# Tester av metoder för värdering av informationssäkerhet

JOHAN BENGTSSON, JONAS HALLBERG,
AMUND HUNSTAD, KRISTOFFER LUNDHOLM

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

FOI
Totalförsvarets forskningsinstitut
Ledningssystem
Box 1165
581 11 Linköping

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

www.foi.se

FOI-R--2901--SE
ISSN 1650-1942

Vetenskaplig rapport
December 2009

**Ledningssystem**

Johan Bengtsson, Jonas Hallberg,
Amund Hunstad, Kristoffer Lundholm

# Tester av metoder för värdering av informationssäkerhet

| | |
|---|---|
| Titel | Tester av metoder för värdering av informationssäkerhet |
| Title | Tests of methods for information security assessment |
| Rapportnr/Report no | FOI-R--2901--SE |
| Rapporttyp<br>Report Type | Vetenskaplig rapport |
| Månad/Month | December |
| Utgivningsår/Year | 2009 |
| Antal sidor/Pages | 68 p |
| ISSN | ISSN 1650-1942 |
| Kund/Customer | Försvarsmakten |
| Kompetenskloss | 26 IT-säkerhet |
| Extra kompetenskloss | |
| Projektnr/Project no | E53077 |
| 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

För rationell styrning av arbetet med informationssäkerheten är det nödvändigt att bygga upp kunskap om vilka faktorer som påverkar informationssäkerhet. Ett redskap för att bygga upp nödvändig kunskap är metoder för värdering av informationssäkerhet. Dessa metoder syftar till att klargöra vilken nivå informationssäkerheten har.

I denna rapport undersöks vilket metodstöd som för närvarande finns tillgängligt för värdering av IT-säkerhet. Det arbete som redovisas inkluderar en litteraturstudie för att identifiera intressanta metoder för värdering av IT-säkerhet samt testning av ett urval av dessa.

Litteraturstudien identifierade 25 metoder som ansågs relevanta att testa. Av dessa 25 metoder testades 7 under detta arbete. Resultaten från testerna visar att inga av dessa metoder är relevanta för Försvarsmakten. En slutsats av detta är att det krävs mer specifika beskrivningar av de situationer där värderingsbehov uppstår för att kunna testa metoder mer utförligt.

Nyckelord: informationssäkerhet, IT-säkerhet, värdering, testning

## Summary

In order to manage information security, it is essential to accumulate knowledge on information security. An aid in this task is presented by methods for the assessment of information security. The purpose of these methods is to reveal the levels of information security provided by the assessed systems.

In this report, methods currently available for IT security assessment are characterized. The presented effort includes a literature study performed in order to identify relevant methods and tests performed to reveal the characteristics of a selection of the relevant methods.

The literature study revealed 25 methods considered to fulfill the stated prerequisites for testing. Seven of the 25 identified methods were tested. The test results illustrate that none of the tested methods are relevant for the Swedish Armed Forces. One conclusion is that more specific descriptions, of when needs of security assessment occur, are needed in order to test the methods more thoroughly.


Keywords: information security, IT security, assessment, testing

# Innehåll

# 1 Inledning

Informationssäkerhet är ett omfattande område. Att hantera informations säkerhet, det vill säga att upprätthålla dess konfidentialitet, riktighet och tillgänglighet är en krävande uppgift för alla stora organisationer. Förutom organisationers storlek och komplexiteten hos deras information finns det fler faktorer vilka komplicerar uppgiften. Den första är att den utbredda användningen av datorbaserade informationssystem (IT-system) gör informationen mycket lättflyktig. Därmed kan påverkan på de tre eftersträvade informationssäkerhetsegenskaperna ske mycket snabbt samt vara svår att upptäcka och motverka. Vidare har det visat sig vara svårt att klart definiera vad informationssäkerhet utgörs av, förutom i form av andra generella egenskaper vilkas underliggande faktorer i sin tur är svåra att fastställa. Ett relaterat problem är att säkerhet inte är direkt mätbart, utan måste värderas utifrån andra mätbara fenomen. Detta resulterar i att säkerhet vore svårt att mäta, även om definitionen av informationssäkerhet vore helt klar. Därmed finns behov av strukturerade metoder för värdering av informationssäkerhet.

## 1.1 Problemformulering

Strukturerad värdering av informationssäkerhet som ger kvantitativa resultat är en utmanande uppgift. Samtidigt ökar beroendet av hög informationssäkerhet, vilket inkluderar IT-säkerhet. Därmed ter det sig naturligt att undersöka och beskriva vilka egenskaper metoder för värdering av informationssäkerhet har samt utröna huruvida dessa metoder motsvarar befintliga behov. Då denna rapport är ett resultat av arbete inom ramen för Försvarsmaktens forskning och teknikutveckling (FoT), adresseras Försvarsmaktens behov. Arbetet syftar till att besvara följande frågeställningar.

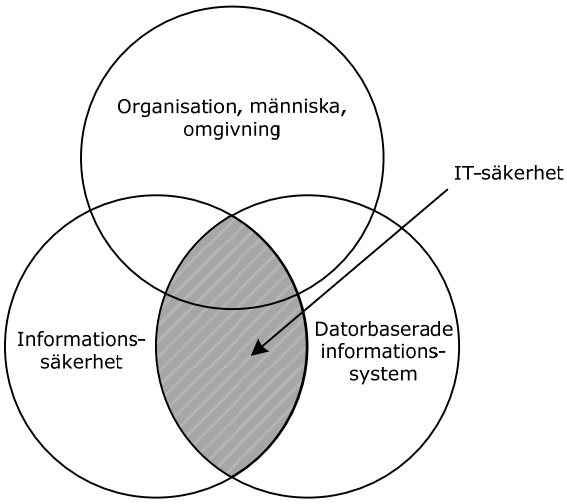
- Hur väl kan dagens värderingsmetoder stödja Försvarsmaktens behov?
- Är det möjligt att på ett formaliserat sätt utvärdera vilka värderingsmetoder som motsvarar specifika behov?

## 1.2 Avgränsning

För att fokusera arbetet som beskrivs i denna rapport gjordes avgränsningar avseende vilka egenskaper som ska värderas samt vilka behov genomförda värderingar ska adressera.

Då allt större del av informationshanteringen sker med hjälp av datorbaserade informationssystem, begränsades studien till skärningen mellan *informationssäkerhet* och *datorbaserade informationssystem*, det vill säga *IT-säkerhet*. Skärningen mellan *informationssäkerhet*, *datorbaserade*

*informationssystem* samt *organisation, människa och omgivning* ingår dock. IT-säkerhet begränsas således inte till tekniska frågor utan inkluderar också organisationers, människors och omgivningens påverkan på datorbaserade informationssystem (Figur 1).




Figur 1: Illustration av begreppet IT-säkerhet.

För att utröna huruvida olika metoder för värdering av IT-säkerhet adresserar existerande behov av värdering måste de aktuella behoven vara kända. När metoder testas utan specifika användningsfall i åtanke, blir behoven oprecisa. Då detta arbete inte baseras på specifika användningsfall, har en modell av IT-systems livscykler använts för att precisera behoven. Därmed blir behoven mindre allmänna än om de hade härletts från generella behov avseende värdering av IT-säkerhet. I detta syfte har Försvarsmaktens IT-livscykelmodell nyttjats (Försvarsmakten, 2004).

## 1.3 Bidrag

Det arbete som redovisas i denna rapport inkluderar:

- en litteraturstudie för att identifiera intressanta IT-säkerhetsvärderingsmetoder,
- utvärdering av en delmängd av de i litteraturstudien identifierade metoderna samt
- specificering av det värderingsstöd som de utvärderade metoderna erbjuder under de olika stegen i Försvarsmaktens IT-livscykelmodell.

# 2 Bakgrund

Denna rapport förutsätter att läsaren har en viss grundkunskap inom området IT-säkerhet. Då begreppsanvändningen inom området i vissa avseenden är otydlig inleds detta kapitel med ett avsnitt avseende begreppsanvändningen i denna rapport. Därefter beskrivs den procedur för testning av värderingsmetoder som används i rapporten samt Försvarsmaktens IT-livscykelmodell.

## 2.1 Begreppsanvändning

I detta avsnitt beskrivs hur vissa begrepp används i denna rapport. För att underlätta uppslagning återges termerna i alfabetisk ordning. Eventuella kortformer redovisas inom parenteser.

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

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

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

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

**IT-system** avser system med teknik som hanterar och utbyter information med omgivningen (Försvarsmakten, 2006).

**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, exempelvis hanteringen av lösenord, även om dessa aktiviteter och rutiner i sig inte ingår i IT-systemet.

**IT-säkerhetsegenskaper** (säkerhetsegenskaper) är de egenskaper som påverkar IT-säkerhetsnivåer i system. Termen **relevanta IT-säkerhetsegenskaper** används för de egenskaper som används för att beskriva IT-säkerheten i system. Om, exempelvis, konfidentialitet, riktighet och tillgänglighet är de egenskaper

som ska användas för att beskriva ett IT-systems säkerhet, utgör dessa tre de relevanta IT-säkerhetsegenskaperna för den aktuella värderingen.

**IT-säkerhetsvärdering** (säkerhetsvärdering) är en aktivitet som syftar till att öka kunskapen om IT-säkerheten hos system, detta genom att fastställa IT-säkerhetsvärden för relevanta IT-säkerhetsegenskaper.

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

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

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

**Risk** utgörs av oönskade händelser med negativa konsekvenser och beskrivs som en ”kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad” (SIS, 2007).

## 2.2 Procedur för test av värderingsmetoder

Att ta fram metoder för värdering av säkerhet är kostsamt. Därför är det en fördel när tidigare utvecklade metoder kan användas. Som ett stöd för analys av metoder för värdering av IT-säkerhet har proceduren *Test of Security Assessment Relevance and validity*, TSAR, utvecklats. Syftet med TSAR är att stödja strukturerade analyser av värderingsmetoder. Dessa analyser ska vara okomplicerade och kräva lite resurser samt ge resultat som kan nyttjas för att jämföra olika metoder. Vidare ska resultaten kunna utgöra underlag för mer djuplodande analyser.

Testning med TSAR resulterar i kvalitetsvärden. Dessa värden indikerar i vilken grad säkerhetsvärderingsmetoder uppfyller de generella kvaliteterna *relevans* och *validitet*. Det vill säga hur väl lämpade olika värderingsmetoder är för en specifik situation samt hur väl de erhållna säkerhetsvärdena återspeglar verkligheten. För att kunna avgöra till vilken grad de två kvaliteterna är uppfyllda görs mätningar av en mängd definierade egenskaper. Dessa egenskaper finns definierade i de så kallade TSAR-tabellerna, som tagits fram i samband med utvecklingen av TSAR-proceduren. I dessa tabeller finns en mängd mätbara egenskaper definierade som har att göra med kvaliteterna relevans och validitet.

Proceduren är framtagen inom forskningsprojektet *Testning av metoder och verktyg för värdering av informationssäkerhet*. Den första versionen av TSAR beskrivs i rapporten *The TSAR procedure – Test of Security Assessment Relevance and validity* (Bengtsson, J. Hallberg, Hunstad, & Löfvenberg, 2008). Under 2009 har TSAR utvecklats vidare. De nya och uppdaterade egenskaperna i

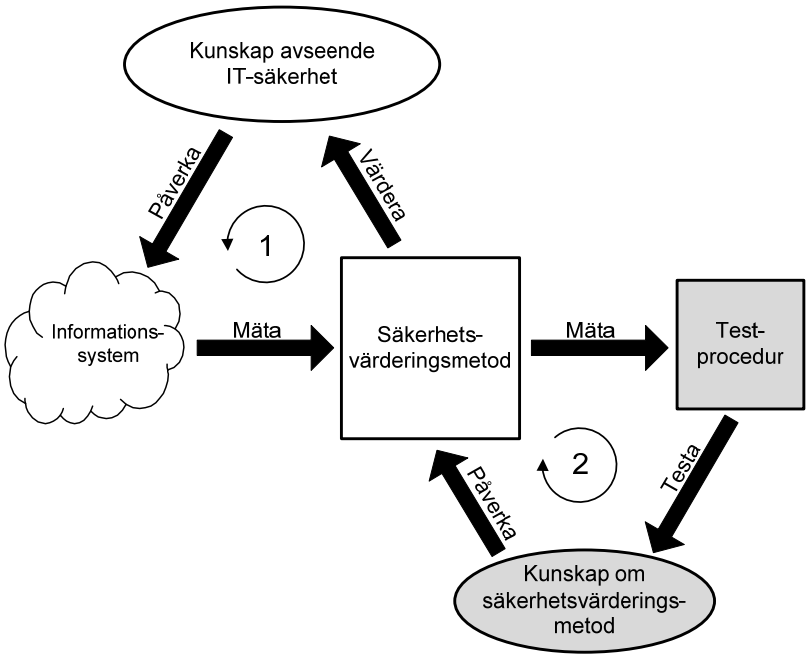
TSAR-tabellerna återfinns i bilaga A. I återstoden av detta avsnitt beskrivs relationen mellan metoder för säkerhetsvärdering och testprocedurer, såsom TSAR, samt genomförandet av ett test, så som det genomförs med senaste versionen av TSAR.

### 2.2.1 Relation mellan säkerhetsvärdering och testning

Säkerhetsvärdering är nödvändigt för att skaffa kunskap om säkerheten i informationssystem. Denna kunskap behövs för att kunna justera säkerhet så att en bra riskbalansering erhålls. Det vill säga att säkerhetsvärdering ger den återkoppling som krävs för att kunna reglera säkerheten.

Testning av värderingsmetoder är nödvändigt för att erhålla kunskap om de metoder som används för att värdera säkerheten. Denna kunskap behövs för att välja och anpassa värderingsmetoder så att de ger den kunskap om säkerhet som behövs. Det vill säga testning ger den återkoppling som krävs för att kunna styra värderingsmetoderna.

Värdering och testning resulterar därmed i två återkopplingar. I det första fallet är det informationssystemet och i det andra fallet är det värderingsmetoden som ska påverkas för att önskade resultat ska erhållas (Figur 2).




Figur 2: Samband mellan säkerhetsvärderingsmetod och testprocedur.

### 2.2.2 Genomförande av TSAR test

Testet är indelat i fem aktiviteter med två typer av aktörer – användare och testansvarig. Användare nyttjar testresultaten och är i behov av en värderingsmetod. Testansvarig är den som ser till att nödvändig testning av värderingsmetod genomförs. Den testansvarige kan ha behov av ytterligare expertis för att genomföra testet.

En förutsättning för genomförandet av ett test är användarbehoven, som utgör grunden för att kunna identifiera relevanta säkerhetsvärderingsmetoder. Användarbehoven kan, exempelvis, formuleras med naturligt språk eller som en checklista.

#### 2.2.2.1 Aktivitet 1 – Välj relevansattribut

De användarbehov avseende värdering som identifierades måste omvandlas till attribut. Med attribut avses de egenskaper hos en säkerhetsvärderingsmetod som ska mätas. Attributen väljs bland de relevansrelaterade egenskaperna i TSAR-tabellerna. Denna aktivitet utförs av den testansvarige i samarbete med användaren för att säkerställa att omvandlingen återspeglar de identifierade användarbehoven. Aktiviteten resulterar i en uppsättning relevansrelaterade attribut.

#### 2.2.2.2 Aktivitet 2 – Tilldela vikter till relevansattribut

Eftersom de olika relevansattributen oftast inte är av samma betydelse för användaren tilldelas de vikter. Tilldelningen av vikter genomförs gemensamt av användaren och den testansvarige. Baserat på de tilldelade vikterna beräknas en viktvektor för de relevansrelaterade attributen. Fler olika metoder kan användas för att tilldela vikter och beräkna viktvektorn.

I denna rapport används en relativt enkel metod, som går till så att attributen delas in i två ungefär lika stora grupper. Attributen i den första gruppen anses ha en högre prioritet än attributen i den andra gruppen. Summan N beräknas som antalet attribut i gruppen med lägre prioritet plus två gånger antalet attribut i gruppen med högre prioritet. Vikterna för de olika attributen blir slutligen 1/N för attributen med lägre prioritet och 2/N för attributen med högre prioritet.

#### 2.2.2.3 Aktivitet 3 – Mätning av attribut

Den testansvarige modellerar säkerhetsvärderingsmetoden genom att mäta de relevansrelaterade attributen, som valdes i aktivitet 2, och de validitetsrelaterade attributen, som är fördefinierade i TSAR. Mätningen genomförs genom att

attributen tilldelas värdet 0 eller 1. Ett attribut som anses uppfyllt på ett tillfredställande sätt ges värdet 1, medan ett attribut som inte anses uppfyllas i tillräcklig grad ges värdet 0. Detta resulterar i en vektor med attributvärden för var och en av kvaliteterna relevans och validitet.

