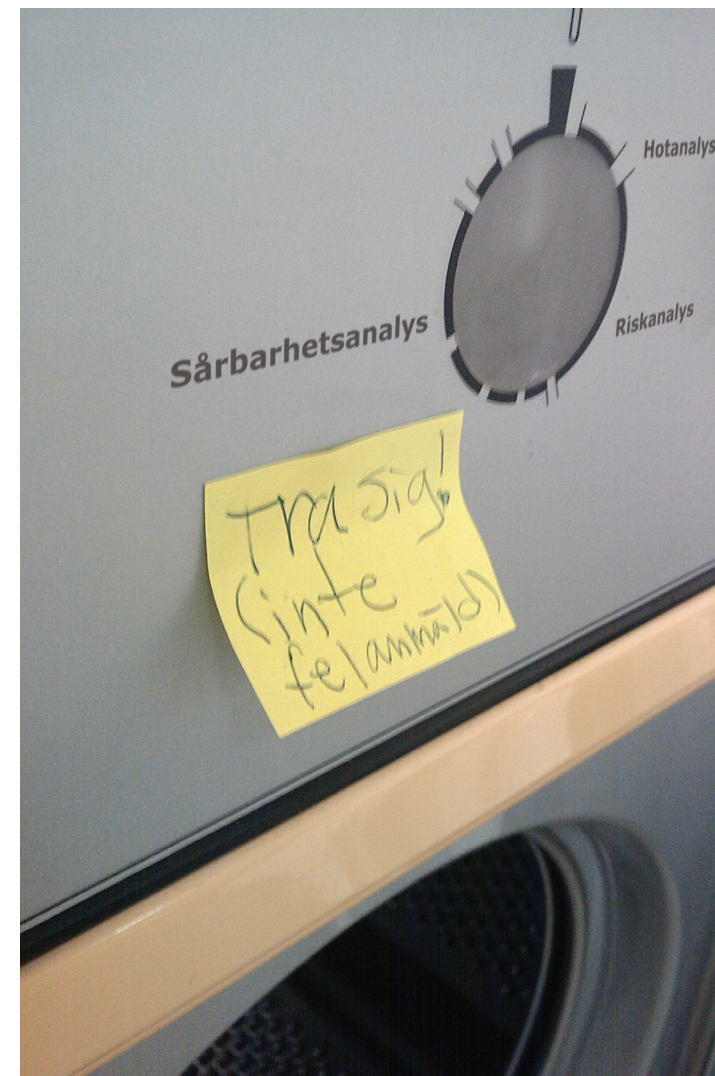




Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten

JOHAN BENGTTSSON, KRISTOFFER LUNDHOLM,
JONAS HALLBERG



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



FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

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

www.foi.se

FOI-R--3452--SE
ISSN 1650-1942

Juni 2012

Johan Bengtsson, Kristoffer Lundholm,
Jonas Hallberg

Behov av stöd vid genomförande av hot-, risk- och sårbarhets- analyser för IT-system inom Försvarmakten

Titel	Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten
Title	Need for support during threat, risk and vulnerability analysis of IT systems in the Swedish Armed Forces
Rapportnr/Report no	FOI-R--3452--SE
Månad/Month	Juni/June
Utgivningsår/Year	2012
Antal sidor/Pages	18
ISSN	1650-1942
Kund/Customer	Försvarsmakten
FoT område	Ledning och MSI
Projektnr/Project no	E36017
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk. All form av kopiering, översättning eller bearbetning utan medgivande är förbjuden

This work is protected under the Act on Copyright in Literary and Artistic Works (SFS 1960:729). Any form of reproduction, translation or modification without permission is prohibited.

Sammanfattning

Målet med projektet *Effektivare hot-, risk- och sårbarhetsanalyser* är att identifiera hur arbetet med dessa analyser kan effektiviseras som ett led i att snabba upp processen för auktorisation och ackreditering av IT-system. Det första steget i detta arbete är att identifiera vilka områden som är i behov av förändring. Detta görs med hjälp av en behovsanalys där de olika intressenternas behov sammanställs och analyseras.

