



FOI MEMO

Projekt/Project

Sidnr/Page no

Värdering av IT-säkerhetsnivå hos
system inom det nätverksbaserade
försvaret

1 (43)

Uppdragsnummer/Project no Kund/Customer

E7046

FÖRSVARSMAKTEN

Forskningsområde/Research area

Ledning med MSI/C4I and Human Factors

Datum/Date

Memo nummer/number

2007-06-19

FOI Memo 2099

Handläggare/Our reference

Jonas Hallberg

Handbok för IT-säkerhetsvärdering

Jonas Hallberg, Amund Hunstad, Niklas Hallberg

FOI MEMO	Datum/Date 2007-06-19	Sida/Page 2 (43)
Titel/Title Handbok för IT-säkerhetsvärdering		Memo nummer/number FOI Memo 2099

Handbok för IT-säkerhetsvärdering

Sammanfattning

Det finns idag ingen allmänt vedertagen ansats för hur värdering av IT-säkerhet ska genomföras. Detta trots att vetskap om vilken nivå av IT-säkerhet som system har är av stort värde för många olika organisationer och kategorier av användare. Denna rapport utgör en handbok i att genomföra värdering av IT-system avseende relevanta IT-säkerhetsegenskaper. Syftet är att (1) tydliggöra (a) områdets innehåll och avgränsningar, (b) vilket stöd som kan erbjudas och (c) vad som krävs för att kunna genomföra värderingar samt (2) utgöra ett stöd för genomförande av värderingar. Genomförandet av värderingen beskrivs som en process bestående av sex aktiviteter. Beskrivningen av aktiviteterna innehåller motivering av aktiviteten, viktiga aspekter att beakta, vilka indata aktiviteten förutsätter, vilka resultat som erhålls, vilka delaktiviteter som måste utföras, verktyg som kan nyttjas för att genomföra aktiviteten, diskussion av genomförandet samt ett exempel.

Innehåll

1	Inledning.....	7
1.1	Begrepp.....	8
1.2	Klargöranden.....	10
2	Bakgrund.....	12
2.1	IT-säkerhetsvärdering	12
2.2	Behovsanalys	13
2.3	Aktivitetsdiagram	14
3	Begreppsapparat för IT-säkerhetsvärdering.....	16
4	Process för IT-säkerhetsvärdering	18
4.1	Inventera behov av IT-säkerhetsvärdering	20
4.2	Fastslå relevanta IT-säkerhetsegenskaper	23
4.3	Överföra relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter.....	27
4.4	Mäta valda systemegenskaper och -effekter.....	33
4.5	Beräkna IT-säkerhetsvärden.....	36
4.6	Tolka IT-säkerhetsvärden	38
5	Referenser	42

1 Inledning

Komplexiteten hos och det ökande beroendet av informationssystem i olika sammanhang, medför att IT-säkerhetens betydelse ökar. För att åstadkomma lämplig säkerhetsnivå, rimliga säkerhetsinvesteringar och goda riskbedömningar, behövs adekvata sätt att värdera säkerhet. Tyvärr saknas metoder och verktyg som motsvarar dessa behov (ACSAC, 2002; Vaughn o.a., 2003; Seddigh o.a., 2004; Geer, 2006).

I denna handbok redogörs för hur IT-säkerhetsvärdering går till. Detta med syfte att:

- tydliggöra
 - områdets innehåll och avgränsningar,
 - vilket stöd som kan ges till den aktuella organisationens verksamhet och andra systemnära processer, såsom systemutveckling och
 - vilka krav som ställs för att kunna genomföra IT-säkerhetsvärdering samt
- utgöra ett stöd för det faktiska genomförandet av IT-säkerhetsvärdering.

För att åstadkomma detta beskrivs i handboken en process för hur IT-säkerhetsvärdering ska genomföras och ett urval av möjliga metoder och verktyg att använda i denna process. Den beskrivna processen för IT-säkerhetsvärdering består av sex olika huvudaktiviteter, vilka var för sig kan anpassas till aktuell värderings förutsättningar och behov.

Då IT-säkerhetsvärdering är ett omfattande och komplext område är handboken inte tillräckligt detaljerad för att värderingar direkt ska kunna baseras på denna. Istället utgör den en grund för att utveckla processer för IT-säkerhetsvärdering, vilka i olika utsträckning kan baseras på befintliga metoder och verktyg. Handboken utgör inte heller någon beskrivning av de metoder och verktyg för IT-säkerhetsvärdering som har framtagits av FOI. För detta refereras till andra dokument (Andersson o.a., 2003; Hallberg o.a., 2004; Andersson o.a., 2006; Hallberg o.a., 2006).

Handboken består av fyra kapitel. Återstående del av kapitel 1 introducerar ett antal begrepp som används i handboken. Kapitel 2 redovisar bakgrund till de presenterade resultaten. Kapitel 3 innehåller en begreppsapparat för IT-säkerhetsvärdering. Kapitel 4 presenterar IT-säkerhetsvärdering som en process bestående av sex olika aktiviteter.

1.1 Begrepp

I detta avsnitt definieras begrepp som används i denna handbok och som är av vikt för IT-säkerhetsvärdering. Begreppsdefinitionerna är anpassade till handbokens omfång (dvs. IT-säkerhetsvärdering) och kan ha annorlunda tolkningar inom andra områden. Efter begreppen finns, inom parenteser, eventuella kortformer av begreppen som används i texten.

Behov beskriver stöd som hos någon/något ska uppfylla sitt syfte. Användare har i sin tur behov av stöd för att genomföra aktiviteter. Behov kan vara antingen medvetna eller omedvetna, samt verkliga eller upplevda. 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 oönskad händelse med för en verksamhet negativa konsekvenser (SIS, 2003).

Intressenter har ett intresse av att en IT-säkerhetsvärdering blir genomförd.

Informationssystem behandlar, dvs. insamlar, bearbetar, lagrar och distribuerar information. Termen har en allmän innebörd, men används oftast för *datorstödda informationssystem*. I definitionen innefattas såväl ett systems tekniska utrustning som dess mänskliga aktiviteter och rutiner. (Nationalencyklopedin, 2007)

Informationssäkerhet relaterar till informationstillgångar samt förmåga att upprätthålla säkerhetsrelaterade egenskaper såsom sekretess, korrekthet och tillgänglighet.

IT-system (system) utgör ett informationssystem tekniska utrustning och gränssnitten mot denna tekniska utrustnings omgivning. Därmed kan kopplingar till mänskliga aktiviteter och rutiner som påverkar den tekniska utrustningen ingå i IT-systemet, även om dessa mänskliga aktiviteter och rutiner i sig inte ingår.

IT-säkerhet (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, 2003). Då definitionen utgår från begrepp som obehörig åtkomst, förändring respektive störning, lyfts aktörsperspektivet fram, med andra ord IT-säkerhet exkluderar inte aktörer, även om fokus är på IT-systemet.

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

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

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

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

Metod är en teoretisk beskrivning av tillvägagångssätt.

Metriker består av tre delar: storhet, skala och tolkning (Hallberg o.a., 2004).

Risk är produkten av sannolikheten för att ett givet hot realiserar och därmed uppkommande skadestånd (SIS, 2003).

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

Systemaspekt används för att beskriva huvudkategorier för olika delar av system. Dessa är organisatoriska, humana, tekniska, operativa och kontextuella systemaspekter.

Systemeffekter utgörs av skeenden som orsakas av system. Systemeffekter som kan härledas till systems IT-säkerhet kan användas för att beskriva denna IT-säkerhet hos systemen. Till exempel kan antalet virusinfektioner användas som ett mått på förmågan att hantera skadlig kod. Då är virusinfektion en systemeffekt och förmåga att hantera skadlig kod en IT-säkerhetsegenskap.

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

Systemkontext beskriver den omgivning som system verkar i. I första hand avses de aspekter och egenskaper i omgivningen som påverkar hur system utformas, dvs. vilka krav som ställs på systemet.