I vissa fall är det inte möjligt att avgöra om en metod uppfyller ett givet attribut. För att hantera dessa fall innehåller TSAR konceptet *täckning*, som anger i vilken grad testet lyckas mäta uppfyllnaden av de olika attributen. För de attribut vars uppfyllnad kan avgöras sätts täckningsvärdet till 1. Om värdet för ett attribut inte kan fastställas, sätts det motsvarande täckningsvärdet till 0. Täckvärdena bildar ytterligare två vektorer – relevanstäckningsvektorn och validitetstäckningsvektorn.

De framtagna vektorerna utgör den modell av den testade säkerhets-värderingsmetoden som används i de följande aktiviteterna. Om några av attributen redan mätts i ett tidigare fortfarande giltigt test, med andra användarbehov, behöver de inte mätas om. De validitetsrelaterade attributen behöver inte mätas på nytt, eftersom användarbehoven inte påverkar validiteten hos en säkerhetsvärderingsmetod.

#### 2.2.2.4 Aktivitet 4 – Beräkna kvalitetsvärden

Beräkningen av kvalitetsvärden för relevans och validitet baseras på de framtagna vektorerna med attributvärden, täckningsvärden och vikter. Vektorn med relevansvärden multipliceras (inre produkt) med relevansattributens viktvektor, vilket ger ett skalärt relevansvärde. Beräkningen av det skalära validitetsvärdet görs på samma sätt. För att illustrera hur väl beskriven metoden är beräknas två täckningsgrader. En viktad täckningsgrad beräknas som summan av vikterna för de attribut som har kunnat bedömas. En procentuell täckningsgrad beräknas som andelen attribut som kunnat bedömas. För att kompensera för eventuella problem med att fastställa attributvärden beräknas alternativa relevans- och validitetsvärden baserat på den viktade täckningsgraden. Beräkningarna genomförs av den testansvarige.

#### 2.2.2.5 Aktivitet 5 – Tolka och diskutera resultatet

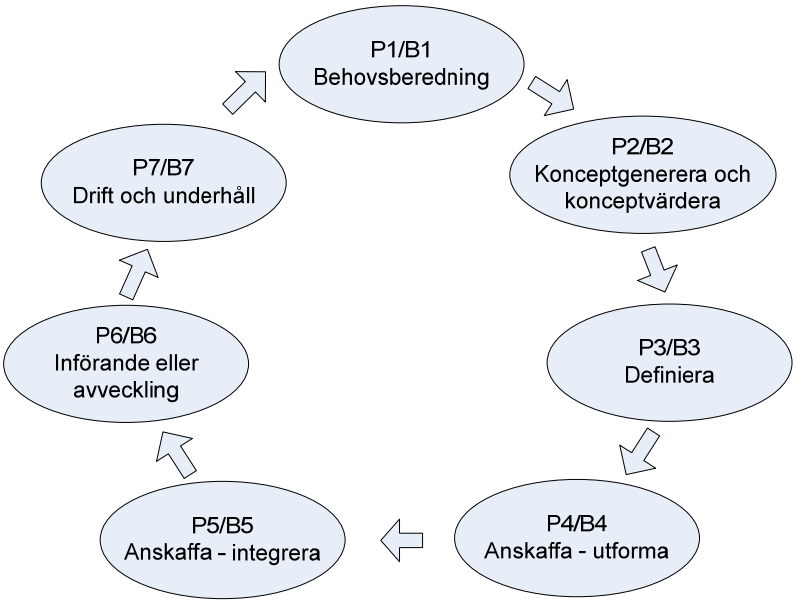
Efter genomfört test ska den testansvarige och användaren diskutera och utvärdera testresultatet. Genom att utvärdera de olika delarna av resultatet är det möjligt att säkerställa att anledningen till de satta attributvärdena och deras genomslag i de fortsatta beräkningarna blir tydliga. Under genomförandet av denna aktivitet kan det även beslutas om att test av andra säkerhetsvärderingsmetoder bör genomföras.

## 2.3 IT-livscykelmodell

I Försvarsmaktens IT-livscykelmodell utgör ackrediterings- och auktorisationsprocesserna två parallella spår. Auktorisation innebär ett bemyndigande att utveckla Försvarsmaktens IT-verksamhet, medan ackreditering utgör ett godkännande av ett IT-system ur säkerhetssynpunkt (Försvarsmakten, 2006).

En schematisk struktur för IT-livscykelmodellen återfinns i Figur 3. Auktorisationsprocessen återfinns under de tidigare stegen (fram till beslut B4), medan ackrediteringsprocessen löper genom hela livscykeln, men med tyngdpunkt vid stegen som leder fram till beslutspunkterna B5 och B6. Försvarsmaktens IT-livscykelmodell är för närvarande under omarbetning. Arbetet som beskrivs i denna rapport utgår dock från den, i nuläget, senast fastställda versionen från 2004. (Försvarsmakten, 2004, kap. 6)

I arbetet med att testa metoder för värdering av IT-säkerhet nyttjas Försvarsmaktens IT-livscykelmodell som en bas för att fastställa relevansattribut. Genom att fastställa en uppsättning relevansattribut för vart och ett av stegen P2 till P7 i livscykelmodellen erhålls relevansvärden för de testade metoderna för dessa steg. Därmed kan användare som är intresserade av olika steg i livscykeln nyttja motsvarande delar av de resultat som presenteras i denna rapport.




Figur 3: Försvarsmaktens IT-livscykelmodell.

# 3 Metod

De resultat som presenteras i denna rapport har tagits fram genom en litteraturstudie samt gruppering, urval och testning av metoder för värdering av IT-säkerhet. I detta kapitel beskrivs metoden för genomförandet av dessa steg. Resultaten samt detaljer avseende tillvägagångssättet återfinns i Kapitel 4 till 6.

## 3.1 Litteraturstudie

För att ta fram underlag för testningen genomfördes en litteraturstudie med syftet att hitta litteratur som beskriver metoder för att värdera IT-säkerhet.

Två frågor som behövde hanteras vid genomförandet av litteraturstudien var omfattningen av aktuell forskning och utveckling samt bristen på standardiserad begreppsanvändning inom området. Den oprecisa begreppsanvändningen gjorde det är svårt att sortera ut intressant litteratur ur den stora massan tillgängliga publikationer. För att hantera dessa frågor omfattade litteraturstudien tre aktiviteter.

- Sökningar i litteraturdatabaser genomfördes med en specificerad uppsättning termer.
- Genomgång av bidrag publicerade vid workshopar, där relevanta artiklar bedöms kunna ha presenterats.
- Ad hoc-sökningar genomfördes genom att tillfråga experter inom området. Även Google och Google Scholar nyttjades för att hitta underlag som inte har publicerats vetenskapligt.

För att kunna avgöra vilka träffar av dem som erhölls, som var intressanta gjordes en bedömning. För att en bedömning ska vara praktiskt möjlig att genomföra behöver den vara okomplicerad. Därför baserades bedömningen på en uppsättning allmänna krav som ska uppfyllas av intressanta metoder. Dessa krav formulerades innan litteraturstudien inleddes. Metoder kunde dock undantas från delmängder av dessa krav, om de ansågs presentera speciellt intressanta aspekter av värdering.

Resultatet av litteraturstudien sammanställdes i form av statistik avseende genomförda sökningar samt en lista med identifierade metoder som passerade den genomförda gallringen.

I de fall då den identifierade litteraturen inte var tillräcklig som underlag för testning av den aktuella metoden gjordes sökningar i databaser efter kompletterande litteratur. Sökningarna gjordes genom identifiering av litteratur

som refererar till det aktuella bidraget och genom att följa referenser från det aktuella bidraget.

## 3.2 Gruppering och urval av metoder

De identifierande metoderna grupperades för att återspegla de egenskaper som är mest framträdande. När flera metoder hade samlats i en grupp namngavs denna så att likheterna hos de ingående metoderna tydliggjordes. Efter grupperingen av de identifierade metoderna valdes en delmängd av dessa ut för att genomgå testning.

## 3.3 Testning av metoder

De prioriterade metoderna fördelades bland de personer som genomförde testningen. Varje metod, som genomgick testning, testades av en person. Den genomförda testningen granskades sedan av en annan testare.

Testningen genomfördes och dokumenterades enligt proceduren TSAR (Avsnitt 2.2). Ett avsteg från TSAR gjordes genom att de utvalda metoderna testades mot alla egenskaper som finns definierade i testproceduren, det vill säga relevansattributen utgörs av alla de egenskaper som finns med i TSAR-tabellerna. Detta för att samla in allt det underlag som behövdes för att ta fram relevansvärden för stegen P2 till P7 i Försvarsmaktens IT-livscykelmodell.

I samband med testet beskrevs metoderna enligt följande mall.

- Metodgrupp, det vill säga vilken kategori metoden associerades med vid grupperingen av metoder.
- Skalbarhet, det vill säga i vilken grad metoden anses vara användbar för omfattande system.
- Dokument, det vill säga vilket underlag som har använts vid testningen.
- Publiceringsdatum.
- Värderingsmål, det vill säga vilka resultat värderingen syftar till.
- Möjliga värderingsobjekt, det vill säga vilken typ av system som värderas.
- Översiktlig beskrivning av metoden.
- Kommentarer avseende de mätdata som testet har resulterat i.

## 3.4 Sammanställning av resultat

Efter att testningen av metoder hade slutförts sammanställdes resultaten genom att ta hänsyn till hur relevansattributen hade viktats för respektive steg i Försvarsmaktens IT-livscykelmodell. Två olika relevansvärden togs fram. Det första relevansvärdet utgörs av summan av vikterna för de attribut som metoden uppfyller. Det andra relevansvärdet utgörs av det första relevansvärdet adderat med summan av vikterna för de attribut som inte kunde bedömas. På så sätt erhölls det maximala relevansvärde som skulle kunna uppnås om alla attribut kunde bedömas.

# 4 Identifierade värderingsmetoder

Detta kapitel presenterar resultaten av litteraturstudien samt gruppering och urval av de i litteraturstudien identifierade metoderna.

## 4.1 Litteraturstudie

Litteraturstudien genomfördes enligt den metod som beskrivs i Kapitel 3. De urvalskriterier som legat till grund för vilka metoder som ansågs intressanta finns listade i Avsnitt 4.1.1. Resterande avsnitt presenterar tillvägagångssättet för att identifiera dessa metoder.

### 4.1.1 Urvalskriterier

De krav som ställdes på värderingsmetoder för att bedömas som intressanta nog för vidare granskning var följande:

1. Värderingsmetoden skall vara applicerbar på datorbaserade informationssystem.
2. Värderingar baserade på metoden skall fokusera på hela system och inte endast enskilda delar som ingår i systemet.
3. Värderingsmetoden skall fokusera på IT-säkerhet.
4. Det skall finnas en beskrivning tillgänglig för hur värderingsmetoden fungerar samt en vägledning om hur värderingsmetoden används.

### 4.1.2 Sökningar i databaser relevanta för området

Tre databaser, IEEE Xplore, ACM Portal och Ingenta användes i litteraturstudien. Vid sökningarna i databaserna användes de söktermer som finns angivna i Tabell 1. För att begränsa antalet träffar begränsades sökningarna till artiklar publicerade år 2000 och framåt. Ett stort antal träffar relaterade till säker elförsörjning. För att undvika dessa träffar begränsades sökningen till artiklar som inte innehåller ordet ”power”.

En sökning på ”security assessment” i IEEE Xplore gav 621 träffar vilket reducerades till 83 med restriktionerna beskrivna ovan. Vid en genomgång av rubrikerna till dessa hittades 11 potentiellt intressanta artiklar, men vid närmare granskning visade det sig att ingen uppfyllde urvalskriterierna. Sökningen på ”security evaluation” gav 193 träffar vilket reducerades till 125 med de införda begränsningarna. För att ytterligare reducera antalet träffar preciserades sökningen till ”IT security evaluation” samt ”information security evaluation”. En genomgång av resultatet för sökning på ”IT security evaluation” gav inga intressanta artiklar medan sökningen på ”information security evaluation” gav tre tänkbara artiklar av vilka en uppfyller de uppsatta urvalskriterierna. Den

identifierade metoden beskrivs i artikeln *A Method of Security Evaluation Based on Fuzzy Mathematics* (Guo-Ming Lu, Zhi-Hong Chen, Xue-Zhi He, & Jian-Ping Li, 2008).

En sökning på ”security assessment” i ACM Portal gav 118 träffar. Dessa reducerades till 81 med samma restriktioner som ovan. En genomgång av träffarna resulterade i att en artikel identifierades som intressant och denna visade sig även uppfylla de ställda kriterierna. Den identiferade artikeln var AMBRA: automated model-based risk analysis (Aime, Atzeni, & Pomi, 2007). Sökningen på ”security evaluation” gav 261 träffar, vilket reducerades till 148. Sökningar på ”IT security evaluation” samt ”information security evaluation” resulterade inte i att några intressanta artiklar hittades.

En sökning på ”security assessment” i Ingentas ”electronic content” gav 69 träffar, vilket reducerades till 16 med restriktioner enligt ovan. En genomgång av de 16 träffarna resulterade dock inte i att några intressanta artiklar identifierades. En sökning på ”security evaluation” i Ingenta gav 28 träffar vilket reduceras till 8. Bland dessa var dock inga artiklar av intresse.

Tabell 1: Söktermer och antal träffar för de tre databaserna.

| Sökterm | IEEE Xplore | ACM Portal | Ingenta |
|---|---|---|---|
| security assessment | 632 | 3825 | 855 |
| Restriktion: år 2000- | 404 | 3553 | 679 |
| Restriktion: år 2000-, ej ”power” | 88 | 2086 | 588 |
| ”security assessment” | 621 | 118 | 69 |
| Restriktion: år 2000- | 396 | 111 | 32 |
| Restriktion: år 2000-, ej ”power” | 83 | 81 | 16 |
| ”information security assessment” | 6 | 5 | 1 |
| Restriktion: år 2000- | 5 | 5 | 1 |
| Restriktion: år 2000-, ej ”power” | 4 | 4 | 1 |
| ”IT security assessment” | 2 | 1 | 0 |
| Restriktion: år 2000- | 2 | 1 | 0 |
| Restriktion: år 2000-, ej ”power” | 2 | 1 | 0 |
| ”security evaluation” | 193 | 261 | 28 |
| Restriktion: år 2000- | 154 | 222 | 10 |
| Restriktion: år 2000-, ej ”power” | 125 | 148 | 8 |
| ”information security evaluation” | 8 | 6 | 0 |
| Restriktion: år 2000- | 8 | 6 | 0 |
| Restriktion: år 2000-, ej ”power” | 7 | 5 | 0 |
| ”IT security evaluation” | 6 | 14 | 4 |
| Restriktion: år 2000- | 5 | 13 | 2 |
| Restriktion: år 2000-, ej ”power” | 5 | 11 | 2 |

### 4.1.3 Genomgång av bidrag till relevanta konferenser

För att komplettera sökningarna i databaser gicks bidrag från relevanta konferenser igenom. De konferenser som studerats är Quality of Protection Workshop (från 2009 kallad International Workshop on Security Measurement

and Metrics) samt IEEE Information Assurance Workshop. Quality of Protection valdes för att det är den enda workshop som helt fokuserar på området värdering av IT-säkerhet och vars dokumentation innehåller de presenterade artiklarna. Information Assurance Workshop valdes eftersom författarna, av denna rapport, har personlig erfarenhet av att det presenterats intressanta artiklar på denna och att det därför potentiellt kan ha publicerats fler intressanta arbeten.

Genomgången av bidragen till konferenserna skedde på följande strukturerade sätt.

1. Innehållsförteckningen till dokumentationen från varje konferens genomsöktes för att identifiera artiklar som potentiellt kunde vara relevanta.
2. Sammanfattningarna studerades för de artiklar som identifierats i punkt 1 för att sålla bort de artiklar som uppenbart behandlade områden utanför intressesfären.
3. Återstående artiklar lästes i sin helhet varvid de som inte uppfyllde urvalskriterierna sållades bort.

De metoder som valdes ut från genomgången av konferenser listas nedan.