Under 2011 genomfördes en behovsanalys avseende metod- och verktygsstöd vid genomförandet av de hot-, risk- och sårbarhetsanalyser som genomförs vid framtagandet av säkerhetsmålsättningen för Försvarmaktens IT-system. Denna rapport presenterar en kompletterad version av den tidigare analysen. Den nya versionen innehåller 32 behov indelade i fem kategorier. De flesta behoven kan härledas till flera olika källor. Det behov som uttalades av flest källor (9 av 10) var *behov av instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram*. De befintliga instruktionerna är bristfälliga avseende beskrivning av *hur* de efterfrågade analysresultaten ska tas fram samt vilken omfattning de framtagna analysresultaten förväntas ha.

Behov av kunskap om den verksamhet som IT-systemet ska stödja samt *Behov av egen personal inom Försvarmakten som har tid för och kompetens att genomföra analyserna* är också behov som lyftes fram av flertalet (8 respektive 7 av 10) av källorna. Att hot-, risk- och sårbarhetsanalyserna ofta genomförs av externa parter kan vara en anledning till den uttalade brist på förståelse för den verksamhet som IT-systemet ska stödja.

Alla de identifierade behoven kommer att ligga till grund för vidare arbete inom projektet med att ta fram lösningsförslag och därefter implementera demonstratorer och konceptverktyg för ett urval av dessa förslag.

Nyckelord: Hotanalys, riskanalys, sårbarhetsanalys, behovsanalys, IT-system, auktorisation, ackreditering

Summary

The goal of the project *Improved threat, risk and vulnerability analysis* is to identify how these analyzes can be rationalized as part of an effort to speed up the process for accreditation of IT systems. The first step is to identify which areas are in need of improvement. This is done through a needs analysis where the different stakeholder's needs are compiled and analyzed.

In 2011, a needs analysis was conducted. The analysis focused on method and tool support for threat, risk and vulnerability analysis undertaken in the development of the security objectives of the Armed Forces' IT systems. This report presents a revision of the earlier analysis. The revision resulted in 32 needs divided into five categories. The identified needs will be used as a basis for further work on designing and implementing demonstrators and conceptual tools.

Keywords: Threat analysis, risk analysis, vulnerability analysis, needs analysis, information system, accreditation

Innehåll

1	Inledning	7
1.1	Syfte	7
1.2	Bidrag	8
1.3	Målgrupp	8
1.4	Rapportstruktur.....	8
2	Bakgrund	9
3	Komplettering av behovsanalys	10
3.1	Genomförande	10
3.2	Resultat	10
4	Diskussion	13
Bilaga A	Identifierade behov	17

1 Inledning

En effektivisering av Försvarmaktens process för auktorisation och ackreditering av IT-system skulle ge väsentliga fördelar, bl.a. avseende säkerhet och kostnadseffektivitet. Om processen är mindre tidskrävande ökar chansen att ordentliga analyser genomförs för planerade IT-system. Med bättre underlag från hot-, risk- och sårbarhetsanalyserna finns förutsättningar för en större medvetenhet i risktagandet avseende systemen samt att den senare framtagna designen motsvarar de faktiska säkerhetskraven.

Auktorisations- och ackrediteringsprocessen består av flera delmoment varav ett är genomförandet av hot-, risk- och sårbarhetsanalyser. I dagsläget genomförs inte dessa analyser på ett enhetligt sätt. En av anledningarna till detta är att det saknas tydliga instruktioner för *hur* analysresultaten ska tas fram. Ett sätt att tydliggöra hur analysresultaten ska tas fram är att tillhandahålla metod- och verktygsstöd.

En förutsättning för att metod- och verktygsstöd ska vara relevanta är att de motsvarar de behov som finns i verksamheten. Detta kan uppnås genom att basera utvecklingen på en behovsanalys, vilken syftar till att identifiera, sammanställa och prioritera de behov som finns hos berörda delar i en verksamhet. Behovsanalyser ska identifiera aktiviteter eller resurser som är nödvändiga för att olika aktörer ska kunna genomföra sina uppgifter och uppnå uppsatta mål.

I sammanhanget hot-, risk- och sårbarhetsanalyser syftar behovsanalysen till att

- identifiera behov hos de aktörer som ska genomföra hot-, risk- och sårbarhetsanalyser
- identifiera behov hos de aktörer som ska nyttja resultaten från hot-, risk- och sårbarhetsanalyserna.

1.1 Syfte

Syftet med denna rapport är att beskriva den komplettering som gjorts av den tidigare behovsanalysen avseende metod- och verktygsstöd vid genomförandet av de hot-, risk- och sårbarhetsanalyser som genomförs vid framtagandet av säkerhetsmålsättningen för Försvarmaktens IT-system. Kompletteringen syftar till att:

- bekräfta de tidigare identifierade behoven
- identifiera kompletterande behov
- förbättra presentationen av de identifierade behoven.

