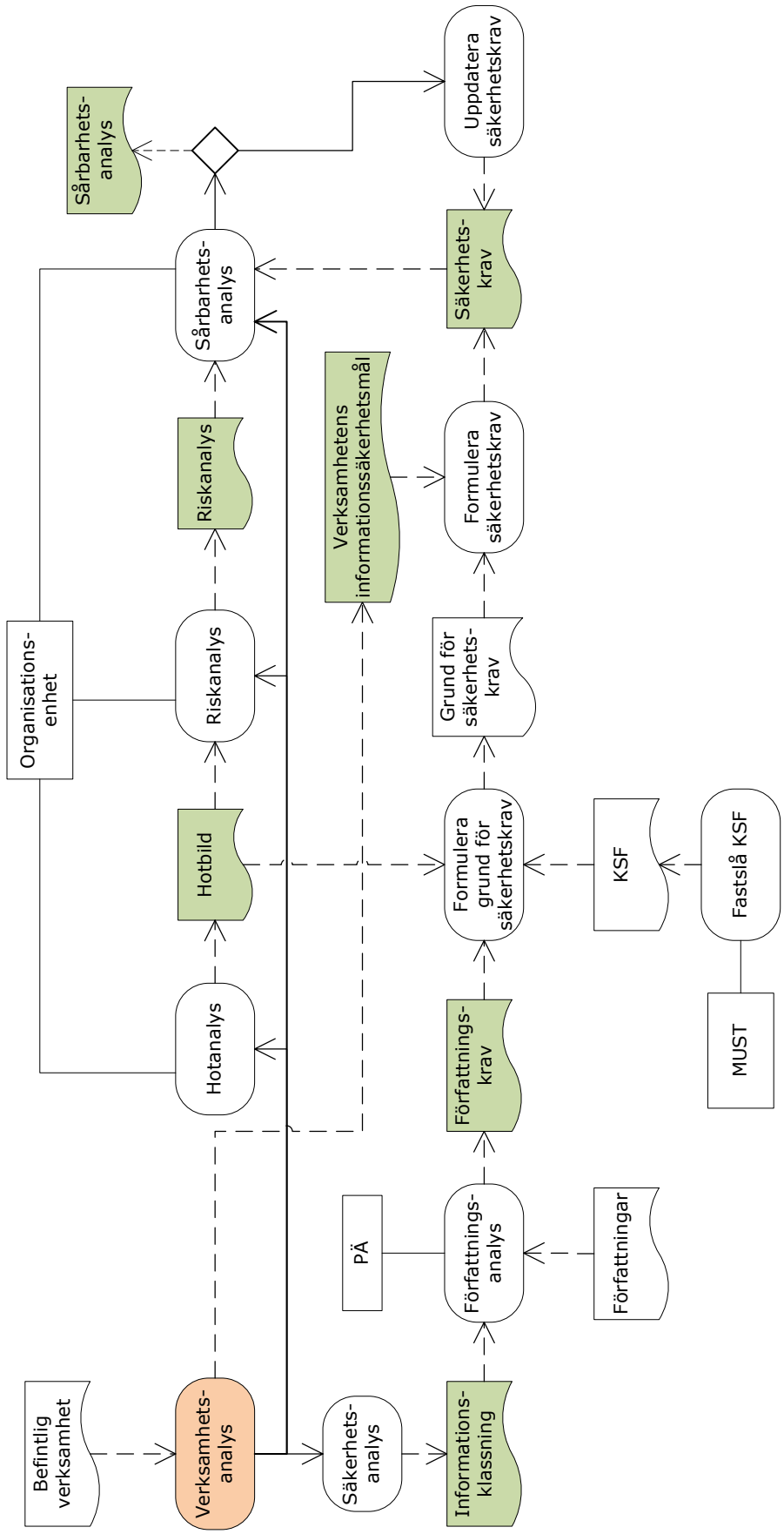
Framtagandet av ackrediteringsunderlag inleds med genomförandet av en *verksamhetsanalys*. Verksamhetsanalysen syftar till att, genom en övergripande beskrivning, analysera den befintliga eller önskade verksamheten. Verksamhetsanalysen inkluderar även en informationsklassning som bedömer säkerhetsklassen 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.

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.