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

1.2 Klargöranden

Det är svårt att strikt definiera IT-säkerhetsrelaterade begrepp så att deras innebörd och användning är helt fastslagen. Gränsdragningar är av vikt, men för hårt dragna gränser riskerar att försvåra resonemang och analys. Sådana avvägningar ligger bakom definitionerna ovan. Ett par områden som förtjänar specifika klargöranden relaterar till begreppen IT-säkerhet, informationssystem och IT-system samt vilka systemaspekter som ingår vid IT-säkerhetsvärdering

Vid IT-säkerhetsvärdering studeras situationer av obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning *vid databehandling samt dator- och telekommunikation*. Däremot studeras *inte* obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning *vid manuell hantering av information*. Det senare ingår i informationssäkerhet, men inte i IT-säkerhet.

Likaså studeras tekniska system och påverkan från användare och övrig omgivning på dessa, dock värderas inte användarna och övrig omgivning i sig. En enklare avgränsning vore att hårt sätta gränsen för vad som studeras vid IT-systemets teknik, men en sådan avgränsning gör att många faktorer som påverkar tekniken faller bort. Det är av vikt att inse att IT-säkerhet handlar om säkerhet i IT-system, inte vilken säkerhet IT-systemen själva ger. Därmed måste fler systemaspekter än den tekniska beaktas. En parallell är personsäkerhet som innefattar mycket mer än egenskaper hos de personer vars säkerhet avses. Därför ingår kopplingar till mänskliga aktiviteter och rutiner som påverkar den tekniska utrustningen i IT-systemet, när detta är rimligt för värderingen. Precis var avgränsningen görs mellan omgivning och påverkan från omgivning kan variera och måste klargöras i respektive värderingsfall.

Lösenordshantering kan som exempel illustrera detta. Om ett IT-system har en väl fungerande teknisk lösenordshantering, kan detta ändå omkullkastas av slarvighet hos användare som sätter upp lappar med lösenord på sina skärmar och på annat sätt sprider lösenord. För att få en användbar och realistisk IT-säkerhetsvärdering, är

det därför inte rimligt att avgränsa värderingen hårt till endast den tekniska lösenordshanteringen. Kopplingen till den mänskliga aktiviteten att vårdslöst sprida lösenord är högst rimlig att ta med, även om man inte analyserar den mänskliga aktiviteten i sig. Därmed beaktas den vårdslösa mänskliga lösenordshanteringen och dess effekter på den tekniska lösenordshanteringen, men inte varför människor är vårdslösa.

2 Bakgrund

I detta kapitel ges ett förtydligande av området IT-säkerhetsvärdering och dess avgränsningar. Då IT-säkerhetsvärdering ska baseras på intressenters behov, presenteras även området behovsanalys. I kapitlet *Process för IT-säkerhetsvärdering* används aktivitetsdiagram för processmodellering, varför en introduktion till aktivitetsdiagram återfinns i detta kapitel.

2.1 IT-säkerhetsvärdering

IT-säkerhetsvärdering syftar till att öka kunskapen om kvaliteter avseende IT-säkerhet hos system. Denna kunskap behövs inom ett antal informationssystemnära processer, såsom riskhantering, systemutveckling och systemdriftstöd, men även för beslutsunderlag avseende till exempel resursallokering inom organisationer. Detta medför en stor spännvidd avseende krav på värderingens resultat och dess omfattning beroende på aktuell situation och givna förutsättningar. Värderingar kan exempelvis utgöras av ad hoc-mässigt resonerande alternativt omfattande, detaljerade och resurskrävande evalueringar.

IT-säkerhetsvärderingar kan utgöra relevant underlag för riskhantering genom att kvantifiera systems sårbarheter. Det är av vikt att inte förväxla säkerhets- och riskbegrepp med varandra. IT-säkerhet relaterar till egenskaper och effekter inom informationssystem. Riskresonemang inkorporerar även externa faktorer, det vill säga hot initierade av hotagenter, och konsekvenser, det vill säga skadekostnader. Hotagenter utnyttjar sårbarheter i system för att realisera de möjliga, oönskade händelser som ett hot utgör.

För att exemplifiera vad de olika termerna innebär, återgår vi till det i inledningen omnämnda exemplet med lösenordshantering. Lappar med lösenord uppsatta på skärmar utgör en sårbarhet, som därmed kan räknas in i det studerade systemet att värdera. En illvillig person (hotagent) som utnyttjar denna sårbarhet initierar därmed ett hot mot systemet, men hotagenten och hotet ingår, i enlighet med tidigare resonemang, inte i det studerade systemet.

Med avseende på värdering av säkerhet respektive risk, resonerar Hallberg o.a. (2004) i termer av tre olika begrepp:

- *Säkringsbarhet* är en designegenskap hos informationssystem, som anger en bedömning av till vilken nivå system kan säkras till vid användning. Detta medför att säkringsbarheten är konstant given en viss design. Först vid ändring av designen kan säkringsbarheten ändra sin nivå.

- *Säkerhetsnivå* värderas för system i drift med beaktande av operativa aspekter, såsom konfiguration och underhåll.
- *Riskenivå* bedömer även hot, hotagenter och skadestnader.

Systemets omfattning, rumsligt såväl som vilka systemaspekter (organisatoriska, humana, tekniska och operativa) som ska beaktas, måste bestämmas. Tillvägagångssätt för värderingen måste också specificeras, till exempel avseende detaljeringsgrad. Kortfattat kan detta beskrivas med begreppen *vad* och *hur*:

- *Systemomfattning* besvarar frågan: *Vad ska värderas?*
- *Tillvägagångssätt för värdering* besvarar frågan: *Hur ska värderingen gå till?*

Ett centralt begrepp inom IT-säkerhetsvärdering är metriker. Hallberg o.a. (2004) diskuterar metriker som bestående av tre delar: storhet, skala och tolkning. Säkerhetsvärden är, enligt denna syn, kopplade till en viss storhet och relaterade till en skala. Vidare innebär definitionen av säkerhetsmetriker att fokus sätts på vilka storheter som lämpar sig för mätning och vilken representation (skala) som lämpligast ska användas för värdena. För enkla mätningar, som av temperatur, är uppbyggandet av metriker relativt enkelt. De betydligt komplexare samband och beroenden som säkerhetsvärden måste avspegla innebär att uppbyggandet, eller designen, av säkerhetsmetriker blir betydligt svårare. (Bengtsson, 2007)

2.2 Behovsanalys

De flesta har en intuitiv förståelse för vad begreppet *behov* står för, men upplever det svårt att exakt förklara dess innebörd. I denna rapport motsvarar begreppet *behov* *brist*. Det finns ett behov av kunskap, det vill säga en *brist* på kunskap.

Behovsanalys innebär att identifiera och analysera behov. Det finns ett flertal olika ansatser för att genomföra detta. Den enklaste formen är att, baserat på individuella intervjuer, försöka tolka vilka behov som finns (McClelland, 1994a). Det är dock viktigt att notera att användare och övriga intressenter sällan har förmåga att formulera konkreta behov, utan formulerar dessa i form av problem som de upplever och lösningar som de tror skulle tillfredställa deras behov (Hallberg, 1999). Vidare så ger de inte uttryck för samtliga typer av behov, utan enbart de som de tror kan lösas. Behov som intressenterna upplever som självklara, vilket de inte behöver vara för den som genomför behovsanalysen, eller inte ser som möjliga att uppfylla, utelämnas (Kano, 1995).