1.2 Bidrag

Resultaten i denna rapport ger en sammanställning av de behov som finns inom Försvarmakten avseende metod- och verktygsstöd vid genomförandet av hot-, risk- och sårbarhetsanalyser för IT-system. De behov som har identifierats kommer att ligga till grund för vidare arbete med att ta fram lösningsförslag, vilka kommer att presenteras i en FOI-rapport under kvartal fyra 2012. Under 2013 kommer demonstratorer och konceptverktyg att utvecklas för att visa hur Försvarmaktens framtida metodstöd skulle kunna se ut.

1.3 Målgrupp

Målgruppen för denna rapport är personer som jobbar med hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarmakten. Rapporten syftar främst till att presentera de resultat som uppnåtts och diskutera dessa snarare än att beskriva den metodik och de tillvägagångssätt som nyttjats. Målet är att på ett enkelt och tydligt sätt presentera resultaten av den genomförda behovsanalysen.

1.4 Rapportstruktur

Återstående del av rapporten inleds med kapitel 2 som ger en kort beskrivning till bakgrunden till projektet samt tidigare resultat. Kapitel 3 beskriver kompletteringen av behovsanalysen samt resultaten från denna. Avslutningsvis förs i kapitel 4 en diskussion om resultaten från behovsanalysen.

2 Bakgrund

Denna rapport är skriven inom ramen för projektet *Effektivare hot-, risk- och sårbarhetsanalyser* som är den del i Försvarsmaktens beställning inom *Forskning och Teknikutveckling* (FoT). Projektet löper över tre år från 2011 till och med 2013.

Inom ramen för projektet genomfördes under 2011 en behovsanalys för att identifiera de behov som finns inom Försvarsmakten avseende genomförandet av hot-, risk- och sårbarhetsanalyser. Behovsanalysen fokuserade på de hot-, risk- och sårbarhetsanalyser som genomförs som en del i framtagandet av säkerhetsmålsättning för IT-system i enlighet med Försvarsmaktens IT-livscykelmodell.

Behovsanalysen utgick från Försvarsmaktens tillgängliga dokumentation samt sju intervjuer. De personer som intervjuades kommer i kontakt med säkerhetsmålsättningen för IT-system antingen genom att delta i dess framtagande, som granskare eller som mottagare av analysresultaten.

Den genomförda behovsanalysen resulterade i 77 behov som var indelade i sex huvudkategorier och 17 underkategorier. Indelningen i kategorier gjordes för att ge en tydligare bild över behov av liknande karaktär. Arbetet med behovsanalysen samt den resulterande uppsättningen behov återfinns i sin helhet i FOI-rapporten¹ från 2011. Utifrån de mest uttalade behoven togs följande rekommendationer till Försvarsmakten fram:

- Utveckla kunskap om de faktorer som påverkar analyserna
- Ta fram tydliga instruktioner för hur analyserna ska genomföras
- Tillhandahåll relevant utbildning
- Ta fram stöd för nödvändiga bedömningar
- Fokusera analyserna på det specifika snarare än det generella
- Ta fram stöd för att avgöra verksamhetens krav på IT-säkerheten

¹ Hot-, risk- och sårbarhetsanalys - Grunden för IT-säkerhet inom Försvarsmakten (FOI-R--3349--SE)

3 Komplettering av behovsanalys

I detta kapitel presenteras kompletteringen av den behovsanalys som genomfördes under 2011 och presenterades i form av en FOI-rapport². Fokus för behovsanalysen är detsamma som 2011, det vill säga behov avseende metod- och verktygsstöd för genomförande av de hot-, risk- och sårbarhetsanalyser som görs vid framtagandet av en säkerhetsmålsättning för Försvarmaktens IT-system.

3.1 Genomförande

Kompletteringen av behovsanalysen skedde i två steg. Under det första steget utökades underlaget som den tidigare behovsanalysen baserats på. Det utökade underlaget bestod av två nya intervjuer samt anteckningar från den diskussion som hölls i samband med den seminariedag³ som genomfördes vid FM LS UtvC avseende forskning inom IT-säkerhet. Under intervjuerna gjordes anteckningar som sedan verifierades av de intervjuade. Utifrån anteckningarna från intervjuerna och diskussionen identifierades utsagor som sedan analyserades. Behovsanalysen resulterade i en ny uppsättning behov som slogs ihop med de behov som identifierades vid den första behovsanalysen.