- Analysis and statistical properties of critical infrastructure interdependency multiflow models (Svendsen & Wolthusen, 2007)
- Analyzing the security and survivability of real-time control systems (Oman, Krings, Conte de Leon, & Alves-Foss, 2004)
- Assessing the risk of using vulnerable components (Balzarotti, Monga, & Sicari, 2005)
- Toward measuring network security using attack graphs (Wang, Singhal, & Sushil Jajodia, 2007)
- Measuring the attack surfaces of FTP daemons (Manadhata, Wing, Flynn, & McQueen, 2006)
- Qualitative and quantitative analytical techniques for network security assessment (Clark, Tyree, Dawkins, & Hale, 2004)
- A weakest-adversary security metric for network configuration security analysis (Pamula, S. Jajodia, Ammann, & Swarup, 2006)
- Measuring IT security - a method based on Common Criteria's security functional requirements (Hunstad, J. Hallberg, & Andersson, 2004)
- Performance measurements guide for information security (Chew et al., 2008)

- PANEMOTO: Network Visualization of Security Situational Awareness Through Passive Analysis (Streilein, Kratkiewicz, Sikorski, Piwowarski, & Webster, 2007)
- A new assessment and improvement model of risk propagation in information security (Kondakci, 2007)
- Methodology of Risk Assessment in Mobile Agent System Design (McLean, Szymanski, & Bivens, 2003)
- Model-based security analysis in seven steps – a guided tour to the CORAS method (den Braber, Hogganvik, Lund, Stølen, & Vraalsen, 2007)
- Security risks: Fusing enterprise objectives and vulnerabilities (Clark, Dawkins, & Hale, 2005)

### 4.1.4 Ad hoc sökningar

Utöver de strukturerade metoder som beskrivits ovan inkluderades även metoder sedan tidigare kända av rapportförfattarna. Dessutom tillfrågades medlemmar i kompetensgruppen IT-säkerhet vid FOI. Vidare har mer generella sökningar gjorts först med Google och sedan med Google scholar.

Genom författarna och IT-säkerhetsgruppens övriga medlemmar identifierades sex metoder, varav en metod (XMASS) är under utveckling inom gruppen. De identifierade metoderna refereras enligt följande lista.

- Complete Guide to Security and Privacy Metrics (Herrmann, 2007),
- Security Metrics: Replacing Fear, Uncertainty, and Doubt (Jaquith, 2007),
- eXtended Method for Assessment of System Security (XMASS) (J. Hallberg, N. Hallberg, & Hunstad, 2006),
- Nessus (http://www.nessus.org/documentation/, besökt oktober 2009), samt
- RedSeal (RedSeal, 2009a, 2009b)
- Assessment of Enterprise Information Security (Johansson, 2005)

När sökningar med Google gjordes användes samma sökbegrepp som vid sökningarna i databaser (4.1.2). Som framgår av Tabell 2 erhålles ohanterligt många träffar vid samtliga sökningar och med anledning av detta studerades endast den första sidan av sökträffarna mycket översiktligt, det vill säga rubrikerna lästes igenom och intressanta länkar studerades vidare. Sökningarna med Google gav en metod som ansågs vara intressant nämligen Microsoft

Security Assessment Tool (MSAT) (http://technet.microsoft.com/en-us/security/cc185712.aspx, besökt oktober 2009).

Vid sökningen med Google scholar fås färre träffar än vid generell sökning med Google men antalet träffar är, som framgår av Tabell 2 fortfarande mestadels ohanterligt många. Liksom för den mer allmänna sökningen gicks endast första sidan igenom förutom för sökningen på ”IT security assessment” där alla 56 träffar gicks igenom. Sökningen med Google scholar gav dock inga nya intressanta metoder. Flera tidigare identifierade metoder återfanns dock under sökningarna.

Tabell 2: Antal sökträffar med Google och Google scholar.

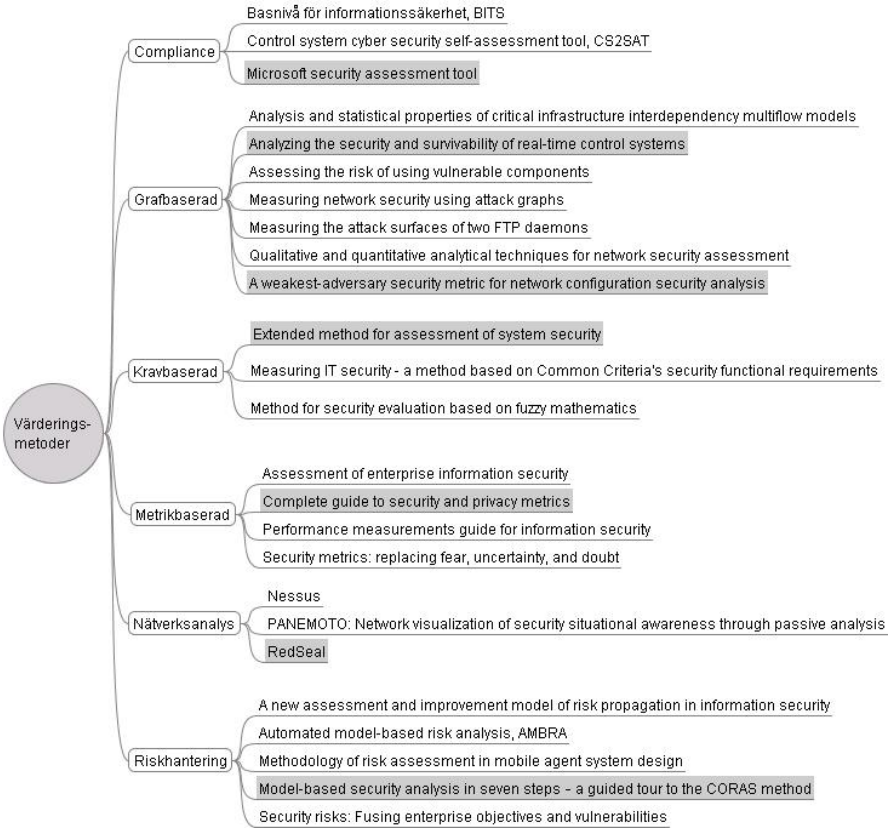
| Sökterm | Google.com | Google scholar |
|---|---|---|
| security assessment | 21 300 000 | 1 880 000 |
| ”security assessment” | 586 000 | 10 700 |
| ”information security assessment” | 891 000 | 161 |
| ”IT security assessment” | 586 000 | 52 |
| ”security evaluation” | 176 000 | 8 490 |
| ”information security evaluation” | 456 000 | 331 |
| ”IT security evaluation” | 395 000 | 598 |

## 4.2 Gruppering av metoder

För att gruppera de identifierade metoderna gicks de igenom med syfte att identifiera de mest framträdande egenskaperna. Därefter samlades metoder med liknande framträdande egenskaper i grupper. De metoder som inte grupperades i den första omgången sågs som egna grupper vilka under några iterationer slogs ihop med de tidigare skapade grupperna. I en del fall resulterade detta i att den större gruppen vidgades. Ett exempel på detta är gruppen *grafbaserad* som i tidigare skeden av grupperingen kallades ”attackgrafer”. I andra fall baserades hopslagningen av grupperna på att andra egenskaper än tidigare beaktades för metoden i den mindre gruppen. Resultatet av grupperingen återfinns i Figur 4.

Metoder i gruppen *compliance* syftar till att säkerställa att system uppfyller uppsättningar av krav ställda på systemnivå. Gruppen *grafbaserad* innehåller metoder som utgår ifrån att värderingsproblemet kan beskrivas med en graf. Algoritmer för lösning av problem beskrivna med grafer kan då tillämpas. Metoder i gruppen *kravbaserad* utgår ifrån analyser baserade på uppfyllnad av säkerhetskrav. Metoder i gruppen *metriker* utgår från uppsättningar med specificerade mätobjekt hos, eller i omgivningen av, system. Ofta relaterar mätobjekten till så kallade systemeffekter, det vill säga effekter som beror på den säkerhet som ska värderas. Gruppen *nätverksanalys* innehåller metoder som utgår från data som samlas in från nätverk i drift. Metoder i gruppen *riskhantering* går ett steg längre än att värdera säkerhet och inkluderar konceptet

risk. Riskhantering utgör en av de processer som kan nyttja data från genomförda säkerhetsvärderingar. Därigenom är det endast vissa delar av dessa metoder som är av intresse vid testning av metoder för värdering av IT-säkerhet.




Figur 4: Gruppering av identifierade metoder. De gråmarkerade metoderna är de som i Avsnitt 4.3 väljs ut för testning.

## 4.3 Urval av metoder för testning

För att begränsa testarbetet, men ändå erhålla en representativ mängd med tester, gjordes ett urval av metoder. Urvalet gjordes så att alla de grupper som resulterade från grupperingen i föregående avsnitt skulle vara representerade. Att en metod inte blivit utvald för test betyder inte att den är ointressant att testa. Följande metoder valdes ut för testning:

- RedSeal

- A Weakest-Adversary Security Metric for Network Configuration Security Analysis
- eXtended Method for Assessment of System Security, XMASS
- Analyzing the security and survivability of real-time control systems
- Complete Guide to Security and Privacy Metrics – Measuring Regulatory Compliance, Operational Resilience, and ROI
- Microsoft Security Assessment Tool
- Model-based security analysis in seven steps – a guided tour to the CORAS method

# 5 Metodtest

I detta kapitel presenteras och testas de metoder som valdes i Avsnitt 4.3. Varje metod presenteras först med en översikt och en sammanfattande beskrivning. Sedan följer resultatet av de mätningar som gjorts i testet.

För de flesta metoder ges även en förklaring till de attribut som har fått noll i täckning. Tanken är att ge läsaren inblick i varför detta alternativ valts istället för att endast ange att metoden inte uppfyller attributet.

## 5.1 RedSeal

*RedSeal Network Advisor* och *RedSeal Vulnerability Advisor* är två kommersiella produkter för analys av datornätverk som tagits fram av RedSeal systems.

### 5.1.1 Metodöversikt

| **Metodinformation** | |
|---|---|
| Metodgrupp | Nätverksanalys |
| Skalbarhet | Automatiskt verktyg – uppskalning till större nätverk sker genom att använda en kraftigare server. |
| Dokument som utgjort underlag för testet | (RedSeal, 2009a, 2009b) |
| Publiceringsdatum | 2009-06-05 |
| Värderingsmål | • automatisk identifiering av sårbarheter i nätverk<br>• stöd för hantering av identifierade sårbarheter<br>• verifiering av att säkerhetspolicy och regelverk följs<br>• analys av intrång och validering av åtgärder<br>• automatisk testning av säkerhetskontroller |
| Möjliga värderingsobjekt | Datornätverk |

### 5.1.2 Sammanfattande beskrivning av metoden

De två produkterna *Network Advisor* och *Vulnerability Advisor* är så pass lika att det är svårt att hitta skillnader mellan dem. Med anledning av detta har mätning

genomförts baserat på båda produktspecifikationerna även om det huvudsakligen är *Vulnerability Advisor* som är av intresse.

RedSeal tillhandahåller en automatisk metod för säkerhetsvärdering av datornätverk. Värdering sker av en dedikerad server placerad i nätverket. Den dedikerade servern kan, med tillgång till konfigurationsdata, automatiskt kontrollera att exempelvis switchar och brandväggar följer uppsatt policy. RedSeal har även stöd för att söka av nätverket efter sårbarheter och prioritera dessa efter hur stor påverkan de bedöms kunna ha på systemet.

Efter att data har samlats in presenteras analysen av systemet med hjälp av tabeller och grafer där det exempelvis går att se svaga punkter i nätverket.

### 5.1.3 Mätdata

Nedan presenteras resultaten av de gjorda mätningarna för RedSeal avseende relevans (Tabell 3) och validitet (Tabell 4).

Tabell 3: Mätvärden avseende relevansattribut för RedSeal.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.1 Requirements engineering | 0 | 1 |
| 1.1.2 Systems development | 0 | 1 |
| 1.1.3 Risk management | 1 | 1 |
| 1.1.4 Verification and validation | 1 | 1 |
| 1.1.5 Accreditation | 1 | 1 |
| 1.1.6 Operations support | 1 | 1 |
| 1.2.1.1 Technical | 1 | 1 |
| 1.2.1.2 Organizational | 0 | 1 |
| 1.2.1.3 Human | 0 | 1 |
| 1.2.1.4 Operational | 0 | 1 |
| 1.2.1.5 Contextual | 1 | 1 |
| 1.2.2 Temporal aspects | 1 | 1 |
| 1.2.3.1 Observation | 0 | 1 |
| 1.2.3.2 Test | 1 | 1 |
| 1.2.3.3 Entity characteristics | 1 | 1 |
| 1.2.3.4 System-wide characteristics | 0 | 1 |
| 1.2.3.5 Structural characteristics | 1 | 1 |
| 1.3.1.1 Computer components | 1 | 1 |
| 1.3.1.2 Computers | 1 | 1 |
| 1.3.1.3 Networked systems | 1 | 1 |
| 1.3.1.4 Humans | 0 | 1 |
| 1.3.1.5 Organizational units | 0 | 1 |
| 1.3.1.6 System processes | 1 | 1 |
| 1.3.1.7 System characteristics | 0 | 1 |
| 1.3.1.8 System effects | 0 | 0 |
| 1.3.2 System entity-inter-relations | 1 | 1 |
| 1.3.3 Multiple abstraction levels | 1 | 1 |
| 1.3.4 Hierarchical models | 1 | 1 |
| 1.3.5 Established modeling technique/language | 0 | 1 |
| 1.4.1 Input selection | 0 | 0 |

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.4.2 Security values aggregation | 0 | 0 |
| 1.5.1 Related to system modeling | 1 | 1 |
| 1.5.2 Related to computations modeling | 1 | 1 |
| 1.5.3 Related to security values computation | 1 | 1 |
| 1.5.4 Related to measurements | 1 | 1 |
| 1.8 Interpret security values | 0 | 0 |
| 1.9.1 Reuse produced data from previous assessments of the same system | 1 | 1 |
| 1.9.2 Reuse produced data from previous assessments of other systems | 0 | 1 |
| 1.9.3 No external experts needed to prepare the input | 0 | 1 |
| 1.9.4 No external experts needed to perform the security assessment | 1 | 1 |

Tabell 4: Mätvärden avseende validitetsattribut för RedSeal.

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

### 5.1.4 Kommentarer till mätresultat

För relevansen gäller att attributet om att kunna modellera interaktionen mellan systemet och omgivningen har inte kunnat utläsas. Då metoden skall kunna presentera identifierade sårbarheter samt avvikelser från policys anser vi dock att detta bör vara möjligt. Angående att kunna välja indata eller hur indata aggregeras känns det högst troligt att detta är möjligt, men då det inte framgår av dokumentationen går det inte att säga att det är uppfyllt. Det går inte att avgöra huruvida det finns en metod för hur säkerhetsvärden skall tolkas. Det finns flera olika säkerhetsvärden som systemet kan leverera, men ingen beskrivning av hur dessa ska tolkas.

När det gäller validitetsaspekterna av mätningen hittades inga referenser till experiment som påvisar att metoden fungerar. Då det är ett kommersiellt verktyg

är det högst troligt att det finns praktiska resultat som validerar metoden, men då detta inte har kunnat påvisas kan beskrivningen av metoden inte anses täcka detta attribut. Det gick heller inte att avgöra om det finns rutiner för att undvika att irrelevant eller felaktig information används samt om det finns rutiner för att undvika att relevant information exkluderas från värderingen.

## 5.2 A Weakest-Adversary Security Metric

*A Weakest-Adversary Security Metric* är framtagen 2006 vid Center for Secure Information Systems på George Mason University, USA.

### 5.2.1 Metodöversikt

| **Metodinformation** | |
|---|---|
| Metodgrupp | Grafbaserad |
| Skalbarhet | Den beskrivna metoden är förmodligen svår att skala upp, om det inte finns några automatiska verktyg för modellera systemet. |
| Dokument som utgjort underlag för testet | (Pamula et al., 2006) |
| Publiceringsdatum | 2006 |
| Värderingsmål | Att hitta kortaste kedjan från en hotagent till en specifik skyddsvärd entitet i ett system. |
| Möjliga värderingsobjekt | Datornätverk |

### 5.2.2 Sammanfattande beskrivning av metoden

*A Weakest-Adversary Security Metric* använder sig av en kvantitativ säkerhetsmetrik för att mäta säkerheten i datornätverk. Säkerhetsmetriken som föreslås ska beskriva den ”svagaste motståndare” som klarar att angripa systemet. Detta innebär att man räknar ut den lättaste vägen att få tillgång till ett skyddsvärt objekt. Resultatet av värderingen blir den eller de vägar in till det skyddsvärda objektet som kräver den minsta uppsättningen av initiala resurser, vilket kan nyttjas som mått på säkerheten i systemet.

Vid modelleringen av ett system utgår man från systemets topologi och tar för varje nod i systemet fram de hot som är aktuella. Systemets topologi och de aktuella hoten används som grund för att ta fram en attackgraf som används för att beräkna den lättaste vägen in till det skyddsvärda objektet.

Metodbeskrivningen innehåller även ett förslag på hur man kan implementera en beräkningsfunktion för att utifrån en framtagen attackgraf automatiskt beräkna den lättaste vägen in.

### 5.2.3 Mätdata

Nedan presenteras resultaten av de gjorda mätningarna för *Weakest-Adversary Security Metric* avseende relevans (Tabell 5) och validitet (Tabell 6).