Fokusgrupper kan nyttjas för att fördjupa kunskapen utifrån redan insamlad information kring vilka behov som föreligger (McClelland, 1994b). En variant på fokusgrupper, som dock inte kräver tidigare insamlad information, är "Future workshop" vilka genomförs som tre sekventiella "brainstorming"-aktiviteter med

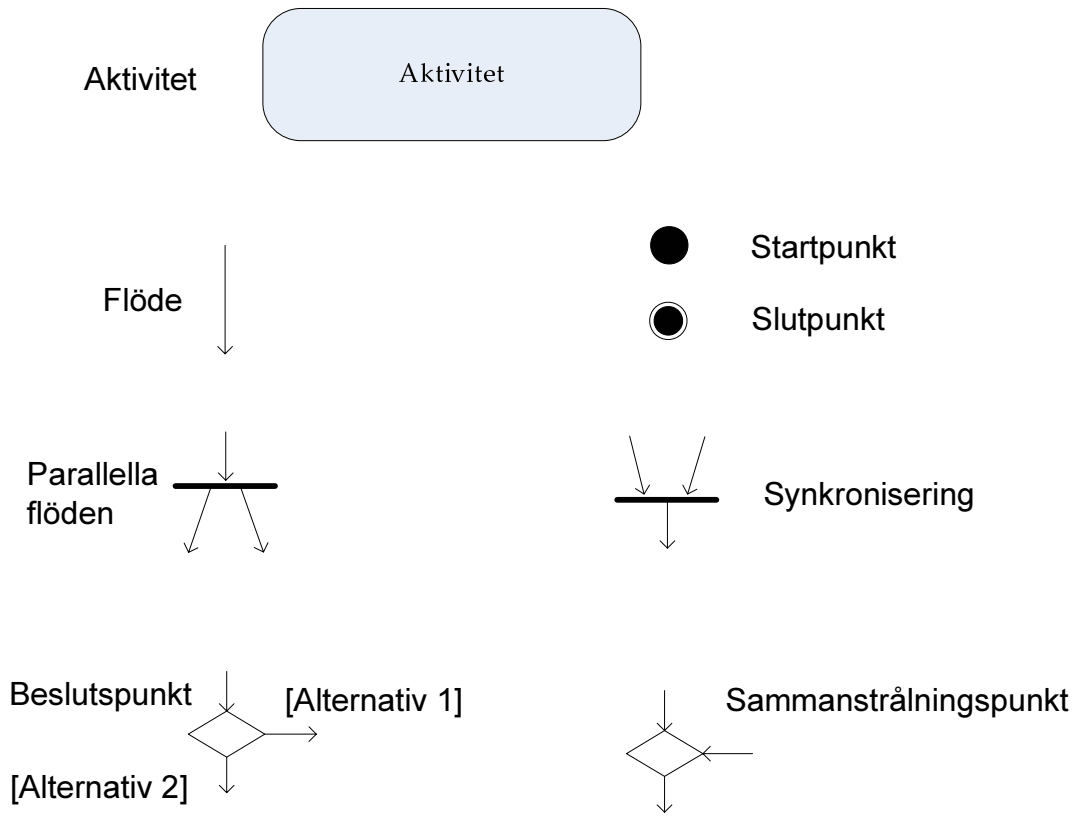
syfte att klarlägga: (1) problem, (2) visionära lösningar och (3) realiserbara lösningar (Kensing & Halskov Madsen, 1991). Den information som erhålls i ett steg används som utgångsläge för det efterkommande steget. Till exempel är det de problem som identifieras under den första aktiviteten som de visionära lösningarna ska tillgodose. Under samtliga aktiviteter kan det komma upp behov, men det är främst den första aktiviteten, där de problem som finns kartläggs, som kan användas för att identifiera behov (brister). Även enkäter och frågeformulär används för att identifiera behov (McClelland, 1994b). En typ av enkäter som bygger på The critical incident technique (Flanagan, 1954) har vist sig vara användbara vid behovsanalyser (Ölvingson o.a., 2002).

Även analyser av styrande dokument kan vara ett sätt att ta fram behov. En metod som kan användas för detta är *Kvalitetsdriven kravhantering* där varje utsaga i texter analyseras minutiöst baserat på frågorna: *vem* behöver det identifierade, *när* behövs det, *var* behövs det, *vad* anses behövas samt *hur* ser de att behovet skulle kunna tillfredställas. Därefter kategoriseras och struktureras behoven samtidigt som formuleringar skärps och dubletter tas bort. Denna analys ger underlag för att kunna fastställa de faktiska behoven. (Hallberg o.a., 2005a)

2.3 Aktivitetsdiagram

Aktivitetsdiagram används för att modellera dynamiken hos system genom att visa flöden av aktiviteter. Det vill säga i vilken ordning aktiviteter sker, samt beslutspunkter, alternativa och parallella flöden.

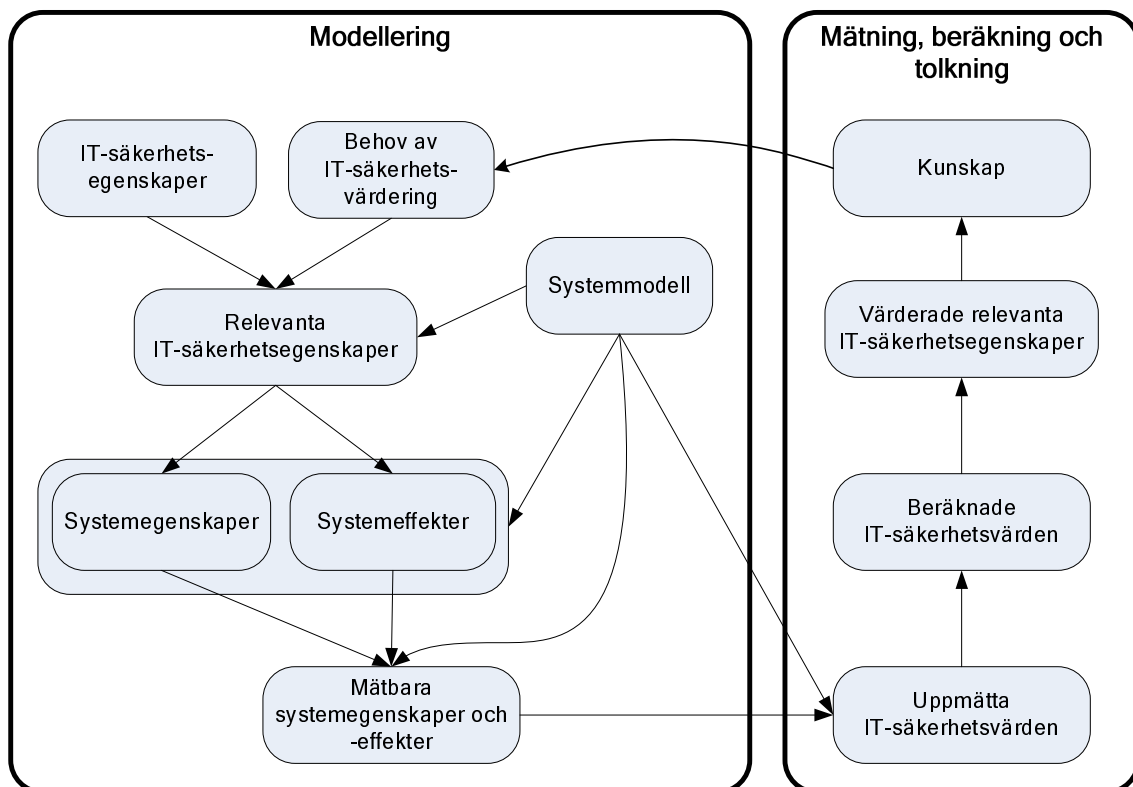
Aktivitetsdiagram är en av notationerna i UML (Unified Modeling Language) som främst används inom programvaruutveckling, men som vunnit allt större användning inom andra områden som exempelvis verksamhetsmodellering. Inom systemutveckling utgör aktivitetsdiagram ett komplement för att förtydliga och detaljera beskrivningar av användningsfall. Genom att använda sig av så kallade simbanor, kan även vem som gör vad beskrivas med aktivitetsdiagram, det vill säga vilken aktör som utför en given aktivitet. Aktivitetsdiagram innehåller sex olika symboler: aktivitet, flöde, parallellt flöde, synkronisering, beslutspunkt och sammanstrålningspunkt (Figur 1).



Figur 1: Symboler för aktivitetsdiagram.

3 Begreppsapparat för IT-säkerhetsvärdering

Vid genomförande av IT-säkerhetsvärdering är det väsentligt med en begreppsapparat som tydliggör vilken terminologi som används. I Figur 2 återfinns centrala termer inom IT-säkerhetsvärdering och relationer mellan dessa. I detta kapitel beskrivs dessa termer, vilka i texten markeras med kursiv stil där de introduceras. Termerna är uppdelade i de två huvudkategorierna *modellering* respektive *mätning, beräkning och tolkning*.



Figur 2: Begreppsapparat för IT-säkerhetsvärdering.