I den första behovsanalysen framkom det att hot-, risk- och sårbarhetsanalysen oftast ses som en analys snarare än tre separata analyser. Med anledning av detta genomfördes steg två av kompletteringen som innebar att de identifierade behoven strukturerades om genom att kategorierna som representerade de tre stegen i hot-, risk- och sårbarhetsanalysen slogs ihop till en kategori. Därigenom försvann en nivå i behovsstrukturen och kategorierna i den nya strukturen består huvudsakligen av underkategorier från den tidigare behovsstrukturen. Vissa av dessa underkategorier har slagits samman då det fanns överlapp mellan de ingående behoven. Omstruktureringen av behoven ledde till en enklare struktur och att ett flertal behov som tidigare återfanns i olika kategorier kunde slås ihop.

3.2 Resultat

Kompletteringen av behovsanalysen resulterade i en enklare struktur med färre, men mer omfattande behov. Antalet behov minskade från 77 till 32 stycken. Sex av de 32 behoven är nya behov som identifierats från det utökade underlaget.

² Hot-, risk- och sårbarhetsanalys - Grunden för IT-säkerhet inom Försvarmakten (FOI-R--3349--SE)

³ Seminariedag 2011 - Diskussion angående genomförandet av hot-, risk- och sårbarhetsanalyser för IT-system (FOI MEMO 3885)

Den nya uppsättningen behov har delats in i följande fem kategorier: *organisatoriska förutsättningar*, *tillvägagångssätt*, *kunskap*, *stöd vid bedömningar* och *analysresultat*.

- **Organisatoriska förutsättningar**
Kategorin *organisatoriska förutsättningar* innehåller behov som berör organisationens syn på genomförandet av analyserna samt tillgång till de resurser som behövs för genomförandet.
- **Tillvägagångssätt**
Kategorin *tillvägagångssätt* innehåller de behov som huvudsakligen rör metoder, instruktioner och arbetssätt vid genomförandet av analyserna. I denna kategori återfinns således de behov som är kopplade till *hur* analyserna ska genomföras.
- **Kunskap**
Kategorin *kunskap* innehåller de behov som beskriver olika typer av kunskap som anses vara nödvändig för genomförandet av analyserna.
- **Stöd vid bedömningar**
Kategorin *stöd vid bedömningar* innehåller behov som huvudsakligen påtalar olika typer av stöd som anses nödvändiga att ha tillgång till vid genomförande av analyserna.
- **Analysresultat**
Slutligen innehåller kategorin *analysresultat* behov som beskriver vilka egenskaper analysresultatet behöver ha för att vara användbart för mottagaren.

Kompletteringen av behovsanalysen resulterade i att ett flertal behov bekräftades av ytterligare källor. Utöver detta identifierades totalt sex nya behov:

- behov av att de antaganden och bedömningar som görs under analysarbetet motiveras
- behov av att icke avsiktliga hot beaktas vid genomförandet av hotanalysen
- behov av att representanter från alla berörda delar av organisationen deltar i analysarbetet
- behov av engagemang och intresse från ledningen
- behov av instruktioner och arbetssätt som stämmer överens med varandra
- behov av vetenskaplig förankring av de antaganden och bedömningar som görs under analysarbetet.

Underlaget för behovsanalysen är, som nämnts tidigare, tio olika källor (nio intervjuer och anteckningar från en diskussion). Merparten av de identifierade behoven kan härledas till fler än en källa. En lista över alla identifierade behov återfinns i Bilaga A. Nedan återges de fem oftast uttalade behoven, med andelen källor som behovet kan härledas inom parenteser.

1. Behov av instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram. (9 av 10)
2. Behov av kunskap om den verksamhet som IT-systemet ska stödja. (8 av 10)
3. Behov av egen personal inom Försvarmakten som har tid och kompetens att genomföra analyserna. (7 av 10)
4. Behov av stöd för att bedöma sannolikhet för realisering av hot. (6 av 10)
5. Behov av stöd för att bedöma konsekvens vid realisering av hot. (6 av 10)

4 Diskussion

En förutsättning för ett väl fungerande hot-, risk- och sårbarhetsanalysarbete är att det finns erforderligt stöd vid genomförandet. Ett adekvat stöd möjliggör analysresultat av den omfattning och kvalitet som krävs för att det planerade IT-systemet ska kunna bedömas. För att kartlägga vilket stöd som krävs för att kunna genomföra de aktuella arbetsuppgifterna genomfördes en behovsanalys.