Tabell 5: Mätvärden avseende relevansattribut för *Weakest-Adversary Security Metric.*

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.1 Requirements engineering | 0 | 1 |
| 1.1.2 Systems development | 0 | 1 |
| 1.1.3 Risk management | 1 | 1 |
| 1.1.4 Verification and validation | 1 | 1 |
| 1.1.5 Accreditation | 1 | 1 |
| 1.1.6 Operations support | 0 | 0 |
| 1.2.1.1 Technical | 1 | 1 |
| 1.2.1.2 Organizational | 0 | 1 |
| 1.2.1.3 Human | 0 | 1 |
| 1.2.1.4 Operational | 0 | 1 |
| 1.2.1.5 Contextual | 0 | 1 |
| 1.2.2 Temporal aspects | 0 | 0 |
| 1.2.3.1 Observation | 0 | 1 |
| 1.2.3.2 Test | 1 | 1 |
| 1.2.3.3 Entity characteristics | 1 | 1 |
| 1.2.3.4 System-wide characteristics | 0 | 1 |
| 1.2.3.5 Structural characteristics | 1 | 1 |
| 1.3.1.1 Computer components | 1 | 1 |
| 1.3.1.2 Computers | 1 | 1 |
| 1.3.1.3 Networked systems | 1 | 1 |
| 1.3.1.4 Humans | 0 | 1 |
| 1.3.1.5 Organizational units | 0 | 1 |
| 1.3.1.6 System processes | 0 | 1 |
| 1.3.1.7 System characteristics | 0 | 1 |
| 1.3.1.8 System effects | 0 | 1 |
| 1.3.2 System entity-inter-relations | 1 | 1 |
| 1.3.3 Multiple abstraction levels | 0 | 1 |
| 1.3.4 Hierarchical models | 0 | 1 |
| 1.3.5 Established modeling technique/language | 0 | 1 |
| 1.4.1 Input selection | 1 | 1 |
| 1.4.2 Security values aggregation | 1 | 1 |
| 1.5.1 Related to system modeling | 0 | 0 |
| 1.5.2 Related to computations modeling | 0 | 0 |
| 1.5.3 Related to security values computation | 0 | 0 |
| 1.5.4 Related to measurements | 0 | 0 |
| 1.8 Interpret security values | 1 | 1 |
| 1.9.1 Reuse produced data from previous assessments of the same sys. | 1 | 1 |
| 1.9.2 Reuse produced data from previous assessments of other systems | 1 | 1 |
| 1.9.3 No external experts needed to prepare the input | 1 | 1 |
| 1.9.4 No external experts needed to perform the security assessment | 1 | 1 |

Tabell 6: Mätvärden avseende validitetsattribut för *Weakest-Adversary Security Metric.*

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

### 5.2.4 Kommentarer till mätresultat

När det gäller relevansen är det osäkert om attackgraferna har något att tillföra det operativa arbetet. Anledningen till detta är att sårbarheter måste vara kända för att kunna modelleras och borde därför även vara kända av systemansvariga. Vidare växer attackgrafernas omfattning och komplexitet snabbt med storleken hos det aktuella systemet. Det är även svårt att avgöra om metoden kan utvärdera temporala aspekter så som hur säkerhetsuppdateringar påverkar systemet. Anledningen till detta är som nämndes ovan att de sårbarheter som används i modellen behöver vara kända och att det därför bara går att ta hänsyn till det tänkta resultatet av en säkerhetsuppdatering.

Vid mätning på validitet kan konstateras att det från dokumenten inte går att avgöra att mätningar sker objektivt men det går heller inte att avskriva utifrån den beskrivning som finns. Vidare är det inte möjligt att avgöra om det finns stöd för att undvika att irrelevanta eller felaktiga värden tas med eller för att undvika att relevanta värden exkluderas. Detta på grund av att beskrivningen om hur data skall samlas in är kortfattad.

## 5.3 eXtended Method for Assessment of System Security

*eXtended Method for Assessment of System Security* (XMASS) är en kravbaserad värderingsmetod som är framtagen av Totalförsvarets forskningsinstitut (FOI) i Linköping.

### 5.3.1 Metodöversikt

| **Metodinformation** | |
|---|---|
| Metodgrupp | Kravbaserad |
| Skalbarhet | Det finns ett befintligt verktyg (SANTA) för att underlätta genomförandet av en värdering, men för stora system kan modelleringen ändå bli tidskrävande. |
| Dokument som utgjort underlag för testet | (J. Hallberg et al., 2006; J. Hallberg, Bengtsson, & Andersson, 2007; Sundmark, 2008; Bengtsson & Brinck, 2008) |
| Publiceringsdatum | 2008-12-19 |
| Värderingsmål | Att ge ett övergripande säkerhetsvärde för system, men även säkerhetsvärden för enskilda entiteter med hänsyn till deras kontext. |
| Möjliga värderingsobjekt | Datornätverk |

### 5.3.2 Sammanfattande beskrivning av metoden

Värderingsmetoden XMASS använder ett egendefinierat modelleringsspråk som består av entiteter och relationer. Det finns två olika typer av entiteter – trafikgeneratorer och trafikförmedlare. Trafikgeneratorer representerar de typer av entiteter som genererar trafik, som exempelvis servrar och arbetsstationer. Trafikförmedlare representerar entiteter som används för att förmedla trafik, som exempelvis switchar, routrar och brandväggar.

Relationer kan modelleras som antingen fysiska relationer eller logiska relationer. En fysisk relation representerar en dubbelriktad koppling över fysiska medier såsom trådad eller trådlös kommunikation. De logiska relationerna beskriver enkelriktade beroenden och kopplingar mellan entiteter vilket exempelvis kan vara en VPN-tunnel. Varje relation har en *relationsprofil* som beskriver hur de ihopkopplade entiteterna påverkar varandra.

För att avgöra säkerhetsnivån i ett system utgår man från en uppsättning krav. Denna uppsättning kan exempelvis vara Försvarsmaktens *Krav på SäkerhetsFunktioner* (KSF) (Försvarsmakten, 2004). Säkerhetsnivån för ett system beräknas genom en aggregering av säkerhetsvärden för alla entiteter i systemet. Relationerna används för att avgöra hur de olika entiteterna påverkar varandra och på så sätt påverkar varandras säkerhetsvärden.

Säkerhetsvärden för varje entitet tas fram genom att avgöra i vilken grad de ställda kraven uppfylls. Denna uppfyllnad anges genom att ett värde [0,1] sätts för varje krav, där 0 innebär att kravet ej är uppfyllt medan 1 innebär att kravet är helt uppfyllt. Ett värde mellan 0 och 1 innebär delvis kravuppfyllnad.

Kravuppfyllnaden används sedan för att beräkna säkerhetsvärden som motsvarar en uppsättning specificerade säkerhetsegenskaper. Dessa säkerhetsvärden bildar tillsammans en vektor som i XMASS kallas för *säkerhetsprofil*.

Trafikförmedlare har även en *filterprofil* som beskriver hur den genomflytande trafiken filtreras. En filterprofil består av en vektor som med värden [0,1] beskriver i vilken grad trafikförmedlarens tillgängliga filtreringsfunktioner filtrerar den genomflytande trafiken. Värdena i filterprofilen beräknas från en uppsättning specificerade krav på filtreringsfunktioner.

### 5.3.3 Mätdata

Nedan presenteras resultaten av de gjorda mätningarna för XMASS avseende relevans (Tabell 7) och validitet (Tabell 8).

Tabell 7: Mätvärden avseende relevansattribut för *XMASS*.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.1 Requirements engineering | 1 | 1 |
| 1.1.2 Systems development | 1 | 1 |
| 1.1.3 Risk management | 0 | 1 |
| 1.1.4 Verification and validation | 0 | 1 |
| 1.1.5 Accreditation | 1 | 1 |
| 1.1.6 Operations support | 0 | 1 |
| 1.2.1.1 Technical | 1 | 1 |
| 1.2.1.2 Organizational | 0 | 1 |
| 1.2.1.3 Human | 0 | 1 |
| 1.2.1.4 Operational | 0 | 1 |
| 1.2.1.5 Contextual | 0 | 1 |
| 1.2.2 Temporal aspects | 0 | 1 |
| 1.2.3.1 Observation | 0 | 1 |
| 1.2.3.2 Test | 0 | 1 |
| 1.2.3.3 Entity characteristics | 1 | 1 |
| 1.2.3.4 System-wide characteristics | 0 | 1 |
| 1.2.3.5 Structural characteristics | 1 | 1 |
| 1.3.1.1 Computer components | 0 | 1 |
| 1.3.1.2 Computers | 1 | 1 |
| 1.3.1.3 Networked systems | 1 | 1 |
| 1.3.1.4 Humans | 0 | 1 |
| 1.3.1.5 Organizational units | 0 | 1 |
| 1.3.1.6 System processes | 0 | 1 |
| 1.3.1.7 System characteristics | 0 | 1 |
| 1.3.1.8 System effects | 0 | 1 |
| 1.3.2 System entity-inter-relations | 1 | 1 |
| 1.3.3 Multiple abstraction levels | 1 | 1 |
| 1.3.4 Hierarchical models | 0 | 1 |
| 1.3.5 Established modeling technique/language | 0 | 1 |
| 1.4.1 Input selection | 1 | 1 |
| 1.4.2 Security values aggregation | 1 | 1 |
| 1.5.1 Related to system modeling | 1 | 1 |
| 1.5.2 Related to computations modeling | 1 | 1 |

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.5.3 Related to security values computation | 1 | 1 |
| 1.5.4 Related to measurements | 0 | 1 |
| 1.8 Interpret security values | 0 | 1 |
| 1.9.1 Reuse produced data from previous assessments of the same sys. | 1 | 1 |
| 1.9.2 Reuse produced data from previous assessments of other systems | 1 | 1 |
| 1.9.3 No external experts needed to prepare the input | 0 | 1 |
| 1.9.4 No external experts needed to perform the security assessment | 0 | 1 |

Tabell 8: Mätvärden avseende validitetsattribut för *XMASS*.

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

## 5.4 Analyzing the security and survivability of real time control systems

*Analyzing the security and survivability of real time control systems* är en grafbaserad värderingsmetod som är utvecklad av forskare vid University of Idaho.

### 5.4.1 Metodöversikt

| **Metodinformation** | |
|---|---|
| Metodgrupp | Grafbaserad |
| Skalbarhet | Beror på systemet som modelleras, dock är metoden troligen svår att skala upp utan automatiska verktyg. |
| Dokument som utgjort underlag för testet | (Oman et al., 2004; Krings & Azadmanesh, |

| | |
|---|---|
| | 2002) |
| Publiceringsdatum | 2005-06-06 |
| Värderingsmål | Att värdera/mäta förmåga hos det värderade systemet att bibehålla funktionalitet vid störningar och attacker. |
| Möjliga värderingsobjekt | Kritisk infrastruktur (data och telekommunikationsnät, el-, vatten-, olja- och gasledningar, osv.) |

### 5.4.2 Sammanfattande beskrivning av metoden

Metoden bygger på transformering av ett system till en graf som beskriver systemet och sedan görs utvärdering och eventuell förändring i denna graf för att sedan transformera tillbaka. Metoden sker i följande fem steg:

A: Generera modell

Modellen genereras genom att entiteter i systemet omvandlas till noder och relationer mellan entiteter omvandlas till bågar vilka sammanbinder noderna.

B: Tag fram parametrar

I detta steg tas de parametrar som är intressanta att modellera fram. Exempel på parametrar kan vara nätverkskapacitet, kommunikationskostnad, känslighet eller sekretessgrad. När intressanta parametrar har fastslagits skall noder och/eller bågar tilldelas värden motsvarande vikter för de utvalda parametrarna. Noder eller bågar kan om det krävs tilldelas värden för flera parametrar genom att vikterna anges som vektorer.

C: Abstrahering och modellrepresentation

I detta steg väljs om det i fortsättningen är grafteoretiska metoder som skall användas eller om grafen skall ses som ett schemaläggningsproblem. Oavsett vilket som väljs behöver anpassningar ske.

D: Algoritmer för hantering av grafer eller schemaläggning

I det här steget hittas en lösning, optimal eller sub-optimal, på problemet genom att applicera grafteoretiska eller schemaläggningsalgoritmer. För att hitta en lösning på ett problem kan många algoritmer behöva prövas för att hitta den bästa lösningen.

E: Transformera tillbaka

I det här steget transformeras den lösning på problemet som hittades i D tillbaka till ursprungsrepresentationen.

### 5.4.3 Mätdata

Nedan presenteras resultaten av de gjorda mätningarna för *Analyzing the security and survivability of real time control systems* avseende relevans (Tabell 9) och validitet (Tabell 10).

Tabell 9: Mätvärden avseende relevansattribut för *Analyzing the security and survivability of real time control systems*.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.1 Requirements engineering | 0 | 1 |
| 1.1.2 Systems development | 0 | 1 |
| 1.1.3 Risk management | 1 | 1 |
| 1.1.4 Verification and validation | 0 | 1 |
| 1.1.5 Accreditation | 0 | 1 |
| 1.1.6 Operations support | 0 | 1 |
| 1.2.1.1 Technical | 1 | 1 |
| 1.2.1.2 Organizational | 0 | 1 |
| 1.2.1.3 Human | 0 | 0 |
| 1.2.1.4 Operational | 1 | 1 |
| 1.2.1.5 Contextual | 0 | 0 |
| 1.2.2 Temporal aspects | 0 | 1 |
| 1.2.3.1 Observation | 0 | 1 |
| 1.2.3.2 Test | 0 | 1 |
| 1.2.3.3 Entity characteristics | 1 | 1 |
| 1.2.3.4 System-wide characteristics | 0 | 1 |
| 1.2.3.5 Structural characteristics | 1 | 1 |
| 1.3.1.1 Computer components | 1 | 1 |
| 1.3.1.2 Computers | 1 | 1 |
| 1.3.1.3 Networked systems | 1 | 1 |
| 1.3.1.4 Humans | 0 | 1 |
| 1.3.1.5 Organizational units | 0 | 1 |
| 1.3.1.6 System processes | 1 | 1 |
| 1.3.1.7 System characteristics | 0 | 1 |
| 1.3.1.8 System effects | 1 | 1 |
| 1.3.2 System entity-inter-relations | 1 | 1 |
| 1.3.3 Multiple abstraction levels | 0 | 1 |
| 1.3.4 Hierarchical models | 0 | 1 |
| 1.3.5 Established modeling technique/language | 1 | 1 |
| 1.4.1 Input selection | 1 | 1 |
| 1.4.2 Security values aggregation | 1 | 1 |
| 1.5.1 Related to system modeling | 0 | 1 |
| 1.5.2 Related to computations modeling | 0 | 1 |
| 1.5.3 Related to security values computation | 1 | 1 |
| 1.5.4 Related to measurements | 0 | 1 |
| 1.8 Interpret security values | 1 | 1 |
| 1.9.1 Reuse produced data from previous assessments of the same sys. | 1 | 1 |
| 1.9.2 Reuse produced data from previous assessments of other systems | 1 | 1 |
| 1.9.3 No external experts needed to prepare the input | 0 | 0 |
| 1.9.4 No external experts needed to perform the security assessment | 0 | 0 |

Tabell 10: Mätvärden avseende validitetsattribut för *Analyzing the security and survivability of real time control systems*.

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

### 5.4.4 Kommentarer till mätresultat

För relevansattributen går det inte att avgöra om metoden kan ta hänsyn till mänskliga faktorer för systemet. Det finns inget hinder för att modellera människor som noder i graferna men detta nämns inte. För kontextuella aspekter, det vill säga legala och fysiska aspekter verkar det högst troligt att modellen skulle kunna hantera fysiska aspekter men detta är inte beskrivet. Vidare kunde det inte avgöras huruvida det behövs experter för att ta fram indata till metoden eller för att genomföra en utvärdering.

För validitet uppfyller metoden en del av attribut 2.6.2, då metoden beskriver var gränsen mellan det modellerade systemet och omgivningen ligger. Dock är det inte tydligt om övriga delvillkor för attributet är uppfyllda. Det är möjligt att resonera sig fram till ett svar på detta men då metoden inte har en explicit beskrivning om hur, sätts täckningen till 0.

## 5.5 Complete Guide to Security and Privacy Metrics

*Complete Guide to Security and Privacy Metrics* är en bok skriven av Debra Herrman. I detta avsnitt testas bokens metodik för framtagning av metriker samt användning av de framtagna metrikerna.