Värdering är inget självändamål utan syftar till att uppfylla behov hos andra processer, såsom riskhantering, systemutveckling och systemdriftsstöd. Dessa *behov av IT-säkerhetsvärdering* utgör en del av grunden för genomförandet av värdering. De övriga grundstenarna består av modeller av aktuella system och en uppsättning av IT-säkerhetsegenskaper. *IT-säkerhetsegenskaper* används för att beskriva IT-säkerhet hos system. Exempel på övergripande IT-säkerhetsegenskaper är sekretess, tillgänglighet och korrekthet. En ändamålsenlig uppsättning av säkerhetsegenskaper är avgörande för framgångsrik IT-säkerhetsvärdering. *Systemmodeller* innehåller de data som kan användas för att beskriva systemets IT-säkerhetsegenskaper. Detta betyder att en värdering aldrig kan bli bättre än den modell som den utgår ifrån. Systemmodeller kan vara explicit specificerade eller implicit finnas i personers medvetande. Inom ramen för säkerhetsvärdering byggs systemmodellen upp successivt.

Relevanta IT-säkerhetsegenskaper är de egenskaper som används för att beskriva IT-säkerheten i det aktuella systemet. Säkerhet kan i allmänhet inte mätas direkt i form av övergripande IT-säkerhetsegenskaper som exempelvis sekretess, tillgänglighet och korrekthet. Därför måste andra, mer specifika säkerhetsegenskaper analyseras. Dessa kan vara *systemegenskaper* som påverkar IT-säkerheten (exempelvis säkerhetsfunktioner) eller *systemeffekter* som beror av aktuell säkerhet (exempelvis intrång). Inte heller alla systemegenskaper och -effekter kan mätas, utan måste brytas ner till *mätbara systemegenskaper och -effekter* erhålls. Systemeffekter kan anses ligga utanför systemmodellen, men den information som behövs för att avgöra vilka systemeffekter som ska mätas erhålls från systemmodellen.

Uppmätta IT-säkerhetsvärden är de resultat som erhålls vid mätning av identifierade mätbara systemegenskaper och -effekter. *Beräknade IT-säkerhetsvärden* erhålls genom aggregation av uppmätta värden. *Värderade relevanta IT-säkerhetsegenskaper* utgör de tolkade slutresultaten av mätningarna och beräkningarna av IT-säkerhetsvärden.

Syftet med värdering av IT-säkerhet är att öka kunskapen om kvaliteter avseende IT-säkerhet hos system. Denna *kunskap* erhålls från de värderade relevanta IT-säkerhetsegenskaperna och ska motsvara de behov som var ursprunget till värderingsprocessen.

4 Process för IT-säkerhetsvärdering

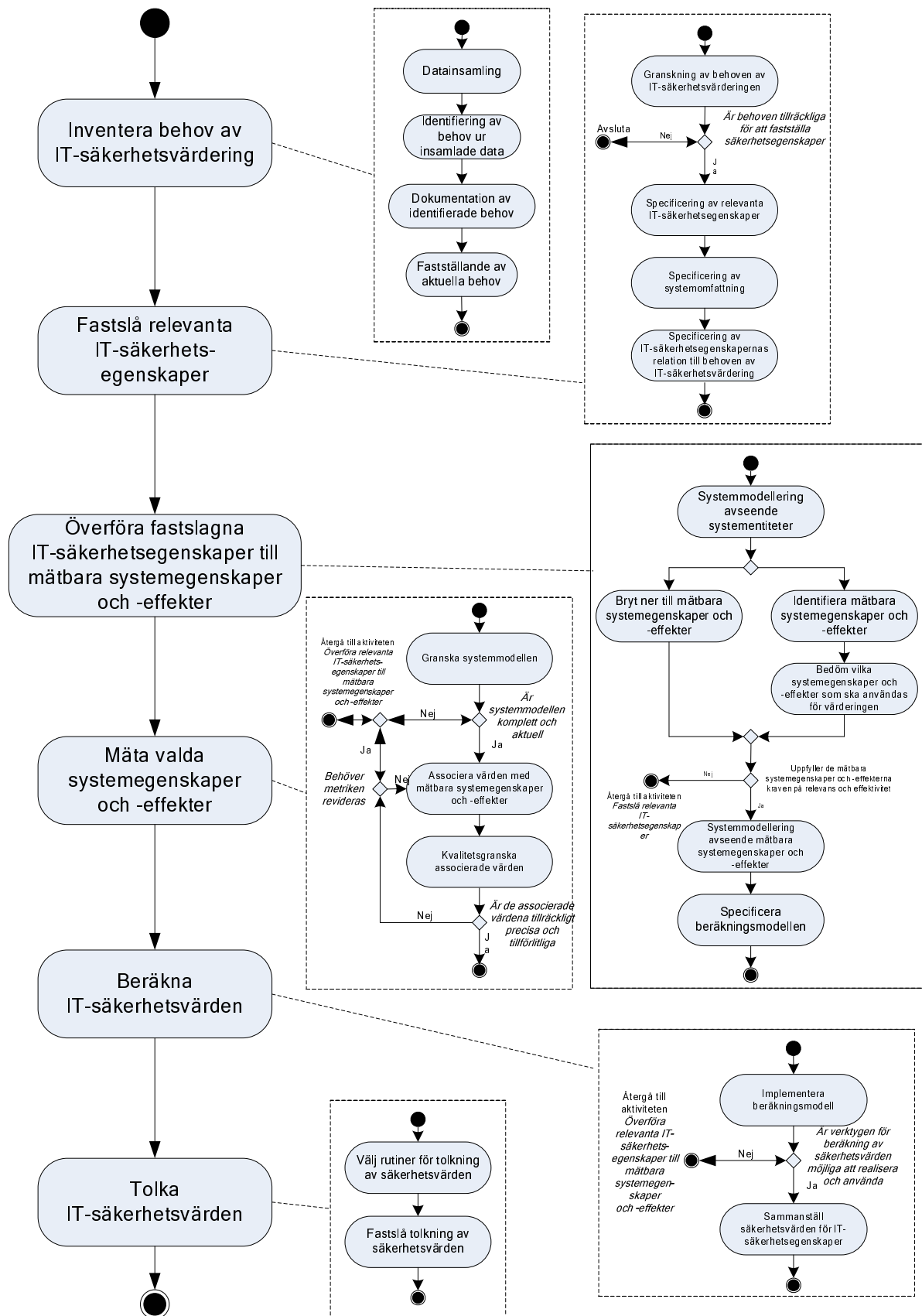
I detta kapitel presenteras strukturen hos processen för IT-säkerhetsvärdering respektive de ingående aktiviteternas uppbyggnad och funktion. Processen för IT-säkerhetsvärdering (Figur 3) består av de sex aktiviteterna:

- inventera behov av IT-säkerhetsvärdering,
- fastslå relevanta IT-säkerhetsegenskaper,
- överföra fastslagna IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter,
- mäta valda systemegenskaper och -effekter,
- beräkna IT-säkerhetsvärden samt
- tolka IT-säkerhetsvärden.

Processer för IT-säkerhetsvärdering syftar till att ge innehåll åt de termer som introducerades inom ramen för begreppsapparaten i föregående kapitel. Därmed finns det en tydlig koppling mellan Figur 2 och Figur 3. Skillnaden är att Figur 2 fokuserad på terminologi medan Figur 3 illustrerar aktiviteter. Båda dessa figurer har också en tydlig koppling till ramverket Crossroads (Hallberg o.a., 2006). Crossroads tar dock sin utgångspunkt i hur metoder för IT-säkerhetsvärdering ska kunna kategoriseras, inte hur den fullständiga processen kan beskrivas.

Var och en av aktiviteterna beskrivs avseende:

- motivering, varför den aktuella aktiviteten är en väsentlig del av processen för IT-säkerhetsvärdering.
- viktiga aspekter, frågor av speciell vikt för genomförandet av aktiviteten,
- ingångsvärden, de data som behövs för att kunna genomföra aktiviteten,
- resultat, resulterande utdata efter genomförandet,
- ingående delaktiviteter, uppräknig av de delaktiviteter som har identifierats för aktiviteten,
- verktyg, vilka stöd finns för att genomföra aktiviteten,
- genomförande, på vilket eller vilka sätt kan aktiviteten genomföras, beskrivs utgående från angivna delaktiviteter,
- tillämpningsexempel, illustrationer av hur aktiviteten kan genomföras.



Figur 3: De sex aktiviteter som ingår i en säkerhetsvärderingsprocess samt miniatyrer av de aktivitetsdiagram som beskriver deras utförande i avsnitten 4.1 till 4.6 (Figur 4 till 9).