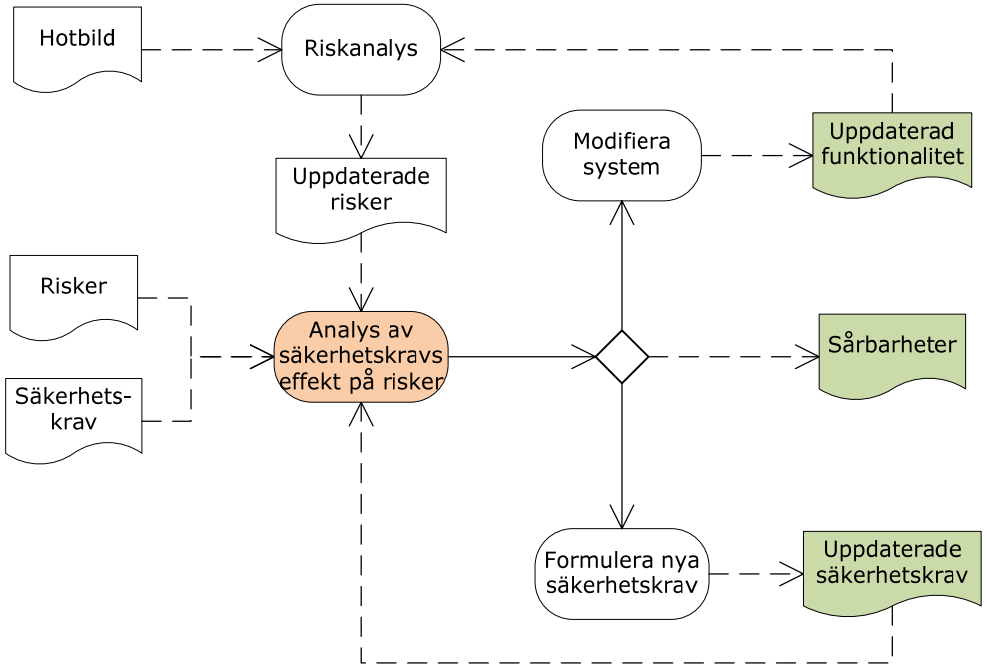
Den avslutande aktiviteten är *sårbarhetsanalysen*, som vidare beskrivs i avsnitt 4.3.



Figur 41: Framtagande av ackrediteringsunderlag.

4.3 Sårbarhetsanalys

Med hjälp av de framtagna säkerhetskraven, hotbilden samt riskanalysen kan sårbarhetsanalysen genomföras. Identifierade hot och risker bemöts med de framtagna säkerhetskraven för att bedöma om säkerhetskraven kan användas för 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 säkerhetskraven omformuleras för att bättre kunna reducera de förekommande riskerna, alternativt måste 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 små (Figur 42).



Figur 42: Sårbarhetsanalys.

5 Diskussion

Det arbete som redovisas i denna rapport har lett till att ett stort antal värderingsaspekter har identifierats. Värderingsaspekterna pekar på situationer där IT-säkerhetsvärdering är nödvändigt för att kunna genomföra nödvändiga aktiviteter, fatta välgrundade beslut eller producera efterfrågade resultat. Följande exempel visar på bredden hos de identifierade värderingsaspekterna.

- Hot-, risk- och sårbarhetsanalys
- Beslut om tillräcklig skyddsnivå
- IT-säkerhetsarbetets effektivitet

Antalet värderingsaspekter och deras bredd visar på att det bedrivs en omfattande värderingsverksamhet inom Försvarsmaktens IT-säkerhetsarbete. I vilken omfattning detta arbete kan underlättas genom vidare utveckling av metoder och verktyg för IT-säkerhetsvärdering återstår att utreda.

Vidare utveckling av metoder och verktyg för IT-säkerhetsvärdering kräver en fortsatt dialog med Försvarsmakten för att på så sätt skapa en tydligare bild över hur IT-säkerhetsvärdering används inom Försvarsmakten. Detta arbete kan utgå från de identifierade värderingsaspekterna med tillhörande frågeställningar.

Då ackrediteringsprocessen är central i Försvarsmaktens IT-säkerhetsarbete, utgår processbeskrivningarna i kapitel 4 från dessa värderingsaspekter. Även om processbeskrivningarna är övergripande visar de på aktiviteter och beslut som innehåller värderingsfrågor. Dessa aktiviteter och beslutspunkter behöver, i dialog med Försvarsmakten, ytterligare specificeras för att utveckla processbeskrivningarna till ett ändamålsenligt underlag för de av FOI planerade testerna av metoder för IT-säkerhetsvärdering. Detta kommer i förlängningen att utgöra underlag för FOIs vidare arbete med utveckling av metoder för IT-säkerhetsvärdering. Metod för genomförande av dessa tester är under utveckling.

Referenser

(Försvarsmakten, 2004)

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

(Försvarsmakten, 2006a)

Försvarsmakten (2006a). *Försvarsmaktens interna bestämmelser, FIB 2006:2*.

(Försvarsmakten, 2006b)

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

(Försvarsmakten, 2006c)

Försvarsmakten (2006c). *Mall Spårbarhet, krav-säkerhetsmål - Bilaga till Säkerhetsmålsättning*, maack-mall version 1.5 edition.

(Försvarsmakten, 2007)

Försvarsmakten (2007). *Mall Säkerhetsmålsättning*, maack-mall version 1.6 edition.

(Hallberg et al., 2007)

Hallberg, J., Hunstad, A., & Hallberg, N. (2007). *Handbok för IT-säkerhetsvärdering (in Swedish)*. Technical report, FOI, Linköping, Sweden.

(SIS, 2007)

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