### 5.5.1 Metodöversikt

| **Metodinformation** | |
|---|---|
| Metodgrupp | Metrikbaserad |
| Skalbarhet | Att välja ut metriker är troligen inte mycket mer avancerat att göra för en större organisation än en mindre. Dock kan den anpassning av organisationen som krävs för att genomföra och dra nytta av mätningarna begränsa skalbarheten. |
| Dokument som utgjort underlag för testet | (Herrmann, 2007) |
| Publiceringsdatum | 2007 |
| Värderingsmål | Att mäta informationssäkerhetsnivå hos en organisation.<br>Tre olika typer av metriker definieras tänkta att:<br>• mäta hur väl krav från regelverk uppfylls,<br>• mäta robustheten i nuvarande säkerhetsfunktionalitet, samt<br>• mäta återbetalningsgrad på säkerhetsinvesteringar (ROI). |
| Möjliga värderingsobjekt | Metrikerna i boken fokuserar på att mäta egenskaper som påverkar eller beror på informationssäkerheten för en organisation. För detta ändamål delas mätningarna in i fyra delområden:<br>• fysiska hot<br>• avsiktlig eller oavsiktlig skada orsakad av personal<br>• IT-säkerhet<br>• säkerställande av drift |

### 5.5.2 Sammanfattande beskrivning av metoden

Herrmann (2007) utgår från en metod baserad på serier av mål, frågor och metriker (Goal, Question, Metric: GQM (Basili, Caldiera, & Rombach, 1994)). Användandet av GQM är inte nödvändig för att kunna använda den presenterade urvalsmetoden, men rekommenderas av författaren.

Ansatsen baseras på ett tänkt universum av metriker för säkerhet och personlig integritet. Detta universum består av följande tre galaxer.

- Uppfyllnadsgrad avseende givna regelverk (compliance)

- Motståndskraft (resilience), vilken baseras på IT-, operativ, fysisk och personalsäkerhet
- Avkastning (ROI), vilken baseras på IT-, operativ, fysisk och personalsäkerhet samt uppfyllande av regelverk

Syftningen till att boken skulle innehålla en komplett guide till säkerhetsmetriker kommer från ansatsen att den enligt författaren täcker alla områden inom informationssäkerhet och inte bara IT-säkerhet.

Metoden för att ta fram de säkerhetsmetriker man behöver görs genom att använda ett flödesschema, som finns i boken. I detta flödesschema skall användaren börja med att välja vilken eller vilka av de tre galaxerna (compliance, resilience, ROI) som är intressanta för det metrikprogram som skall skapas. Genom att följa flödesschemat blir användaren slutligen hänvisad till en eller flera sektioner i en tabell. I denna tabell har det aktuella området styckats upp i mindre bitar för att underlätta urvalet av relevanta metriker. Genom att välja ut de delområden som är intressanta erhålls referenser till de avsnitt i boken där relevanta metriker listas

För uppfyllnadsgrad (compliance) är det bara två av de listade regelverken som är intressanta i Sverige: *OECD Security and privacy guidelines* och *Data protection directive 95/46/EC* vilka båda handlar om skydd av personlig integritet.

För de två andra galaxerna (resilience och ROI) är metrikerna inte kopplade till speciella regelverk vilket innebär att alla metriker inom de presenterade delområdena potentiellt kan vara av intresse men detta måste avgöras från fall till fall av den om skall skapa metrikprogrammet.

### 5.5.3 Mätdata

Nedan presenteras resultaten av de gjorda mätningarna för *Complete Guide to Security and Privacy Metrics* avseende relevans (Tabell 11) och validitet (Tabell 12).

Tabell 11: Mätvärden avseende relevansattribut för *Complete Guide to Security and Privacy Metrics*.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.1 Requirements engineering | 0 | 1 |
| 1.1.2 Systems development | 0 | 1 |
| 1.1.3 Risk management | 1 | 1 |
| 1.1.4 Verification and validation | 1 | 1 |
| 1.1.5 Accreditation | 0 | 1 |
| 1.1.6 Operations support | 0 | 1 |
| 1.2.1.1 Technical | 1 | 1 |

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.2.1.2 Organizational | 1 | 1 |
| 1.2.1.3 Human | 1 | 1 |
| 1.2.1.4 Operational | 1 | 1 |
| 1.2.1.5 Contextual | 1 | 1 |
| 1.2.2 Temporal aspects | 0 | 0 |
| 1.2.3.1 Observation | 1 | 1 |
| 1.2.3.2 Test | 1 | 1 |
| 1.2.3.3 Entity characteristics | 0 | 1 |
| 1.2.3.4 System-wide characteristics | 1 | 1 |
| 1.2.3.5 Structural characteristics | 0 | 1 |
| 1.3.1.1 Computer components | 0 | 1 |
| 1.3.1.2 Computers | 0 | 1 |
| 1.3.1.3 Networked systems | 0 | 1 |
| 1.3.1.4 Humans | 0 | 1 |
| 1.3.1.5 Organizational units | 0 | 1 |
| 1.3.1.6 System processes | 0 | 1 |
| 1.3.1.7 System characteristics | 0 | 1 |
| 1.3.1.8 System effects | 0 | 1 |
| 1.3.2 System entity-inter-relations | 0 | 1 |
| 1.3.3 Multiple abstraction levels | 0 | 1 |
| 1.3.4 Hierarchical models | 0 | 1 |
| 1.3.5 Established modeling technique/language | 0 | 1 |
| 1.4.1 Input selection | 1 | 1 |
| 1.4.2 Security values aggregation | 0 | 1 |
| 1.5.1 Related to system modeling | 0 | 1 |
| 1.5.2 Related to computations modeling | 0 | 1 |
| 1.5.3 Related to security values computation | 0 | 1 |
| 1.5.4 Related to measurements | 0 | 1 |
| 1.8 Interpret security values | 0 | 0 |
| 1.9.1 Reuse produced data from previous assessments of the same sys. | 1 | 1 |
| 1.9.2 Reuse produced data from previous assessments of other systems | 0 | 1 |
| 1.9.3 No external experts needed to prepare the input | 0 | 0 |
| 1.9.4 No external experts needed to perform the security assessment | 0 | 0 |

Tabell 12: Mätvärden avseende validitetsattribut för *Complete Guide to Security and Privacy Metrics*.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 2.1.1 Temporal aspects | 0 | 1 |
| 2.2.1 System entity inter-relations | 0 | 1 |
| 2.3.1 Security values inter-relations | 0 | 1 |
| 2.4.1 Implementation of the computational model | 0 | 1 |
| 2.4.2 Objective measurement | 0 | 0 |
| 2.5 Security assessment results | 0 | 1 |
| 2.6.1 Specification of relevant security characteristics | 1 | 1 |
| 2.6.2 Specification of system extent | 0 | 1 |
| 2.7.1 System modeling regarding system entities | 0 | 1 |
| 2.7.2 Identification of system characteristics and effects | 0 | 1 |
| 2.7.3 System modeling regarding measurable system charac. and effects | 0 | 1 |

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 2.7.4 Specification of a computational model | 0 | 1 |
| 2.8.1 Review of the quality of associated values | 0 | 1 |
| 2.8.2 Association of values with measurable system charac. and effects | 0 | 1 |
| 2.9.1 Adding information to computations | 0 | 1 |
| 2.9.2 Detecting relevant information | 0 | 1 |
| 2.9.3 Handling system context factors | 0 | 1 |

### 5.5.4 Kommentarer till mätresultat

Relevansattribut som inte kan utläsas inkluderar huruvida skapandet och användningen av ett metrikprogram kan utvärdera temporala aspekter. Metrikprogram skall, enligt de erfarenheter författarna har, utvecklas och förändras allteftersom organisationen som skapade programmet förändras. Detta torde vara rimligt även för metriker skapade från Herrmans bok. Om detta skall göras eller hur finns dock inte beskrivet. Användandet av boken skapar ett metrikprogram för mätningar inom organisationen. Detta inkluderar inte någon form av modellering vilket är anledningen till att inga attribut under 1.3 är uppfyllda. De säkerhetsvärden som erhålls genom att skapa ett metrikprogram utgörs av de mätdata som metrikerna anger. Huruvida dessa värden kan tolkas eller inte beror på formuleringen hos de enskilda metrikerna. Det är således fullt möjligt att det finns en tolkning för de erhållna säkerhetsvärdena, men detta är inte garanterat. Det är valet av metriker som avgör hur mycket extern experthjälp som behövs då ett metrikprogram skall tas fram och användas. Med anledning av detta anses att det inte är möjligt att avgöra om experthjälp behövs vid framtagande av indata eller vid användandet av metrikerna.

När det gäller validitet är beskrivningen av vad som skall mätas med metrikerna ofta detaljerad, så det är troligt att det går att göra en objektiv bedömning av mätningen. Detta förutsätter dock att det finns en metrik som stämmer in på det som önskas mätas.

## 5.6 Microsoft Security Assessment Tool

*Microsoft Security Assessment Tool* (MSAT) är ett fritt tillgängligt verktyg framtaget av Microsoft. Verktyget samt tillgänglig information om verktyget på Microsofts hemsida har använts som underlag för testet.

### 5.6.1 Metodöversikt

| **Metodinformation** | |
|---|---|
| Metodgrupp | Compliance |
| Skalbarhet | Metoden har bra skalbarhet då den är |

| | |
|---|---|
| | frågebaserad samtidigt som alla frågor är på systemnivå. Ett system med ett större antal noder borde således inte ta längre tid att utvärdera än ett system med ett mindre antal noder. |
| Dokument som utgjort underlag för testet | MSAT-verktyget (v.4.0.2.35) samt tillgänglig information hos Microsofts (http://technet.microsoft.com/en-us/security/cc185712.aspx) |
| Publiceringsdatum | 2009-10-09 |
| Värderingsmål | Att ge en holistisk förståelse för säkerhetsrisker och ta fram en plan för hur säkerheten kan förbättras. |
| Möjliga värderingsobjekt | Datornätverk |

### 5.6.2 Sammanfattande beskrivning av metoden

*Microsoft Security Assessment Tool* (MSAT) är en säkerhetsvärderingsmetod som baserar sin värdering på en enkät med systemövergripande frågor. Enkäten består av över 200 frågor som innefattar områden som infrastruktur, programvaror, drift, organisation och personer.

Utifrån frågornas svar genereras ett värderingsresultat som består av en åtgärdsrapport. Denna rapport ger förslag på aktiviteter som ska leda till höjd säkerhet i systemet. Aktiviteterna är prioriterade efter hur viktiga de är att åtgärda. Resultat från en värdering kan jämföras med tidigare värderingsresultat för att illustrera hur säkerhetsnivån i systemet har förändrats över tiden.

Både frågor och resulterande rekommendationer på åtgärder härrör exempelvis från ”best practices”, ISO 17799 och NIST-800.x.

Beroende på kunskapsnivån inom företaget avseende nätverket kan enkäten besvaras med eller utan hjälp av extern experthjälp. Då frågorna i enkäten är ganska elementära bör de kunna besvaras utan extern experthjälp. Enkäten tar en till två timmar att besvara.

### 5.6.3 Mätdata

Nedan presenteras resultaten av de gjorda mätningarna för MSAT avseende relevans (Tabell 13) och validitet (Tabell 14).

Tabell 13: Mätvärden för relevansattribut för *MSAT*.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.1 Requirements engineering | 0 | 1 |
| 1.1.2 Systems development | 0 | 1 |
| 1.1.3 Risk management | 1 | 1 |

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.4 Verification and validation | 0 | 1 |
| 1.1.5 Accreditation | 0 | 1 |
| 1.1.6 Operations support | 1 | 1 |
| 1.2.1.1 Technical | 1 | 1 |
| 1.2.1.2 Organizational | 1 | 1 |
| 1.2.1.3 Human | 1 | 1 |
| 1.2.1.4 Operational | 1 | 1 |
| 1.2.1.5 Contextual | 1 | 1 |
| 1.2.2 Temporal aspects | 1 | 1 |
| 1.2.3.1 Observation | 0 | 1 |
| 1.2.3.2 Test | 0 | 1 |
| 1.2.3.3 Entity characteristics | 0 | 1 |
| 1.2.3.4 System-wide characteristics | 1 | 1 |
| 1.2.3.5 Structural characteristics | 0 | 1 |
| 1.3.1.1 Computer components | 0 | 1 |
| 1.3.1.2 Computers | 0 | 1 |
| 1.3.1.3 Networked systems | 0 | 1 |
| 1.3.1.4 Humans | 0 | 1 |
| 1.3.1.5 Organizational units | 0 | 1 |
| 1.3.1.6 System processes | 0 | 1 |
| 1.3.1.7 System characteristics | 1 | 1 |
| 1.3.1.8 System effects | 0 | 1 |
| 1.3.2 System entity-inter-relations | 0 | 1 |
| 1.3.3 Multiple abstraction levels | 0 | 1 |
| 1.3.4 Hierarchical models | 0 | 1 |
| 1.3.5 Established modeling technique/language | 0 | 1 |
| 1.4.1 Input selection | 0 | 1 |
| 1.4.2 Security values aggregation | 0 | 1 |
| 1.5.1 Related to system modeling | 1 | 1 |
| 1.5.2 Related to computations modeling | 1 | 1 |
| 1.5.3 Related to security values computation | 1 | 1 |
| 1.5.4 Related to measurements | 0 | 1 |
| 1.8 Interpret security values | 1 | 1 |
| 1.9.1 Reuse produced data from previous assessments of the same sys. | 1 | 1 |
| 1.9.2 Reuse produced data from previous assessments of other systems | 0 | 1 |
| 1.9.3 No external experts needed to prepare the input | 1 | 1 |
| 1.9.4 No external experts needed to perform the security assessment | 1 | 1 |

Tabell 14: Mätvärden för validitetsattribut för *MSAT*.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 2.1.1 Temporal aspects | 1 | 1 |
| 2.2.1 System entity inter-relations | 0 | 1 |
| 2.3.1 Security values inter-relations | 0 | 1 |
| 2.4.1 Implementation of the computational model | 1 | 1 |
| 2.4.2 Objective measurement | 0 | 1 |
| 2.5 Security assessment results | 0 | 0 |
| 2.6.1 Specification of relevant security characteristics | 0 | 1 |
| 2.6.2 Specification of system extent | 0 | 1 |
| 2.7.1 System modeling regarding system entities | 0 | 1 |
| 2.7.2 Identification of system characteristics and effects | 1 | 1 |

| | | |
|---|---|---|
| 2.7.3 System modeling regarding measurable system charac. and effects | 0 | 1 |
| 2.7.4 Specification of a computational model | 0 | 1 |
| 2.8.1 Review of the quality of associated values | 0 | 1 |
| 2.8.2 Association of values with measurable system charac. and effects | 0 | 1 |
| 2.9.1 Adding information to computations | 0 | 1 |
| 2.9.2 Detecting relevant information | 0 | 1 |
| 2.9.3 Handling system context factors | 0 | 1 |

### 5.6.4 Kommentarer till mätresultat

Enligt Microsoft baseras frågor samt de rekommenderade åtgärderna på exempelvis best practices och standarder. Detta skulle kunna betyda att metodens validitet på något sätt är bevisad. Dock har ingen information hittats som tydligt visar att värderingsresultatets validitet har bevisats, därav en nolla på attribut 2.5.

## 5.7 CORAS

CORAS-metoden är en värderingsmetod baserad på riskhantering som är framtagen av SINTEF ICT i Norge.

### 5.7.1 Metodöversikt

| **Metodinformation** | |
|---|---|
| Metodgrupp | Riskhantering |
| Skalbarhet | Då de modeller som byggs baseras på identifierade risker kan metoden skalas upp till hur stora system som helst men detta påverkar givetvis precisionen i analysen. |
| Dokument som utgjort underlag för testet | (den Braber et al., 2007; Dahl, Hogganvik, & Stølen, 2007) |
| Publiceringsdatum | Januari 2005 |
| Värderingsmål | Att identifiera de potentiella risker som inte kan försummas och ta fram åtgärdsförslag för att ta ner dessa risker till acceptabel nivå. |
| Möjliga värderingsobjekt | Generellt applicerbar för riskanalys av system av alla typer |

### 5.7.2 Sammanfattande beskrivning av metoden

CORAS är en metod för riskanalys i sju steg. Analysen genomförs av ett expertteam bestående av en analysledare och en sekreterare. Analysen genomförs hos en klient från vilken representanter från olika delar av organisationen deltar.

Vilka roller de deltagande representanterna skall ha beror på vilken av metodens sju steg som behandlas.

Steg 1 – Inledande möte

I detta steg introduceras metoden för representanterna. Dessa får sedan presentera de övergripande målen för analysen samt vad det är som skall analyseras. Syftet är att expertteamet och representanterna skall få en gemensam förståelse för den terminologi som skall användas samt ha en gemensam bild av vad som skall analyseras och omfattningen av analysen. I det här steget planeras även framtida möten och workshopar.

Steg 2 – Översiktlig analys

Expertteamet ger sin bild av vad som skall analyseras och vilka problem som skall beröras. Denna bild baseras på den information som förmedlades av representanterna i steg 1 samt eventuell relevant dokumentation som lämnats till expertteamet. I det här steget identifieras även de resurser som behöver skyddas och en översiktlig analys genomförs för att identifiera uppenbara hot, sårbarheter, hotfulla scenarion och oönskade händelser. Dessa används sedan för att fastställa inriktning för och omfattning av den mer detaljerade analysen.