4.1 Inventera behov av IT-säkerhetsvärdering

Syftet med denna aktivitet är att identifiera, dokumentera och fastslå de relevanta behoven av den IT-säkerhetsvärdering som ska genomföras. Dessa behov används för att ta fram de relevanta IT-säkerhetsegenskaper som IT-säkerhetsvärderingen baseras på. Behoven formuleras utifrån att det finns en brist på kunskap om systems IT-säkerhet, i avseenden som har betydelse. Det vill säga behov som ligger till grund för värderingen bör formuleras "Behov av att veta ...".

4.1.1 Motivering

För att maximera nyttan av IT-säkerhetsvärderingar ska dessa baseras på aktuella och relevanta behov. För att undvika diskrepanser mellan intressenters förväntningar och IT-säkerhetsvärderingsprocessens resultat, avseende exempelvis omfattning, upplösning och kvalitet, är det viktigt att alla är överens om utformningen av de behov som ska adresseras av värderingsprocessen.

4.1.2 Viktiga aspekter

Det är lätt att begå misstaget att formulera värderingsprocesser utifrån vilka metoder och verktyg som finns att tillgå. Värderingsprocesser måste dock utgå ifrån vilka behov som intressenterna har. Nyttjande av metoder och verktyg ska endast syfta till att uppfylla dessa behov. Därför är det viktigt att behoven klargörs och tydligt dokumenteras samt att giltigheten fastställs i samråd med intressenterna.

De identifierade behoven kan vara av vitt skilda slag och härstamma från olika intressenter. Det blir då ett designbeslut att avgöra ifall alla behoven ska hanteras av en bred värderingsprocess, som i princip bygger på flera parallella delprocesser, eller om behoven ska grupperas och en värderingsprocess initieras per behovsgrupp.

När det gäller IT-säkerhetsvärdering kommer en stor del av behoven från andra processer, såsom riskhantering, systemutveckling och driftsstöd, vilka alla krävs för att informationssystem ska fungera väl. Om de inte är givna, krävs det en insats för att kartlägga vilka dessa processer är så att de kan beaktas under behovsanalysen.

4.1.3 Ingångsvärden

Dataunderlag för behovsanalysen utgörs av exempelvis:

- uttalanden av och förfrågningar från ledningen,
- intressent- och expertkunskap,
- efterfrågade ingångsdata till processer för riskhantering, systemutveckling och driftsstöd,
- policydokument,

- förändrad hotbild,
- lagar och regler samt
- externa styrningar och förfrågningar.

4.1.4 Resultat

Resultat av aktiviteten är en (strukturerad) uppsättning behov, vilken motiverar och vägleder genomförandet av IT-säkerhetsvärderingen.

4.1.5 Ingående delaktiviteter

I aktiviteten att inventera IT-säkerhetsvärderingsbehov ingår följande delaktiviteter:

- datainsamling,
- identifiering av behov ur insamlade data,
- dokumentation av identifierade behov samt
- fastställande av aktuella behov.

4.1.6 Verktyg

För genomförande av aktiviteten finns en uppsättning olika verktyg för behovsanalys att tillgå, avsnitt 2.2, exempelvis:

- intervjuer,
- kvalitativ textanalys,
- fokusgrupper, "future workshop",
- kundrösttabell,
- relationsdiagram,
- hierarkiska diagram samt
- användnings- respektive felanvändningsfall.

4.1.7 Genomförande

Ett flertal olika sätt att genomföra behovsinventeringen är tänkbara. Detta avsnitt utgår ifrån att en ansats baserad på *kvalitetsdriven kravhantering* (se avsnitt 2.2) tas (Figur 4).

Datainsamling

Insamling av data kan baseras på intervjuer med intressenter och experter, analys av relevanta dokument etc. Resultatet av delaktiviteten ska vara en samling med texter såsom intervjutranskriptioner och dokument.

Identifiering av behov ur insamlade data

Behovsidentifiering kan genomföras med hjälp av följande steg:

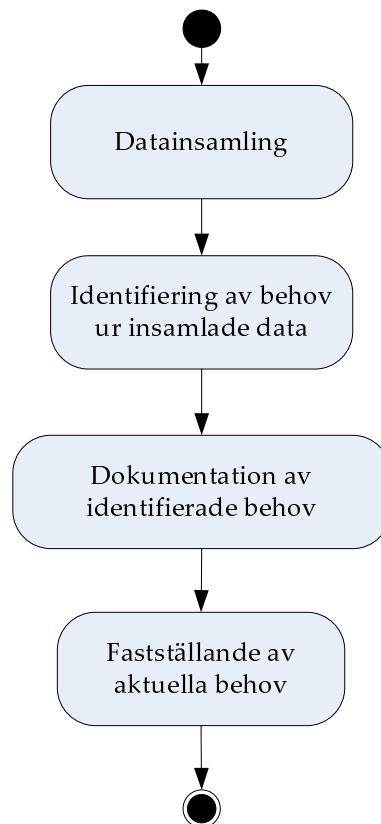
- identifiera utsagor ur insamlade data rörande IT-säkerhetsvärderingsbehov med hjälp av textanalys,
- analysera utsagor och identifiera behov med hjälp av kundrösttabell samt
- analysera och strukturera behoven med hjälp av relationsdiagram och hierarkiska diagram

Dokumentation av identifierade behov

De identifierade behoven dokumenteras enklast som löpande text. Om det är många behov och att dessa är på olika abstraktionsnivå, kan hierarkiska strukturer nyttjas, exempelvis med rubriker och underrubriker. För att öka tydligheten kan de identifierade behoven även modelleras med användningsfall och felanvändningsfall.

Fastställande av aktuella behov

När behoven har analyserats och dokumenterats ska de godkännas och eventuellt prioriteras av intressenterna.



Figur 4: IT-säkerhetsvärderingens första aktivitet; inventera behov av IT-säkerhetsvärdering.

4.1.8 Tillämpningsexempel

I organisation X har ledningen uttryckt oro över att känsliga data kan komma på avvägar beroende på att de lösenord som användarna av Xs informationssystem nyttjar inte är tillräckligt bra eller att de sprids till obehöriga.

Utsagan "är lösenordshanteringen tillräckligt bra" ger behovet "behov av att veta hur bra skyddet mot otillbörlig spridning av Xs data är". Detta behov förankras hos Xs ledning.

4.2 Fastslå relevanta IT-säkerhetsegenskaper

Syftet med denna aktivitet är att fastslå vilka IT-säkerhetsegenskaper hos det studerade systemet som ska värderas. Dessa egenskapers värdering ska motsvara de, under den första aktiviteten, fastslagna behoven av IT-säkerhetsvärdering och göra det möjligt att beskriva systemets IT-säkerhetsnivå på ett för intressenterna meningsfullt sätt.

4.2.1 Motivering

Genomförande av adekvata, giltiga och tillförlitliga IT-säkerhetsvärderingar kräver att värderingen utgår från relevanta IT-säkerhetsegenskaper hos det studerade systemet. Därmed måste dessa relevanta IT-säkerhetsegenskaper fastslås innan värderingsprocessen kan fortsätta.

4.2.2 Viktiga aspekter

Relevanta IT-säkerhetsegenskaper skapar förutsättningar för uppfyllande av behov av IT-säkerhetsvärdering genom att ta hänsyn till:

- vilka egenskaper resultaten av IT-säkerhetsvärdering ska ha för att motsvara intressenternas behov,
- vilka egenskaper processen för IT-säkerhetsvärdering ska ha, avseende exempelvis resursförbrukning och tid det tar att få fram resultat samt
- det system som IT-säkerhetsegenskaperna ska värderas för avseende
 - gränsdragning mellan det studerade systemet och dess omgivning,
 - vilka systemaspekter som ska ingå samt
 - vilka delar av systemets livscykel som ska beaktas, det vill säga systemet, eller delsystemen, är under utveckling, i drift eller under avveckling.

Det är av vikt att klargöra dessa gränser, som varierar mellan olika värderingar och som tydligt påverkar tänkbara resultat, värderingskomplexitet och realism i värderingen. Det har också direkt påverkan på vilka av de fem huvudansatserna till värder-

ing som kan användas. De fem huvudansatserna är observation av systemeffekter, testning av systemeffekter, granskning av systemegenskaper, granskning av egenskaper hos systementiteter samt granskning av systemstruktur (Hallberg o.a., 2006). Till exempel kan inte observation och testning av systemeffekter användas för system, eller delsystem, som ännu inte har realiserats.