Behovsanalysen utgår från Försvarmaktens tillgängliga dokumentation samt nio intervjuer och en diskussion med personer som i sin tjänst kommer i kontakt med säkerhetsmålsättningen. Genom att intervjua personer med relation till olika delar av auktorisations- och ackrediteringsprocessen erhålls en samlad behovsbild utgående från de olika perspektiven.

Denna reviderade version av behovsanalysen baseras på ett större underlag jämfört med den tidigare analysen⁴. Även struktureringen av behov har förbättrats för att ge en enklare och tydligare bild över vilka behov som finns och inom vilka områden. Strukturering av behov kan göras på många olika sätt. Den valda strukturen fokuserar på att tydliggöra inom vilket område ett behov återfinns snarare än att fokusera på för vilka roller det är ett behov. Detta ger en samlad bild av Försvarmaktens behov av stöd vid genomförandet av hot-, risk- och sårbarhetsanalyser för IT-system.

På en övergripande nivå är bilden av vilket stöd som behövs relativt likartad i de olika delarna av Försvarmakten. Flertalet av de personer som intervjuades är medvetna om vilka problem som finns vid genomförandet av deras arbetsuppgifter, och har ofta även idéer på hur problemen skulle kunna lösas, men det behövs tid, resurser och beslut för att kunna genomföra förändringar.

Det är inte nödvändigtvis auktorisations- och ackrediteringsprocessen i sig som är det som ses som problemet, istället ses avsaknaden av stöd för *hur* de efterfrågade underlagen ska tas fram som det största problemet. Det befintliga stödet beskriver oftast *vad* som ska tas fram men inte *hur* detta kan göras. Detta leder till problem både för de som genomför analyserna och för de som ska granska analysresultaten.

Ett problem som dock relaterar till auktorisations- och ackrediteringsprocessen är att arbetet i processen påbörjas allt för sent. Detta får till följd att ett IT-system redan kan vara under utveckling, eller i vissa fall till och med redan färdigt, när processen befinner sig i behovsberedningen inför auktorisationsbeslut B1. På så sätt missas ett av de centrala syftena med processen, vilket är att säkerställa att det finns behov av ett nytt IT-system innan framtagningen påbörjas. Vidare i

⁴ Hot-, risk- och sårbarhetsanalys - Grunden för IT-säkerhet inom Försvarmakten (FOI-R--3349--SE)

processen innebär det även att ett IT-system redan kan vara färdigutvecklat innan hot-, risk- och sårbarhetsanalysen genomförs inför auktorisationsbeslut B2. Detta innebär att utvecklingen har skett innan IT-säkerhetskraven har fastställts. Att göra stora förändringar i ett IT-system i efterhand är något som kan vara både dyrt och tidskrävande.

Något som nämndes vid flertalet intervjuer var svårigheten att avgöra lämplig omfattning på analysarbetet. Detta leder till säkerhetsmålsättningar av antingen bristfällig eller, för ändamålet, onödigt stor omfattning. Resultatet blir i slutändan att processen riskerar att ta onödigt lång tid då det i ena fallet kan krävas omarbetningar av underlaget och i det andra fallet krävs mycket tid för att granska underlaget.

Det lyfts fram som viktigt att de som genomför hot-, risk- och sårbarhetsanalyserna har kunskap om och förståelse för den verksamhet som det tänkta IT-systemet ska stödja. Avsaknad av förståelse för verksamheten kan leda till bristfälliga analyser och i slutändan även system som inte motsvarar verksamhetens behov.

Att Försvarmakten har egen personal som har både tid och resurser för att kunna genomföra analysarbetet är något som många anser behövs. I dagsläget är det vanligt att analysarbetet genomförs av externa parter, vilket kan vara något som påverkar förståelsen för den verksamhet som ska stödjas. Även svårigheter med att göra bedömningar avseende sannolikhet och konsekvens av realiserade hot är något som lyfts fram. Bristande förståelse för verksamheten kan vara en av anledningarna även när det gäller svårigheten att göra dessa bedömningar.