Steg 3 – Godkännande

Det tredje steget kan ske som ett separat möte eller exempelvis via e-post. Målet är färdigställande av det material som specificerar vad som skall analyseras och vilka tillgångar som är viktiga, samt att få ett formellt godkännande från klienten. De identifierade tillgångarna ska även rangordnas efter hur viktiga de anses vara. Skalor som uttrycker olika typer av konsekvenser som kan drabba tillgångarna och sannolikheter för att dessa skall inträffa ska också tas fram. Slutligen skall det fastslås vilken risknivå som kan accepteras för varje identifierad tillgång.

Steg 4 – Riskidentifiering

Identifiering av risker sker med en metod kallad ”structured brainstorming” och genomförs som en workshop. I detta steg skall representanter med olika bakgrunder och insikter relevanta för analysen ge sin syn på risker. Resultatet från workshopen är en uppsättning hotdiagram som skall beskriva de hot, hotfulla scenarier, samt oönskade händelser som har identifierats. Dessa diagram modelleras med de symboler som beskrivs i CORAS språket.

Steg 5 – Riskbedömning

I detta steg som även det utförs som en workshop skall det avgöras för varje hotfullt scenario hur troligt det är att det kommer att inträffa. Dessa bedömningar skall sedan ligga till grund för hur troligt det är att de identifierade oönskade händelserna kommer att inträffa. Förutom att bedöma detta skall även en uppskattning av konsekvenserna för varje koppling mellan en oönskad incident och en tillgång uppskattas.

Steg 6 – Riskutvärdering

I det här steget fastställs de identifierade sannolikheterna och konsekvenserna och placeras i en så kallad riskmatris som presenteras för representanterna. Detta steg kan ske som ett separat möte eller ingå i workshopen för steg sju.

Steg 7 – Hantering av risker

Sista steget i CORAS sker även den som en workshop där åtgärder för att hantera de risker som identifierats tidigare och som inte kan anses som accepterbara tas fram. Dessa åtgärder syftar till att minska antingen sannolikheten och/eller konsekvenserna för de identifierade riskerna. Innan en plan för att minska riskerna fastställs skall åtgärderna även granskas ur kostanad kontra nytta perspektiv. Resultatet från denna workshop är ett eller en samling av diagram som visar identifierade risker samt de åtgärdsförslag som tagits fram för att minska deras betydelse.

### 5.7.3 Mätdata

Nedan presenteras resultaten av de gjorda mätningarna för CORAS avseende relevans (Tabell 15) och validitet (Tabell 16).

Tabell 15: Mätvärden avseende relevansattribut för *CORAS*.

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.1.1 Requirements engineering | 1 | 1 |
| 1.1.2 Systems development | 0 | 1 |
| 1.1.3 Risk management | 1 | 1 |
| 1.1.4 Verification and validation | 0 | 1 |
| 1.1.5 Accreditation | 0 | 1 |
| 1.1.6 Operations support | 1 | 1 |
| 1.2.1.1 Technical | 1 | 1 |
| 1.2.1.2 Organizational | 1 | 1 |
| 1.2.1.3 Human | 1 | 1 |
| 1.2.1.4 Operational | 1 | 1 |
| 1.2.1.5 Contextual | 1 | 1 |
| 1.2.2 Temporal aspects | 0 | 1 |

| Attribut | Uppfylld | Täckning |
|---|---|---|
| 1.2.3.1 Observation | 1 | 1 |
| 1.2.3.2 Test | 0 | 0 |
| 1.2.3.3 Entity characteristics | 1 | 1 |
| 1.2.3.4 System-wide characteristics | 1 | 1 |
| 1.2.3.5 Structural characteristics | 1 | 1 |
| 1.3.1.1 Computer components | 1 | 1 |
| 1.3.1.2 Computers | 1 | 1 |
| 1.3.1.3 Networked systems | 1 | 1 |
| 1.3.1.4 Humans | 1 | 1 |
| 1.3.1.5 Organizational units | 1 | 1 |
| 1.3.1.6 System processes | 1 | 1 |
| 1.3.1.7 System characteristics | 1 | 1 |
| 1.3.1.8 System effects | 1 | 1 |
| 1.3.2 System entity-inter-relations | 1 | 1 |
| 1.3.3 Multiple abstraction levels | 0 | 1 |
| 1.3.4 Hierarchical models | 0 | 1 |
| 1.3.5 Established modeling technique/language | 0 | 1 |
| 1.4.1 Input selection | 1 | 1 |
| 1.4.2 Security values aggregation | 1 | 1 |
| 1.5.1 Related to system modeling | 1 | 1 |
| 1.5.2 Related to computations modeling | 0 | 1 |
| 1.5.3 Related to security values computation | 0 | 1 |
| 1.5.4 Related to measurements | 0 | 1 |
| 1.8 Interpret security values | 1 | 1 |
| 1.9.1 Reuse produced data from previous assessments of the same sys. | 1 | 1 |
| 1.9.2 Reuse produced data from previous assessments of other systems | 1 | 1 |
| 1.9.3 No external experts needed to prepare the input | 0 | 1 |
| 1.9.4 No external experts needed to perform the security assessment | 0 | 1 |

Tabell 16: Mätvärden avseende validitetsattribut för *CORAS*.

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

### 5.7.4 Kommentarer till mätresultat

Det enda attribut som inte gick att avgöra om det är uppfyllt eller inte är huruvida det går att göra utvärderingen baserat på tester. Vid studier av dokumentationen ter det sig som självklart att testresultat skulle kunna utgöra indata, men då det inte finns någon beskrivning angående detta anses det ändå inte möjligt att utläsa.

# 6 Sammanställning av resultat

Detta kapitel inleds med en presentation av resultatet från associationen av relevansattribut till de olika stegen i IT-livscykeln. Därefter presenteras de testade metodernas relevans- och validitetsvärden för varje steg i livscykeln. Detta för att ge en bild över var i livscykeln som varje metod är bäst lämpad.

## 6.1 Association och viktning av attribut

För att vara användbara måste värderingsmetoder vara, eller ha goda förutsättningar att bli, relevanta för den situation som användaren av metoden befinner sig i. Ett sätt att beskriva typiska situationer för värdering är att nyttja de olika stegen i Försvarsmaktens IT-livscykelmodell. För att ge en bild av hur väl de testade metoderna är lämpade för olika steg i IT-livscykelmodellen har en uppsättning relevansattribut från TSAR valts ut för varje steg i modellen. Uppsättningarna av relevansattribut har valts utifrån vad författarna anser vara relevanta behov för en person som ska utföra en värdering i aktuellt steg i IT-livscykelmodellen. Varje sådan uppsättning relevansattribut är således en modell av de värderingsbehov som återfinns i aktuellt steg i IT-livscykelmodellen.

Efter att en uppsättning relevansattribut tagits fram för varje steg viktades relevansattributen enligt metoden som beskrivs i Avsnitt 2.2.2.2. Detta är ett sätt att framhäva vilka attribut som har större betydelse än övriga.

Följande punkter beskriver situationer där behov av värdering avseende IT-säkerhet kan uppstå.

- Under P2 uppstår behov av säkerhetsvärdering när säkerhetskravs effekt avseende påverkan från hot och risker ska bedömas. Säkerhetsvärderingen ska ge en bild av vilken säkerhetsnivå det framtida systemet kommer att få. Denna bild kan sedan användas för att bedöma huruvida identifierade hot och risker kvarstår.
- Under P3 finns behov av att värdera vilken säkerhet som olika systemarkitekturer och -lösningar kommer att resultera i. De erhållna resultaten kan stämmas av mot de specificerade säkerhetskraven alternativt direkt mot identifierande hot och risker.
- Under P4 behöver säkerheten värderas baserat på realiseringar av systemet. Återigen ska resultaten motsvara de säkerhetskrav som ställs på systemet.
- Under P5 ska systemet ackrediteras. Detta medför behov av att visa att systemet, med hänsyn tagen till dess interaktion med andra system, kommer att uppfylla ställda säkerhetskrav.

- Under P6 ska systemet återigen ackrediteras, nu i dess lokala driftsmiljö. Detta medför behov av att visa att systemet, med hänsyn tagen till alla miljöfaktorer, kommer att uppfylla ställda säkerhetskrav.
- Under P7, när systemet är i drift, behöver värderingar ske för att avgöra om beslutad säkerhetsnivå upprätthålls.

Resultaten av valen av attribut samt viktning för de olika stegen i livscykeln återges i Tabell 17. Valda attribut markeras i tabellen med sina framtagna vikter. Rubrikerna P2 till P7 syftar på steg i IT-livscykelmodellen.

Tabell 17: Val och viktning av relevansattribut för varje steg i IT-livscykeln.

| Attribut | P2 | P3 | P4 | P5 | P6 | P7 |
|---|---|---|---|---|---|---|
| 1.1.1 | 2/39 | | | | | |
| 1.1.2 | 2/39 | 2/48 | 2/48 | 1/53 | | |
| 1.1.3 | 2/39 | 1/48 | 2/48 | | | 2/52 |
| 1.1.4 | | | | 2/53 | 2/51 | |
| 1.1.5 | | | | 2/53 | 2/51 | |
| 1.1.6 | | | | | | 2/52 |
| 1.2.1.1 | | 2/48 | 2/48 | 1/53 | 1/51 | 2/52 |
| 1.2.1.2 | 2/39 | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.2.1.3 | 1/39 | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.2.1.4 | 1/39 | 1/48 | 1/48 | 2/53 | 2/51 | 2/52 |
| 1.2.1.5 | 1/39 | 1/48 | 1/48 | 2/53 | 2/51 | 1/52 |
| 1.2.2 | | 2/48 | 2/48 | 2/53 | 2/51 | |
| 1.2.3.1 | | | | | | 1/52 |
| 1.2.3.2 | | | 2/48 | 2/53 | 2/51 | 1/52 |
| 1.2.3.3 | 2/39 | 2/48 | 2/48 | 1/53 | 1/51 | 1/52 |
| 1.2.3.4 | 1/39 | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.2.3.5 | 1/39 | 2/48 | 1/48 | 1/53 | 1/51 | 2/52 |
| 1.3.1.1 | | 1/48 | 2/48 | 2/53 | 2/51 | 1/52 |
| 1.3.1.2 | | 2/48 | 2/48 | 2/53 | 2/51 | 1/52 |
| 1.3.1.3 | 2/39 | 1/48 | 1/48 | 1/53 | 1/51 | 2/52 |
| 1.3.1.4 | 1/39 | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.3.1.5 | 2/39 | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.3.1.6 | | 2/48 | 2/48 | 2/53 | 2/51 | 2/52 |
| 1.3.1.7 | 2/39 | 1/48 | 1/48 | 1/53 | 1/51 | 2/52 |
| 1.3.1.8 | | | | 2/53 | 2/51 | 2/52 |
| 1.3.2 | 2/39 | 2/48 | 2/48 | 2/53 | 2/51 | 2/52 |
| 1.3.3 | | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.3.4 | | 1/48 | 1/48 | 1/53 | 1/51 | 2/52 |
| 1.3.5 | 1/39 | 2/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.4.1 | 1/39 | 2/48 | 1/48 | 2/53 | 2/51 | 2/52 |
| 1.4.2 | 1/39 | 2/48 | 1/48 | 2/53 | 2/51 | 2/52 |
| 1.5.1 | 2/39 | 2/48 | 2/48 | 2/53 | 1/51 | 2/52 |
| 1.5.2 | 1/39 | 1/48 | 1/48 | 1/53 | 1/51 | 2/52 |
| 1.5.3 | 1/39 | 2/48 | 2/48 | 2/53 | 2/51 | 1/52 |
| 1.5.4 | | | | | | 1/52 |
| 1.8 | 2/39 | 2/48 | 2/48 | 2/53 | 2/51 | 2/52 |
| 1.9.1 | 2/39 | 2/48 | 2/48 | 2/53 | 2/51 | 2/52 |
| 1.9.2 | 2/39 | 2/48 | 2/48 | 2/53 | 2/51 | 1/52 |

| Attribut | P2 | P3 | P4 | P5 | P6 | P7 |
|---|---|---|---|---|---|---|
| 1.9.3 | 1/39 | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |
| 1.9.4 | 1/39 | 1/48 | 1/48 | 1/53 | 1/51 | 1/52 |

När det gäller valet av attribut samt vikter för validitet så är de redan definierade i TSAR. Detta då användarens behov inte anses påverka metodens validitet. Validitetsattributen är därför samma för alla steg i IT-livscykeln. Attribut samt tillhörande vikt återges i Tabell 18.

Tabell 18: Viktning av validitetsattribut.

| Attribut | Vikt |
|---|---|
| 2.1.1 | 1/26 |
| 2.2.1 | 2/26 |
| 2.3.1 | 2/26 |
| 2.4.1 | 1/26 |
| 2.4.2 | 2/26 |
| 2.5 | 2/26 |
| 2.6.1 | 1/26 |
| 2.6.2 | 1/26 |
| 2.7.1 | 2/26 |
| 2.7.2 | 2/26 |
| 2.7.3 | 2/26 |
| 2.7.4 | 2/26 |
| 2.8.1 | 1/26 |
| 2.8.2 | 2/26 |
| 2.9.1 | 1/26 |
| 2.9.2 | 1/26 |
| 2.9.3 | 1/26 |

## 6.2 Sammanställning av mätresultat

Nedan återges en sammanställning av de mätningar som gjorts på de testade metoderna (Tabell 19, Tabell 20). Metoderna är i tabellen namngivna efter vart i rapporten de återfinns (5.1 syftar exempelvis på metoden RedSeal). *U* syftar på *uppfyllnad* för aktuellt attribut, medan *T* syftar på *täckning*.

Tabell 19: Sammanställning av mätresultat avseende relevans.

| Attribut | 5.1 | | 5.2 | | 5.3 | | 5.4 | | 5.5 | | 5.6 | | 5.7 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* |
| 1.1.1 | | 1 | | 1 | 1 | 1 | | 1 | | 1 | | 1 | 1 | 1 |
| 1.1.2 | | 1 | | 1 | 1 | 1 | | 1 | | 1 | | 1 | | 1 |
| 1.1.3 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.1.4 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | | 1 | | 1 |
| 1.1.5 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | | 1 | | 1 |
| 1.1.6 | 1 | 1 | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 |
| 1.2.1.1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.2.1.2 | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.2.1.3 | | 1 | | 1 | | 1 | | | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.2.1.4 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.2.1.5 | 1 | 1 | | 1 | | 1 | | | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.2.2 | 1 | 1 | | | | 1 | | 1 | | | 1 | 1 | | 1 |
| 1.2.3.1 | | 1 | | 1 | | 1 | | 1 | 1 | 1 | | 1 | 1 | 1 |
| 1.2.3.2 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | | 1 | | |
| 1.2.3.3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.2.3.4 | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.2.3.5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.1.1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.1.2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.1.3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.1.4 | | 1 | | 1 | | 1 | | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.1.5 | | 1 | | 1 | | 1 | | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.1.6 | 1 | 1 | | 1 | | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.1.7 | | 1 | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 |
| 1.3.1.8 | | | | 1 | | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.3.3 | 1 | 1 | | 1 | 1 | 1 | | 1 | | 1 | | 1 | | 1 |
| 1.3.4 | 1 | 1 | | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| 1.3.5 | | 1 | | 1 | | 1 | 1 | 1 | | 1 | | 1 | | 1 |
| 1.4.1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 |
| 1.4.2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.5.1 | 1 | 1 | | | 1 | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 |
| 1.5.2 | 1 | 1 | | | 1 | 1 | | 1 | | 1 | 1 | 1 | | 1 |
| 1.5.3 | 1 | 1 | | | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | | 1 |
| 1.5.4 | 1 | 1 | | | | 1 | | 1 | | 1 | | 1 | | 1 |
| 1.8 | | | 1 | 1 | | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 |
| 1.9.1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1.9.2 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 1.9.3 | | 1 | 1 | 1 | | 1 | | | | | 1 | 1 | | 1 |
| 1.9.4 | 1 | 1 | 1 | 1 | | 1 | | | | | 1 | 1 | | 1 |

Tabell 20: Sammanställning av mätresultat avseende validitet.

| Attribut | 5.1 | | 5.2 | | 5.3 | | 5.4 | | 5.5 | | 5.6 | | 5.7 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* |
| 2.1.1 | 1 | 1 | | 1 | | 1 | 1 | 1 | | 1 | 1 | 1 | | 1 |
| 2.2.1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 2.3.1 | 1 | 1 | | 1 | 1 | 1 | | 1 | | 1 | | 1 | | 1 |
| 2.4.1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | | 1 |

| Attribut | 5.1 | | 5.2 | | 5.3 | | 5.4 | | 5.5 | | 5.6 | | 5.7 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* | *U* | *T* |
| 2.4.2 | | 1 | | | | 1 | | 1 | | | | 1 | | 1 |
| 2.5 | | | | 1 | | 1 | | 1 | | 1 | | | 1 | 1 |
| 2.6.1 | 1 | 1 | | 1 | | 1 | | 1 | 1 | 1 | | 1 | | 1 |
| 2.6.2 | | 1 | | 1 | | 1 | | | | 1 | | 1 | 1 | 1 |
| 2.7.1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 2.7.2 | | 1 | | 1 | | 1 | | 1 | | 1 | 1 | 1 | | 1 |
| 2.7.3 | | 1 | 1 | 1 | | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 |
| 2.7.4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | | 1 |
| 2.8.1 | | 1 | | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |
| 2.8.2 | | 1 | | 1 | 1 | 1 | | 1 | | 1 | | 1 | | 1 |
| 2.9.1 | | | | | | 1 | | 1 | | 1 | | 1 | | 1 |
| 2.9.2 | | | | | | 1 | | 1 | | 1 | | 1 | | 1 |
| 2.9.3 | | 1 | | 1 | | 1 | | 1 | | 1 | | 1 | | 1 |

## 6.3 Testresultat

I detta avsnitt redovisas de beräknade värdena för de testade metodernas relevans och validitet (Tabell 21 och Tabell 22). I dessa tabeller syftar rubrikerna P2 till P7 på aktuellt steg i IT-livscykelmodellen, medan rubrikerna 5.1 till 5.7 syftar till de testade metoderna.