Relevanta IT-säkerhetsegenskaper kan vara direkt mätbara eller mera övergripande kvaliteter som svårigen låter sig mätas. Nedbrytningen av övergripande säkerhetsegenskaper till mätbara systemegenskaper och -effekter sker i processens tredje aktivitet *Överföra relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter*.

4.2.3 Ingångsvärden

Ingångsvärden till aktiviteten utgörs av:

- behov av IT-säkerhetsvärdering samt
- uppsättningar med IT-säkerhetsegenskaper.

Om behoven inte är kända eller diffusa, finns risk att värderingen baseras på säkerhetsegenskaper utan tillräcklig relevans. Fördefinierade uppsättningar av säkerhetsegenskaper underlättar genomförandet av aktiviteten.

4.2.4 Resultat

Resultatet av att genomföra aktiviteten är:

- en uppsättning, för värderingen, fastslagna relevanta säkerhetsegenskaper,
- beskrivningar av hur de relevanta säkerhetsegenskaperna förhåller sig till behoven av IT-säkerhetsvärderingen samt
- en specificering av omfattningen av det system som ska värderas, det vill säga en initial systemmodell.

4.2.5 Ingående delaktiviteter

I aktiviteten att fastslå relevanta IT-säkerhetsegenskaper ingår följande delaktiviteter:

- granskning av behov av IT-säkerhetsvärdering,
- specificering av relevanta IT-säkerhetsegenskaper,
- specificering av systemomfattning samt
- specificering av IT-säkerhetsegenskapernas relation till behoven av IT-säkerhetsvärdering

4.2.6 Verktyg

Steget från behov till relevanta IT-säkerhetsegenskaper underlättas av att använda befintliga begrepps- och egenskapsdefinitioner inom området, såsom:

- SIS (2003) begreppsbildningen,
- Försvarens krav på säkerhetsfunktioner (Försvarensmakten, 2004),
- Common criteria security functional requirements (CC, 2006) samt
- Uppsättningar med säkerhetsmetriker (Jaquith, 2007).

Dessa definitioner behöver inte följas strikt utan kan väljas och anpassas efter vad som passar bäst för den befintliga situationen. Huvudsaken är att återanvända befintliga och välgenomtänkta egenskaper som passar in i sammanhanget och därmed inte behöva definiera dessa själv. För att strukturera arbetet med att ta fram IT-säkerhetsegenskaper som motsvarar givna behov kan metodik från *kvalitetsdriven kravhantering* (Hallberg, 1999) nyttjas. Exempel på därifrån användbara verktyg är kundrösttabeller som kan användas för att strukturera arbetet med att gå från behov till egenskaper.

4.2.7 Genomförande

Genomförandet av aktiviteten (Figur 5) beskrivs utgående från dess delaktiviteter.

Granskning av behov av IT-säkerhetsvärdering

Vid granskning av de behov som ligger till grund för IT-säkerhetsvärderingen tas ställning till om behoven är tillräckliga för att fastslå en uppsättning av relevanta IT-säkerhetsegenskaper. I detta ingår också att granska behoven för att eliminera redundanta behov och därmed undvika att skapa redundans i uppsättningen av relevanta IT-säkerhetsegenskaper.

Specificering av relevanta IT-säkerhetsegenskaper

Vid specificeringen av relevanta IT-säkerhetsegenskaper måste utgångspunkten vara vilka egenskaper som motsvarar de identifierade behoven. Syftet är alltså att hitta IT-säkerhetsegenskaper vars värdering kommer att eliminera den brist på kunskap som intressenterna har. Detta ställer krav på att IT-säkerhetsegenskaperna kan kopplas till metriker. Egenskaperna behöver dock inte vara direkt mätbara, utan kan istället beräknas baserat på de underliggande egenskaper som bestäms i den följande aktiviteten.

En del behov kan relativt rättframt översättas till IT-säkerhetsegenskaper, medan andra behov kräver mer analys och vissa behov, slutligen, inte låter sig omvandlas till någon eller några av de egenskaper som står till buds. Lämpligen utgår arbetet från befintliga begrepps- och egenskapsdefinitioner (se avsnitt 4.2.6).

Valet av IT-säkerhetsegenskaper har stor betydelse för vilka egenskaper processen för IT-säkerhetsvärdering får. Skillnaden mellan säkerhetsegenskaper som baseras på observation eller testning av systemet, dvs. systemeffekter, respektive granskning, dvs. systemegenskaper, avseende exempelvis resursförbrukning och tid det tar att få fram resultat kan vara avgörande. Observation kan baseras på kostnadseffektiv insamling av loggar, men ta en lång tidsperiod i anspråk då det inte är meningsfullt att mäta över korta tidsperioder (Jaquith, 2007). Granskning kan kräva relativt stora arbetsinsatser för analys av det studerade systemet, men kan leverera resultat kontinuerligt och för system under alla dess livscykler.

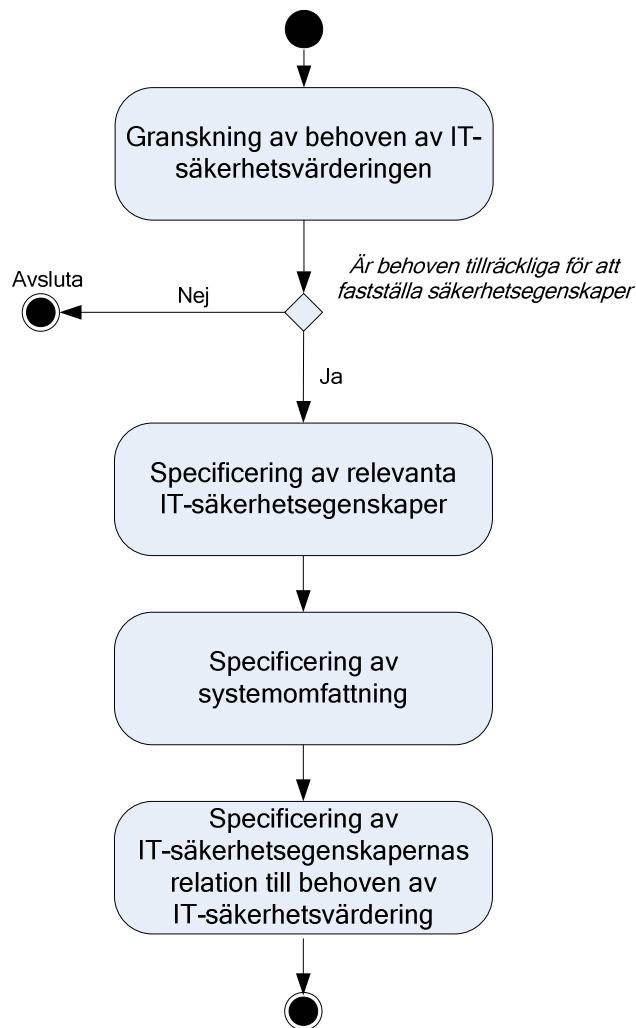
Specificering av systemomfattning

I delaktiviteten ingår att specificera egenskaper och begränsningar hos det studerade systemet. Här existerar en tydlig koppling till den föregående aktiviteten *Inventera behov av IT-säkerhetsvärdering* såväl som den föregående delaktiviteten *Specificering av relevanta IT-säkerhetsegenskaper*. Ur de identifierade behoven och egenskaperna ska följande faktorer som beskriver systemomfattningen härledas:

- gränsdragning mellan det modellerade systemet och dess omgivning,
- vilka systemaspekter som ska ingå i systemmodellen,
- vilka delar av systemets livscykel som ska modelleras, det vill säga systemet, eller delsystemen, är under utveckling, i drift eller under avveckling samt
- vilka typer av IT-säkerhetsegenskaper som ska modelleras, det vill säga systemegenskaper eller systemeffekter.

Specificering av IT-säkerhetsegenskapernas relation till behoven av IT-säkerhetsvärdering

För att säkerställa spårbarhet från IT-säkerhetsegenskaper till behov och vice versa ska relationerna mellan dessa dokumenteras.



Figur 5: IT-säkerhetsvärderingens andra aktivitet; fastslå relevanta IT-säkerhetsegenskaper.