Om analyserna skulle genomföras av Försvarmaktens egen personal behöver det inte per automatik innebära bättre analysresultat. Den grupp av personer som genomför analyserna måste innehålla personer med förståelse för verksamheten, personer med kunskap om IT-säkerhet samt personer med metodkunskap avseende analyserna.

Ett av problemen i dagsläget avseende metodkunskap är att det varierar kraftigt vilka analysmetoder som används. Att tillvägagångssätten skiljer sig åt kan bero på den tidigare beskrivna bristen av beskrivningar av *hur* analysarbetet kan genomföras. Ett annat problem är bristen på deltagande från personer med kunskap om verksamheten. Bristen på deltagande beror inte nödvändigtvis på bristande intresse utan snarare på avsaknad av tilldelad tid och resurser för att kunna delta.

Inom vissa delar av verksamheten ses dock hela auktorisations- och ackrediteringsprocessen mest som ett hinder på vägen. Detta kan delvis bero på avsaknad av förståelse för den aktuella hotbilden mot Försvarmakten och den verksamhet som bedrivs. Det kan vara nödvändigt för Försvarmakten att sprida kunskap internt om den aktuella hotbilden och på så sätt visa varför auktorisation

och ackreditering av IT-system är nödvändigt. För att uppnå ett effektivare arbete med auktorisation och ackreditering av Försvarmaktens IT-system räcker det inte att enbart förmedla till personalen *vad* som ska göras. Det är även nödvändigt att förmedla *hur* det ska göras och *varför*.

Bilaga A Identifierade behov

I denna bilaga presenteras resultatet från den genomförda behovsanalysen. Behoven är indelade i fem kategorier. Inom kategorierna återges behoven utan inbördes ordning. De har dock numrerats för att underlätta referenser till specifika behov.

Organisatoriska förutsättningar

- 1) Förståelse för varför analyserna genomförs
- 2) Att koordinera analyser för olika IT-system mellan vilka det finns beroenden
- 3) Att integrera analyserna med motsvarande analyser som görs för system- och personsäkerhet
- 4) Egen personal inom Försvarmakten som har tid och kompetens att genomföra analyserna
- 5) Att representanter från alla berörda delar av organisationen deltar i analysarbetet
- 6) Engagemang och intresse från ledningen

Tillvägagångssätt

- 7) Ett arbetssätt som beaktar de hot som är specifika för aktuellt IT-system
- 8) Att analysarbetet genomförs enligt fastställda metoder
- 9) Ett arbetssätt som kan anpassas så att det står i proportion till IT-systemets omfattning
- 10) Instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram
- 11) Instruktioner och arbetssätt som stämmer överens med varandra
- 12) Arbetssätt som tillvaratar tillgänglig information om det planerade IT-systemet
- 13) Att de antaganden och bedömningar som görs under analysarbetet motiveras
- 14) Att icke avsiktliga hot beaktas vid genomförandet av hotanalysen
- 15) Att genomföra analyserna innan förslag på realisering av IT-systemet tas fram

Kunskap

- 16) Kunskap om den verksamhet som IT-systemet ska stödja
- 17) Kunskap om den information som IT-systemet ska hantera

- 18) Kunskap om de analysmetoder som ska användas
- 19) Kunskap om de säkerhetslösningar som används av befintliga IT-system
- 20) Kunskap om det planerade systemet
- 21) Kunskap om IT-säkerhet
- 22) Kunskap om hur ett IT-system påverkas av den omgivning i vilken det ska verka

Stöd vid bedömningar

- 23) Stöd för att avgöra hur implementationen av föreslagna säkerhetskrav påverkar identifierade risker
- 24) En fastslagen hotlista som kan användas som utgångspunkt vid genomförande av analyserna
- 25) Dialog med systemarkitekter och systemutvecklare vid formulering av säkerhetskrav
- 26) Stöd för att bedöma nödvändig omfattning hos analyserna
- 27) Stöd för att bedöma sannolikhet för realisering av hot
- 28) Stöd för att bedöma konsekvens vid realisering av hot

Analysresultat

- 29) Spårbarhet för de antaganden som görs under analyserna
- 30) Analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras
- 31) Att analysarbetet påverkar de krav som ställs på det planerade IT-systemet
- 32) Analysresultat som visar vilka risker som kommer att tas vid användning av det planerade IT-systemet