Som ett komplement till relevans (R) och validitet (V) presenteras också testens täckningsgrad. Täckningsgraden beräknas dels som summan av vikterna för de attribut som kunde bedömas ($T_1$) och dels som andelen attribut som testet kunde bedöma ($T_2$). Dessa värden beräknas separat för relevans och validitet, det vill säga det finns två värden för $T_1$ respektive $T_2$ för varje test. Testresultaten består av 42 stycken test, det vill säga ett test för varje metod och steg i IT-livscykelmodellen.

Baserat på $T_1$ beräknas maximal relevans ($R_{max}$) genom att addera $1 - T_1$ till relevansen (R). På samma sätt beräkans maximal validitet ($V_{max}$) genom att addera $1 - T_1$ till validiteten (V). Maximal relevans respektive maximal validitet utgör de värden för relevans och validitet som skulle erhållas ifall de obedömbara attributen var uppfyllda.

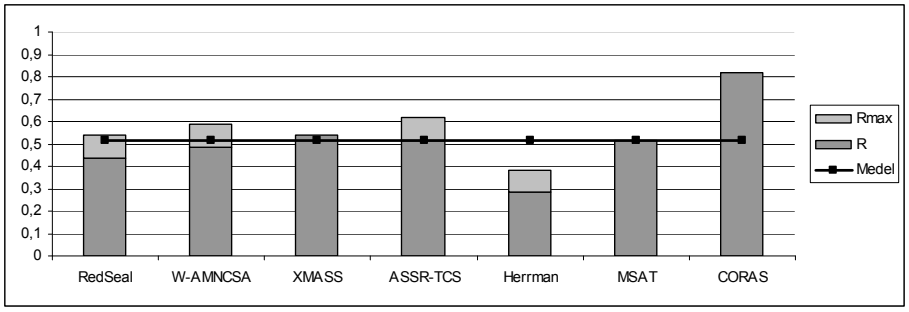
Tabell 21: Sammanställning av testresultat avseende relevans.

| | | 5.1 | 5.2 | 5.3 | 5.4 | 5.5 | 5.6 | 5.7 |
|---|---|---|---|---|---|---|---|---|
| **P2** | **R** | 0,436 | 0,487 | 0,538 | 0,513 | 0,282 | 0,513 | 0,821 |
| | **$R_{max}$** | 0,538 | 0,590 | 0,538 | 0,615 | 0,385 | 0,513 | 0,821 |
| | **$T_1$** | 0,897 | 0,897 | 1,000 | 0,897 | 0,897 | 1,000 | 1,000 |
| | **$T_2$** | 0,885 | 0,885 | 1,000 | 0,846 | 0,885 | 1,000 | 1,000 |
| **P3** | **R** | 0,583 | 0,521 | 0,563 | 0,625 | 0,250 | 0,458 | 0,729 |
| | **$R_{max}$** | 0,708 | 0,667 | 0,563 | 0,708 | 0,375 | 0,458 | 0,729 |
| | **$T_1$** | 0,875 | 0,854 | 1,000 | 0,917 | 0,875 | 1,000 | 1,000 |
| | **$T_2$** | 0,906 | 0,875 | 1,000 | 0,875 | 0,875 | 1,000 | 1,000 |
| **P4** | **R** | 0,646 | 0,542 | 0,500 | 0,583 | 0,292 | 0,479 | 0,708 |
| | **$R_{max}$** | 0,729 | 0,688 | 0,500 | 0,667 | 0,417 | 0,479 | 0,750 |
| | **$T_1$** | 0,917 | 0,854 | 1,000 | 0,917 | 0,875 | 1,000 | 0,958 |
| | **$T_2$** | 0,909 | 0,879 | 1,000 | 0,879 | 0,879 | 1,000 | 0,970 |
| **P5** | **R** | 0,604 | 0,528 | 0,472 | 0,547 | 0,302 | 0,415 | 0,679 |
| | **$R_{max}$** | 0,755 | 0,660 | 0,472 | 0,642 | 0,415 | 0,415 | 0,717 |
| | **$T_1$** | 0,849 | 0,868 | 1,000 | 0,906 | 0,887 | 1,000 | 0,962 |
| | **$T_2$** | 0,886 | 0,886 | 1,000 | 0,886 | 0,886 | 1,000 | 0,971 |
| **P6** | **R** | 0,608 | 0,549 | 0,451 | 0,569 | 0,314 | 0,412 | 0,686 |
| | **$R_{max}$** | 0,765 | 0,667 | 0,451 | 0,667 | 0,431 | 0,412 | 0,725 |
| | **$T_1$** | 0,843 | 0,882 | 1,000 | 0,902 | 0,882 | 1,000 | 0,961 |
| | **$T_2$** | 0,882 | 0,882 | 1,000 | 0,882 | 0,882 | 1,000 | 0,971 |
| **P7** | **R** | 0,596 | 0,481 | 0,442 | 0,577 | 0,308 | 0,481 | 0,788 |
| | **$R_{max}$** | 0,750 | 0,635 | 0,442 | 0,654 | 0,385 | 0,481 | 0,808 |
| | **$T_1$** | 0,846 | 0,846 | 1,000 | 0,923 | 0,923 | 1,000 | 0,981 |
| | **$T_2$** | 0,882 | 0,853 | 1,000 | 0,882 | 0,912 | 1,000 | 0,971 |

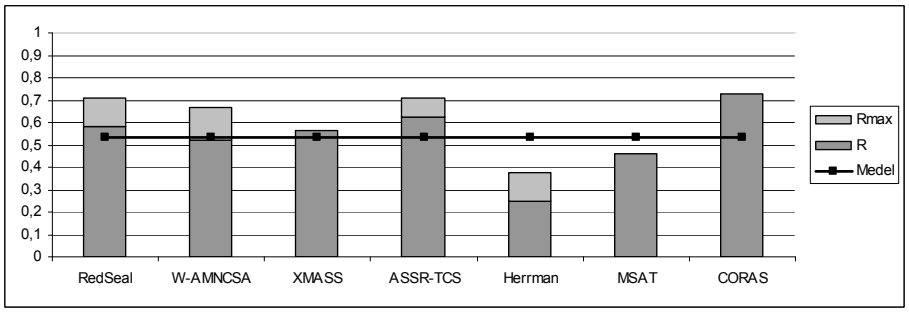
Tabell 22: Sammanställning av testresultat avseende validitet.

| | 5.1 | 5.2 | 5.3 | 5.4 | 5.5 | 5.6 | 5.7 |
|---|---|---|---|---|---|---|---|
| **V** | 0,423 | 0,269 | 0,423 | 0,346 | 0,038 | 0,154 | 0,346 |
| **$V_{max}$** | 0,577 | 0,423 | 0,423 | 0,385 | 0,115 | 0,231 | 0,346 |
| **$T_1$** | 0,846 | 0,846 | 1,000 | 0,962 | 0,923 | 0,923 | 1,000 |
| **$T_2$** | 0,824 | 0,824 | 1,000 | 0,941 | 0,941 | 0,941 | 1,000 |

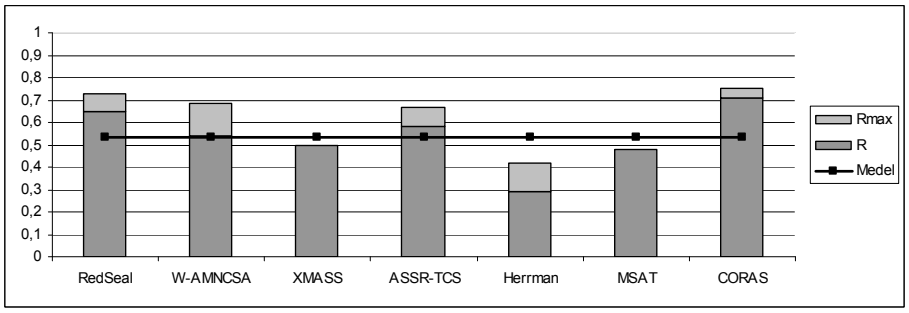
Följande diagram (Figur 5 till Figur 10) innehåller relevans (R) och maximal relevans ($R_{max}$), för de testade metoderna för P2 till P7 i IT-livscykelmodellen. Diagrammen innehåller även medelvärdet av relevansen (R) för de testade metoderna. I Figur 11 återfinns de testade metodernas validitet (V) och maximala validitet ($V_{max}$) samt medelvärdet av validiteten (V) för de testade metoderna.



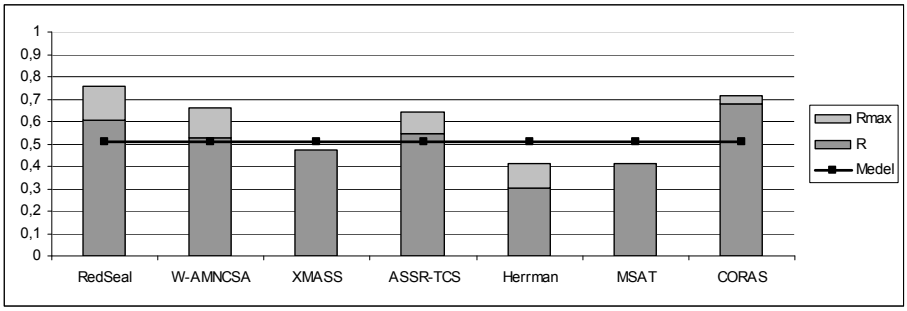

Figur 5: Relevans och maximal relevans för P2.



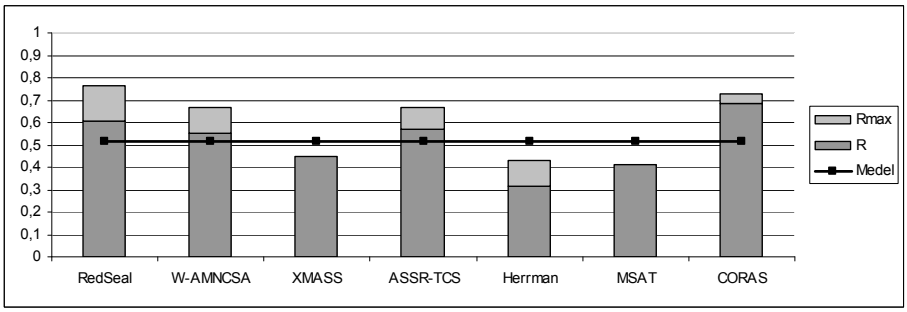

Figur 6: Relevans och maximal relevans för P3.



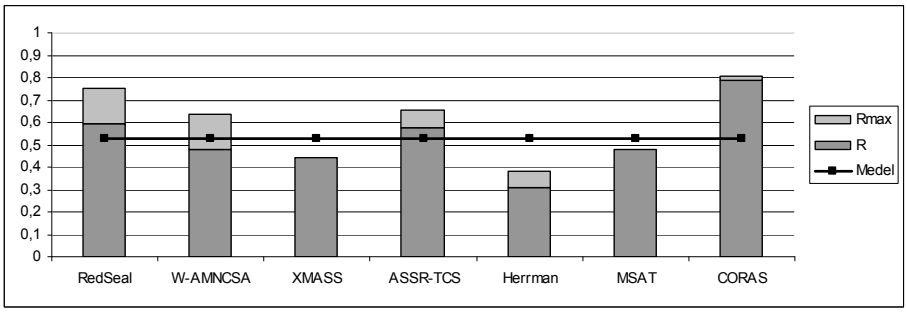

Figur 7: Relevans och maximal relevans för P4.



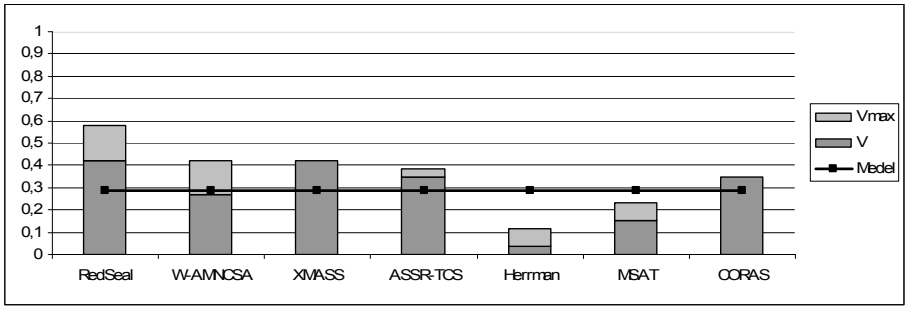

Figur 8: Relevans och maximal relevans för P5.




Figur 9: Relevans och maximal relevans för P6.




Figur 10: Relevans och maximal relevans för P7.




Figur 11: Validitet och maximal validitet.

# 7 Diskussion

En slutsats från genomförandet av litteraturstudien är att det är svårt att sålla ut relevanta metoder via sökningar i litteraturdatabaser, då begreppsapparaten är starkt diversifierad. Det finns stora skillnader i definitionerna av begrepp mellan de identifierade metoderna. Sammantaget ger detta att det är svårt att på ett systematiskt sätt hitta alla relevanta metoder för värdering av IT-säkerhet.

Från de 25 metoder som identifierades under litteraturstudien valdes sju metoder ut för testning. Den största anledningen till detta var att TSAR inte tidigare har använts för att testa ett större antal metoder. Tidigare testomgångar har endast innefattat en eller två metoder. Testen av metoderna i denna rapport blir alltså samtidigt en utvärdering av TSAR. Med anledning av detta gjordes testen med en begränsad mängd metoder. En metod från varje metodgrupp valdes ut, med undantag från den största gruppen (grafbaserad) från vilken två metoder valdes. På så sätt erhölls metoder med olika ansatser till värdering av IT-säkerhet.

De attribut och vikter som används för att representera de olika stegen i IT-livscykelmodellen är framtagna baserat på DIT04 (Försvarsmakten, 2004). För att testen ska ge relevans och validitetsvärden som direkt relaterar till situationer där värderingsbehov uppstår behövs en mer detaljerad indelning än den nuvarande indelningen i livscykelsteg. Mer detaljerade beskrivningar av värderingsbehoven underlättar verifiering av de valda attributen samt deras vikter.

I följande avsnitt diskuteras testresultaten för var och en av de testade metoderna, kopplingen mellan relevansattribut och de olika stegen i Försvarsmaktens IT-livscykelmodell samt möjlig vidareutveckling av TSAR.

## 7.1 Testresultat

I nuläget får fem av de sju testade metoderna liknande relevansvärden för alla steg i livscykeln. Nuvarande viktning av attributen gör att den testade metodens förmåga att modellera ett system får stor inverkan på relevansvärdet. Detta återspeglar sig i testet genom att metoden som saknar systemmodellering får lägsta värdena för både relevans och validitet, samtidigt som högsta relevansvärdena fås av den metod som har mest omfattande modelleringsteknik för systemmodellering.

För flertalet av det testade metoderna fås ett relevansvärde i livscykelsteg då metoden inte är tillämpbar. Huruvida en metod är tillämbar i ett specifikt steg av IT-livscykelmodellen framgår inte av testresultatet och är ett problem som diskuteras i Avsnitt 7.2.

### 7.1.1 RedSeal

RedSeal erbjuder automatisk modellering av system samt generering av en plan för nödvändiga åtgärder för att förbättra säkerheten vilket ger metoden hög relevans. Intressant att notera är att den inte är tillämpbar i P2 och P3 eftersom systemen implementeras först i P4.

I beskrivningen av metoden antyds vilka beräkningar som ligger till grund för värderingen, dock saknas detaljerade beskrivningar av hur resultat beräknas. Trots detta får metoden det högsta validitetsvärdet i testet (samma som XMASS), men värdet får fortfarande anses som lågt.