4.2.8 Tillämpningsexempel

I organisation X har ledningen "behov av att veta hur bra skyddet mot otillbörlig spridning av Xs data är". Detta behov resulterar i flera relevanta säkerhetsegenskaper, såsom

- skydd mot otillbörlig spridning av organisationens data,
- skydd mot att ej öppen information sprids via extern uppkoppling och
- skydd mot obehörig tillgång till organisationens IT-system.

4.3 Överföra relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter

Syftet med denna aktivitet är att utgående från de, i föregående aktivitet, fastslagna relevanta IT-säkerhetsegenskaperna skapa en struktur, där värden för de icke direkt mätbara egenskaperna byggs upp med hjälp av underliggande systemegenskaper

och -effekter. Detta innebär att en beräkningsmodell för den aktuella värderingen skapas.

4.3.1 Motivering

Fört att kunna värdera de IT-säkerhetsegenskaper som bedömts som relevanta, men inte är direkt möjliga att mäta, måste systemegenskaper och -effekter som är mätbara associeras till dessa IT-säkerhetsegenskaper. Därmed erhålls en beräkningsmodell som beskriver hur mätbara systemegenskaper och -effekter sammanställs till värden för de relevanta IT-säkerhetsegenskaperna. En adekvat beräkningsmodell är av avgörande betydelse för vilken kvalitet som erhålls på värderingen.

4.3.2 Viktiga aspekter

Även om arbetet underlättas av existerande uppsättningar av säkerhetsegenskaper kan dessa vara mindre lämpade för värdering. Få uppsättningar har tillhörande metriker eller kommer i form av lämpliga strukturer. Därmed måste egna uppsättningar av systemegenskaper och -effekter tas fram utgående från de existerande uppsättningarna för att passa de fastslagna behoven av IT-säkerhetsvärdering. Detta arbete behöver dock inte genomföras fullt ut för varje värdering, ett stort mått av återanvändning kommer att vara möjligt. Återanvändningen kan även ske interorganisatoriskt vilket illustreras av det arbete som har genomförts inom området (Lippiat o.a, 2007; Swanson o.a., 2003).

En metrik består av de tre delarna storhet, skala och tolkning. Vid överföring av IT-säkerhetsegenskaper till systemegenskaper och -effekter är valet av metriker av stor vikt. Metrikerna måste beskriva relevanta storheter med skalor som går att tolka och har tillräcklig precision för att ge mervärde för intressenterna. De skalor metrikerna innehåller måste vara anpassade för de operationer som används i beräkningsmodellen. Detta är en kritisk faktor, ty olämpligt val av skalor kan medföra otillåtna beräkningar. Därmed kan man riskera att framtagna resultat, i formell matematisk betydelse, inte är meningsfulla. För att hantera dess frågor krävs kunskap om metriker och hur dessa utformas, vilket inkluderar området "measurement theory"¹. "Measurement theory" behandlar frågor såsom vilka operationer som kan användas på olika värden baserat på vilka skalor de anges enligt. (Bengtsson, 2007)

Det är inte säkert att alla IT-säkerhetsegenskaper kan beräknas genom att bygga en trädstruktur där varje IT-säkerhetsegenskap beräknas baserat på beräknade eller uppmätta värden hos underliggande IT-säkerhetsegenskaper. En komplikation är relationer mellan olika entiteter i system, vilka medför att strukturen hos system är avgörande för dess IT-säkerhetsnivå. Detta leder till behov av mer avancerade beräkningsmodeller.

¹ Det verkar inte existera någon svensk term för området. *Mätteori* indikerar en annan tradition.

Även om begreppet mätbara systemegenskaper och -effekter används kan det i vissa fall vara nödvändigt att nyttja subjektiva värderingar av IT-säkerhetsegenskaper.

4.3.3 Ingångsvärden

Nödvändiga ingångsvärden till aktiviteten utgörs av:

- de fastslagna IT-säkerhetsegenskaperna, från föregående aktivitet,
- specifikationen av systemomfattning hos det studerade systemet, från föregående aktivitet samt
- data om det studerade systemet.

4.3.4 Resultat

Aktiviteten resulterar i:

- en systemmodell, som beskriver det studerade systemet och dess ingående enheter samt visar hur de mätbara systemegenskaperna och -effekterna relaterar till dessa, och
- en beräkningsmodell, som beskriver relationerna mellan de mätbara systemegenskaperna och -effekterna respektive de relevanta IT-säkerhetsegenskaperna samt eventuella mellanliggande IT-säkerhetsegenskaper.

Systemmodellen utgör ett förtydligande av den systemomfattning som specificeras under föregående aktivitet. Beräkningsmodellen möjliggör beräkning av alla de egenskaper som inte är direkt mätbara.

4.3.5 Ingående delaktiviteter

I aktiviteten att överföra IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter ingår följande delaktiviteter:

- systemmodellering avseende systementiteter,
- identifiera systemegenskaper och -effekter hos det studerade systemet,
- systemmodellering avseende mätbara systemegenskaper och -effekter samt
- specificera beräkningsmodellen.

4.3.6 Verktyg

Genomförandet av aktiviteten kräver verktyg för system- och beräkningsmodellering.

För att undvika otydligheter i samband med specificering och användning av systemmodeller är det en fördel att använda formella modelleringstekniker, såsom

UML (Unified Modeling Language) (OMG, 2001). Det finns även verktyg för IT-säkerhetsvärdering som stödjer systemmodellering, till exempel NTE (Bengtsson & Brinck, 2007) och programmeringsspråket Prolog (Oman o.a., 2004).

Arbetet med att ta fram en struktur som relaterar de relevanta säkerhetsegenskaperna till mätbara systemegenskaper och -effekter underlättas, liksom för föregående aktivitet, av tillgång till befintliga sammanställningar av säkerhetsegenskaper. Försvarmaktens krav på säkerhetsfunktioner (Försvarmakten, 2004), Common criteria security functional requirements (CC, 2006) samt uppsättningar med säkerhetsmetriker (Jaquith, 2007) är exempel på befintliga sådana sammanställningar.

Att specificera en beräkningsmodell, baserat på strukturer som relaterar relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter, underlättas av tillgången till matematiska metoder såsom Analytic Hierarchy Process (AHP) (Forman & Selly). Värderingsmetoden XMASS (Hallberg o.a., 2006) har realiserats i verktyget NTE, där överförandet från IT-säkerhetsegenskaper till mätbara systemegenskaper baseras på Försvarmaktens krav på säkerhetsfunktioner och beräkningsmodellen tas fram med en metod baserad på AHP, vilken prioriterar de olika systemegenskaperna. Detta utgör en del av beräkningsmodellen i XMASS och NTE, vilken även tar hänsyn till hur systementiteter påverkar varandra.

4.3.7 Genomförande

Genomförandet av aktiviteten (Figur 6) beskrivs utgående från dess delaktiviteter.

Systemmodellering avseende systementiteter

För att kunna avgöra vilka användbara systemegenskaper och -effekter som finns i systemet, behövs en systemmodell som visar vilka entiteter som finns i systemet.

Identifiera systemegenskaper och -effekter hos det studerade systemet

Det finns två principiellt olika huvudsätt för genomförande av denna delaktivitet:

1. Bryt ner de fastslagna IT-säkerhetsegenskaperna till möjliga mätbara systemegenskaper och -effekter².
2. Utgå ifrån tillgängliga mätbara systemegenskaper och -effekter för det studerade systemet och gör en bedömning av vilka av dem som kan användas för att värdera var och en av de relevanta IT-säkerhetsegenskaperna³.

I en del fall kan en kombination av dessa två huvudsätt vara det mest lämpliga tillvägagångssättet. Till exempel kan det vara så att det studerade systemet bryts upp i delsystem och att de relevanta säkerhetsegenskaperna för hela det studerade systemet värderas för vart och ett av delsystemen för att sedan kombineras ihop.

² Motsvarar en så kallad "top-down"-vinkling av problemet.

³ Motsvarar en så kallad "bottom-up"-vinkling av problemet.

Säkerhetsegenskaperna för vart och ett av delsystemen beräknas utgående från en kombination av identifierade mätbara delsystemegenskaper.

Vilka av de mätbara systemegenskaperna och -effekterna som bäst lämpar sig för att värdera de fastslagna IT-säkerhetsegenskaperna beror på en värderingsberoende prioritering avseende till exempel relevans, mätkostnad och mättid för aktuell värdering. Det kan mycket väl vara så att en kombination av systemegenskaper och -effekter krävs för värdering av en IT-säkerhetsegenskap.