### 7.1.2 Weakest-Adversary Security Metric for Network Configuration Security Analysis

Metoden är teoretiskt väl beskriven och resultaten av en värdering är konkreta, men kopplingen till systemets säkerhet är otydlig. Skalbarheten i metoden är låg då antalet tillstånd i graferna växer snabbt. Metoden är inte tillämpbar i P2 eftersom systemet i detta steg beskrivs i form av krav vilket inte är giltig indata till metoden. Metoden bör vara mer relevant ju mer konkret systembeskrivningen är, med reservation för oförmåga att hantera systemets komplexitet. Detta illustreras av ökande relevansvärden för P3 till P6.

### 7.1.3 XMASS

Det är värt att poängtera att XMASS har 1 i täckningsgrad för både relevans och validitet, vilket beror på att metoden utvecklats på FOI och därför har alla eventuella tveksamheter kunnat redas ut. Metoden är inte applicerbar under P2 . I nuvarande version har metoden ej stöd för automatisk insamling av data under drift, vilket resulterar i lågt relevansvärde för P7.

### 7.1.4 Analyzing the security and survivability of real-time control systems

Metoden är tillräckligt generell för att vara tillämpbar i P3 till P7. Liksom metoderna ovan är inte heller denna tillämpbar i P2 då den saknar stöd för kravhantering. Metoden saknar också helt stöd för hur säkerhetsvärderingens indata ska fastställas.

### 7.1.5 Complete Guide to Security and Privacy Metrics

Denna metod skiljer sig från övriga metoder genom att den saknar stöd för systemmodellering. Istället sker värdering genom val av metriker ur en fördefinierad mängd av sådana. Relevansvärdena sänks också av bristen på

tydligt definierad metod. Författarens avsikt har inte varit att beskriva en metod för säkerhetsvärdering utan snarare för att underlätta valet av metriker. Syftet med metriker är dock att samla in data som underlag för beslut, vilket är ett av huvudsyftena med värdering. Även validiteten blir mycket låg, delvis beroende på att det helt saknas stöd för att beräkna säkerhetsvärden utgående från metrikerna.

### 7.1.6 Microsoft Security Assessment Tool

Detta är den enklaste metoden av dem som testats, vilket återspeglas i att en värdering beräknas ta en till två timmar att genomföra. Metoden har inget utrymme för egna anpassningar utan allt utgår från den uppsättning frågor som finns definierad. Metoden är inte tillämpbar i P2 då den saknar stöd för kravhantering. För övriga steg bör relevansen öka ju senare i livscykeln metoden appliceras. Detta återspeglas dock inte i testresultatet. Det finns ingen beskrivning av kopplingen mellan indata och värderingsresultat vilket ger låg validitet.

### 7.1.7 CORAS

Metodens syfte är egentligen inte värdering av IT-säkerhet utan snarare riskhantering för system i allmänhet. Trots att metoden inte fokuserar på problemen kring värdering av säkerhet har den fått högst relevans i alla livscykelsteg. Detta beror på att den har väl utvecklad systemmodelleringsteknik för alla typer av system samt ett generellt beskrivet användningsområde.

## 7.2 TSAR

Testningen av metoderna som presenterats i denna rapport visar att det finns utrymme för förbättringar av TSAR. I nuvarande version kan metoder som inte är applicerbara i en IT-livscykelsteg fortfarande få ett relevansvärde i detta steg. I dagsläget testar således TSAR hur relevant en metod är, förutsatt att det underlag metoden behöver finns tillgänglig. Exempelvis skiljer sig relevansvärdena för RedSeal i P2 och P3 inte nämnvärt från värdena i P4 till P7 trots att metoden inte kan användas i dessa steg.

Vidare visar det sig att de egenskaper som definieras i TSAR är väldigt modelleringstunga, vilket avspeglar sig i att en metod med generell modellering uppfyller ungefär 1/4 av egenskaperna i TSAR. Då egenskaper som relaterar till modellering har getts hög prioritet i flera IT-livscykelsteg kan en metod som bara skapar en modell få ett hyfsat relevansvärde trots att ingen värdering görs.

Utöver detta gör den generella naturen hos beskrivningarna av egenskaperna att mycket generella metoder, såsom CORAS, får höga värden eftersom de täcker in många av egenskaperna i TSAR-tabellerna.

Ytterligare en observation som gjorts är att de flesta metoder uppvisar egenskaper som är tvärt emot de som borde uppvisas gällande hur relevanta de är i olika livscykelsteg. CORAS får exempelvis högre relevans ju senare i livscykeln den appliceras, trots att metoden borde vara mest relevant i början. Vidare sjunker MSATs relevans ju senare i livscykeln den appliceras trots att relevansen rimligtvis borde öka ju närmare drift ett system är.

Med anledning av ovanstående har följande förbättringsmöjligheter för TSAR identifierats:

- Jämna ut kriteriernas genomslag på relevansvärdet så att modelleringen inte får så stort genomslag i resultatet
- Förtydliga kriteriebeskrivningarna och gör dem mer avgränsade bland annat genom att lägga in exempel
- Väldigt övergripande och ”luddigt” definierade metoder bör få lägre relevans än välspecificerade mer precisa metoder.
- Lägg in ett beroende av applicerbarhet för varje IT-livscykelsteg så att ej applicerbara metoder inte får relevansvärden i dessa steg.

## 7.3 Återkoppling till problemformulering

Resultaten från testerna visar att det inte finns några metoder som motsvarar de allmänna behov som nyttjades för att specificera vilka egenskaper metoderna ska ha för att anses vara relevanta för Försvarsmakten. En slutsats av detta är att det krävs mer specifika beskrivningar av situationer där värderingsbehov uppstår för att kunna testa metoder mer utförligt. En mer detaljerad beskrivning av Försvarsmaktens behov inom de olika IT-livscykelstegen leder till att stegen kan delas upp i mer specifika värderingssituationer. Detta i kombination med en utökning av egenskaperna i TSAR-tabellerna med tydligare beskrivningar och fler delegenskaper leder till att testerna bättre återspeglar relevansen hos metoden för den aktuella värderingssituationen. Alltså finns behov av att vidareutveckla TSAR för att på ett formaliserat sätt utvärdera vilka värderingsmetoder som motsvarar specifika behov.

# 8 Referenser

Aime, M. D., Atzeni, A., & Pomi, P. C. (2007). AMBRA: automated model-based risk analysis. *Proceedings of the 2007 ACM workshop on Quality of protection*, 43—48.

Balzarotti, D., Monga, M., & Sicari, S. (2005). Assessing the risk of using vulnerable components. In *Proceedings of the 2nd ACM workshop on Quality of protection*. Springer.

Basili, V., Caldiera, G., & Rombach, H. (1994). The goal question metric approach. *Encyclopedia of software engineering, John Wiley & sons*, *1*, 528-532.

Bengtsson, J., & Brinck, P. (2008). *Design and Implementation of an Environment to Support Development of Methods for Security Assessment*. Linköping University, Department of Electrical Engineering. Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-11307.

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

den Braber, F., Hogganvik, I., Lund, M., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps - a guided tour to the CORAS method. *BT Technology Journal*, *25*(1), 101-117.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance Measurement Guide for Information Security*. National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

Clark, K., Dawkins, J., & Hale, J. (2005). Security risks: Fusing enterprise objectives and vulnerabilities. In *Proc. from the Sixth Annual IEEE SMC Information Assurance Workshop*.

Clark, K., Tyree, S., Dawkins, J., & Hale, J. (2004). Qualitative and quantitative analytical techniques for network security assessment. In *Proc. from the Fifth Annual IEEE SMC Information Assurance Workshop*.

Dahl, H., Hogganvik, I., & Stølen, K. (2007). *Structured semantics for the CORAS security risk modelling language*. Technical report STF07 A970, SINTEF Information and Communication Technology.

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

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

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

Guo-Ming Lu, Zhi-Hong Chen, Xue-Zhi He, & Jian-Ping Li. (2008). A Method of Security Evaluation based on Fuzzy Mathematics. In *Apperceiving Computing and Intelligence Analysis, 2008. ICACIA 2008. International Conference on* (pp. 106-109).

Hallberg, J., Bengtsson, J., & Andersson, R. (2007). *Refinement and realization of security assessment methods*. Scientific report, Swedish Defence Research Agency, FOI.

Hallberg, J., Hallberg, N., & Hunstad, A. (2006). *Crossroads and XMASS: Framework and Method for System IT Security Assessment*. Scientific report, Swedish Defence Research Agency, FOI.

Herrmann, D. (2007). *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*. Auerbach Publications.

Hunstad, A., Hallberg, J., & Andersson, R. (2004). Measuring IT security - a method based on common criteria's security functional requirements. In *Proc. from the Fifth Annual IEEE SMC Information Assurance Workshop* (pp. 226-233).

Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley.

Johansson, E. (2005). *Assessment of Enterprise Information Security*. Royal Institute of Technology, KTH, Stockholm, Sweden.

Kondakci, S. (2007). A new assessment and improvement model of risk propagation in information security. *International Journal of Information and Computer Security*, *1*, 341-366.

Krings, A., & Azadmanesh, M. (2002). *A Graph Based Model for Survivability Analysis*. Technical Report UI-CS-TR-02-024, Computer Science Department, University of Idaho.

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

Manadhata, P., Wing, J., Flynn, M., & McQueen, M. (2006). Measuring the Attack Surfaces of Two FTP Daemons. In *ACM Computer and Communications Security (CCS) Workshop on Quality of Protection (QoP)*. Alexandria, Virginia, USA: ACM.

McLean, I., Szymanski, B., & Bivens, A. (2003). Methodology of Risk Assessment in Mobile Agent System Design. In *Proc. from the Fourth Annual IEEE SMC Information Assurance Workshop*.

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

Oman, P., Krings, A., Conte de Leon, D., & Alves-Foss, J. (2004). Analyzing the security and survivability of real-time control systems. In *Proc. from the Fifth Annual IEEE SMC Information Assurance Workshop* (pp. 342-349).

Pamula, J., Jajodia, S., Ammann, P., & Swarup, V. (2006). A weakest-adversary security metric for network configuration security analysis. In *Proc. 2nd ACM Workshop on Quality of Protection*.

RedSeal. (2009a). RedSeal Network Advisor: Product Overview. RedSeal. Retrieved from http://www.redseal.net/documents/RedSeal_Network_Advisor.pdf.

RedSeal. (2009b). RedSeal Vulnerability Advisor: Product Overview. RedSeal. Retrieved from http://www.redseal.net/documents/RedSeal_Vulnerability_Advisor.pdf.

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

Streilein, W., Kratkiewicz, K., Sikorski, M., Piwowarski, K., & Webster, S. (2007). PANEMOTO: Network Visualization of Security Situational Awareness Through Passive Analysis. In *Proc. from the 8th Annual IEEE SMC Information Assurance Workshop* (pp. 284-290).

Sundmark, T. (2008, December 19). *Improvement and Scenario-based Evaluation of the eXtended Method for Assessment of System Security*. Linköping University, Department of Electrical Engineering.

Svendsen, N., & Wolthusen, S. (2007). Analysis and Statistical Properties of Critical Infrastructure Interdependency Multiflow Models. In *Proc. from the 8th Annual IEEE SMC Information Assurance Workshop* (pp. 247-254).

Wang, L., Singhal, A., & Jajodia, S. (2007). Toward measuring network security using attack graphs. In *Proceedings of the 2007 ACM workshop on Quality of protection* (pp. 49-54). Alexandria, Virginia, USA: ACM. doi: 10.1145/1314257.1314273.

# Bilaga A – Förändringar av TSAR

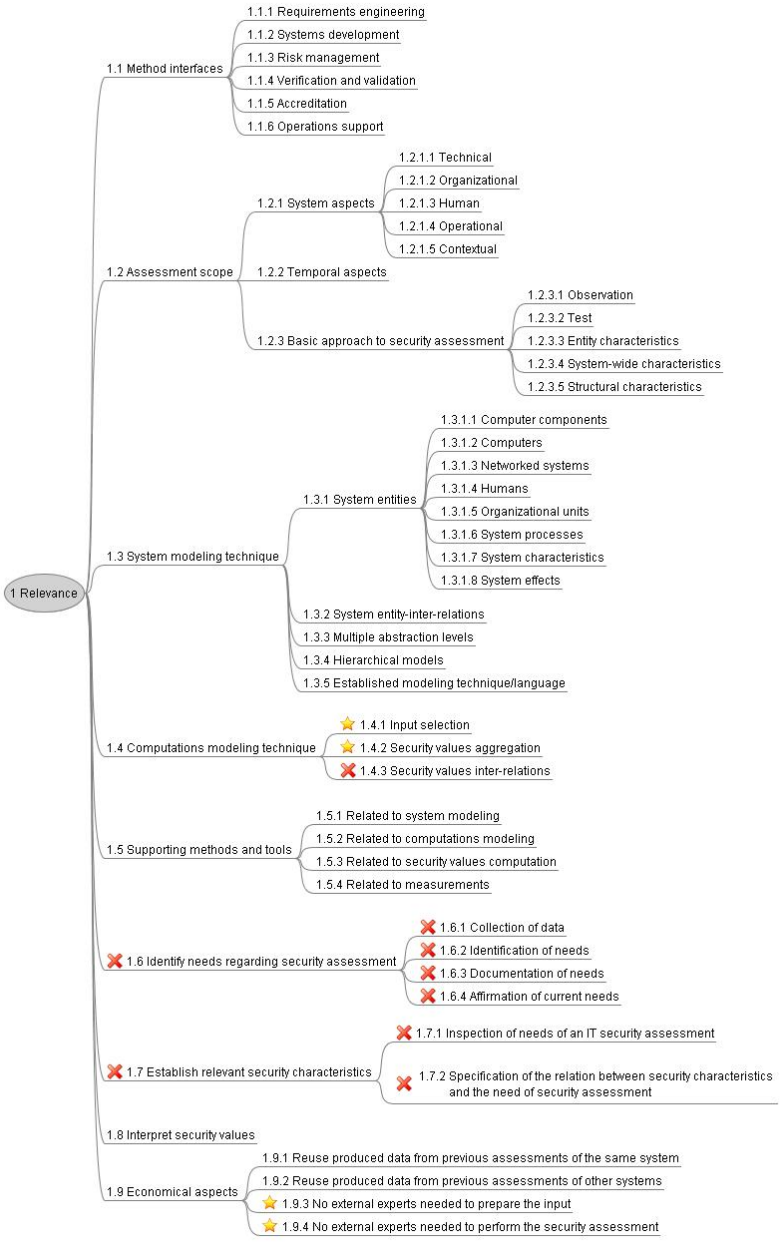
Uppsättningen av egenskaper i TSAR-tabellerna har förändrats jämfört med uppsättningen som definieras i metodbeskrivningen av TSAR (Bengtsson et al., 2008). En uppdaterad översikt återges i Figur 12. Den största förändringen är att egenskaperna 1.4.3, 1.6 med underliggande egenskaper, samt 1.7 med underliggande egenskaper har tagits bort från listan med relevansegenskaper. De fyra egenskaperna 1.4.1, 1.4.2, 1.9.3 samt 1.9.4 har definierats om. De nya definitionerna återges nedan.

| | |
|---|---|
| **ID** | 1.4.1 |
| **Name** | Input selection |
| **Type** | Atomic |
| **Abstract** | This characteristic specifies whether support exists for selecting the input values to the assessment method. |
| **Objective** | The assessment method has explicitly stated support for selection of input values to the assessment method.<br>Having the option to select input values to the assessment method makes it more flexible, thereby it is possible to adapt the assessment method to the current environment. |
| **Tags** | |

| | |
|---|---|
| **ID** | 1.4.2 |
| **Name** | Security values aggregation |
| **Type** | Atomic |
| **Abstract** | This characteristic specifies whether support exists for selecting or modifying how aggregated security values are derived. |
| **Objective** | The assessment method has explicitly stated support for selecting or modifying how security values are aggregated.<br>It should be possible to select the input values that should be aggregated and how the aggregation is performed. Selection could be made freely or from a predefined set. Aggregated security values are used to describe a combination of input values. Aggregated values are typically used to describe inter-relations between security values. |
| **Tags** | |

| | |
|---|---|
| **ID** | 1.9.3 |
| **Name** | No external experts needed to prepare the input |
| **Type** | Atomic |
| **Abstract** | This characteristic specifies whether preparation of the input to the security assessment can be performed *without* consulting external experts. |
| **Objective** | The assessment method has *no explicitly stated need* for experts when input to the security assessment is prepared.<br><br>The characteristic should be considered fulfilled if the assessment method *does not* require external experts to prepare the input to the method. |
| **Tags** | |

| | |
|---|---|
| **ID** | 1.9.4 |
| **Name** | No external experts needed to perform the security assessment |
| **Type** | Atomic |
| **Abstract** | This characteristic specifies whether assessment can be performed *without* consulting external experts. |
| **Objective** | The assessment method has *no explicitly stated* need for experts when the security assessment is performed.<br><br>The characteristic should be considered fulfilled if the assessment method *does not* require experts to perform the security assessment. |
| **Tags** | |




Figur 12: Översikt av relevanskriterier.