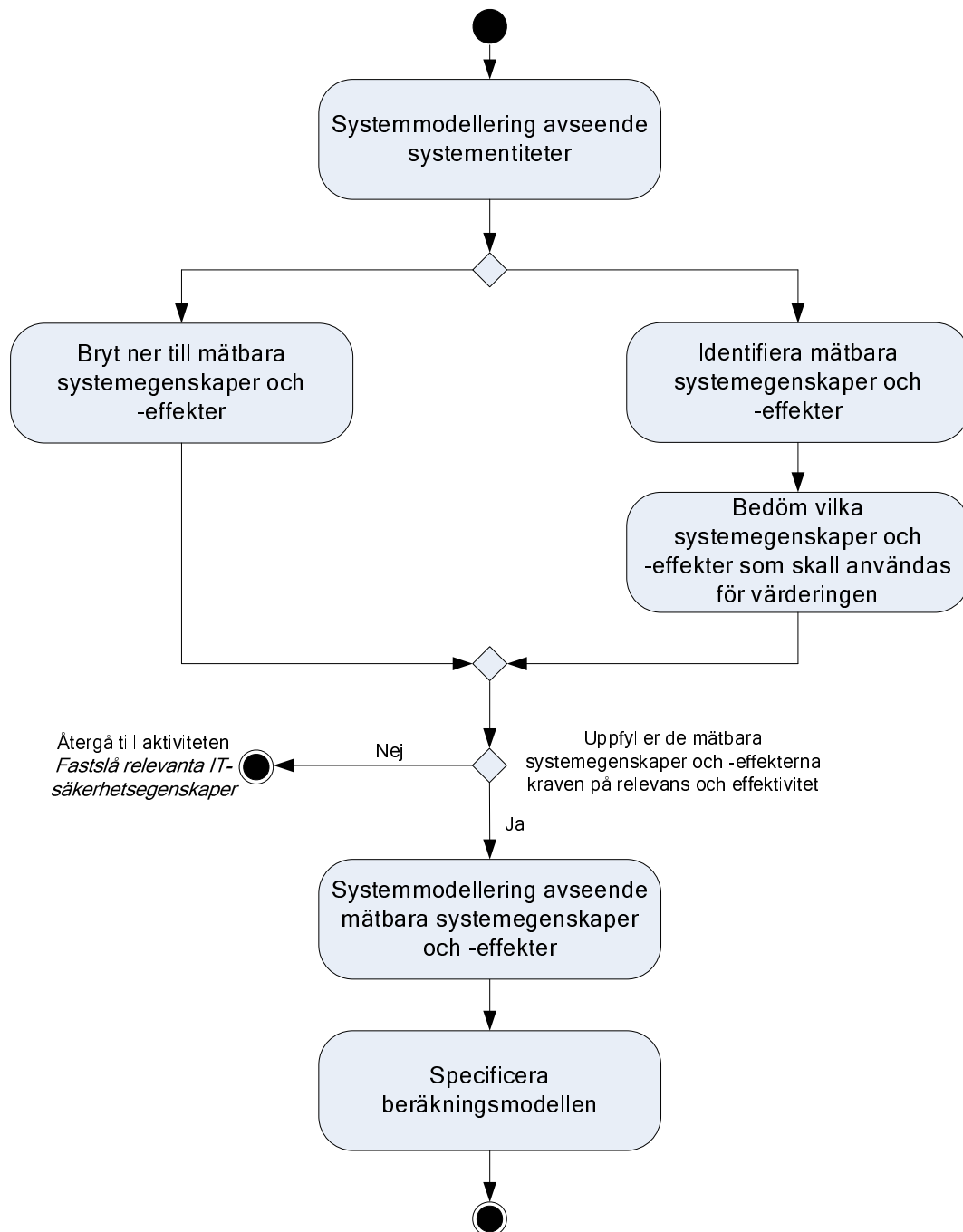
Om de mätbara systemegenskaper och -effekterna inte tillräckligt väl uppfyller kraven på relevans eller effektivitet, återgå till aktiviteten *Fastslå relevanta IT-säkerhetsegenskaper* för att fastställa en alternativ uppsättning med egenskaper.

Systemmodellering avseende mätbara systemegenskaper och -effekter

Oavsett vilket tillvägagångssätts som väljs i föregående delaktivitet så måste en modell av det studerade systemet tas fram. Denna modell ska beskriva dess ingående entiteter, avseende mätbara systemegenskaper och -effekter, och i vissa fall relationer mellan dessa entiteter. Detta utgör en förutsättning för genomförandet av mätningarna.

Specificera beräkningsmodellen

För de systemegenskaper och -effekter som ska mätas, tas metriker fram. Dessutom måste beräkningsmodellen beskriva relationerna mellan de mätbara systemegenskaperna och -effekterna respektive de relevanta säkerhetsegenskaperna. Om en säkerhetsegenskap, till exempel, anses bero på en uppsättning mätbara systemegenskaper kan detta uttryckas med ett viktat medelvärde av de olika systemegenskaperna.



Figur 6: IT-säkerhetsvärderingens tredje aktivitet; överföra relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter

4.3.8 Tillämpningsexempel

Inom organisation X anses säkerhetsegenskapen "skydd mot obehörig tillgång till organisationens IT-system" vara relevant. Denna relevanta säkerhetsegenskap kan brytas ner till flera mätbara systemegenskaper och -effekter, såsom

- frekvens av incidenter med spökprogram (eng. root kits) som ger möjlighet till eskalering av rättigheter i systemet och

- en uppsättning krav avseende IT-systemets funktioner för användarautentisering vilka har prioriterats för att efter avstämning kunna ge ett viktat medelvärde för systemet (detta utgör därmed en samling mätbara systemegenskaper och en modell för hur ett säkerhetsvärde för en mer övergripande säkerhetsegenskap ska beräknas).

De mätbara systemegenskaperna och -effekterna relateras till de motsvarande relevanta säkerhetsegenskaperna genom en beräkningsmodell. Beräkningsmodellen föreskriver, till exempel, att uppfyllandet av kraven avseende användarautentisering ska anges på en skala bestående av intervallet $[0, 1]$ samt att dessa ska sammanställas som viktade medelvärden.

4.4 Mäta valda systemegenskaper och -effekter

Denna aktivitet syftar till att associera värden till de mätbara systemegenskaperna och -effekterna som valdes ut under den föregående aktiviteten.

4.4.1 Motivering

För att kunna beräkna värden för de relevanta IT-säkerhetsegenskaperna är det avgörande att de mätbara systemegenskaperna och -effekterna tilldelas adekvata värden.

4.4.2 Viktiga aspekter

För att underlätta mätningar, måste använda metriker vara anpassade till det studerade systemet och den aktuella värderingen. Detta innebär att de värden som via mätning associeras till systemegenskaper och -effekter ska ha en tydlig relevans för slutresultaten från värderingsprocessen och, i förlängningen, dess intressenter.

Att basera mätningar på vad som för tillfället verkar vara möjligt att värdesätta, det vill säga så kallade ad hoc-mätningar, minskar tillförlitligheten och ska därför undvikas.

4.4.3 Ingångsvärden

Nödvändiga ingångsvärden till aktiviteten utgörs av:

- systemmodell och
- beräkningsmodell.

4.4.4 Resultat

Aktiviteten resulterar i:

- en uppsättning mätvärden associerade till de mätbara systemegenskaperna och -effekterna.

4.4.5 Ingående delaktiviteter

I aktiviteten att mäta valda systemegenskaper och -effekter ingår följande delaktiviteter:

- granska systemmodellen,
- associera värden med mätbara systemegenskaper och -effekter samt
- kvalitetsgranska associerade värden.

4.4.6 Verktyg

För att genomföra aktiviteten att mäta valda systemegenskaper och -effekter krävs:

- metriker anpassade till det studerade systemet och den aktuella värderingsprocessen,
- verktyg för loggning av IT-säkerhetsrelevanta händelser i systemet samt
- metoder och verktyg för att avgöra systems faktiska IT-säkerhetsrelevanta systemegenskaper.

4.4.7 Genomförande

Genomförandet av aktiviteten (Figur 7) beskrivs utgående från dess delaktiviteter.

Granska systemmodellen

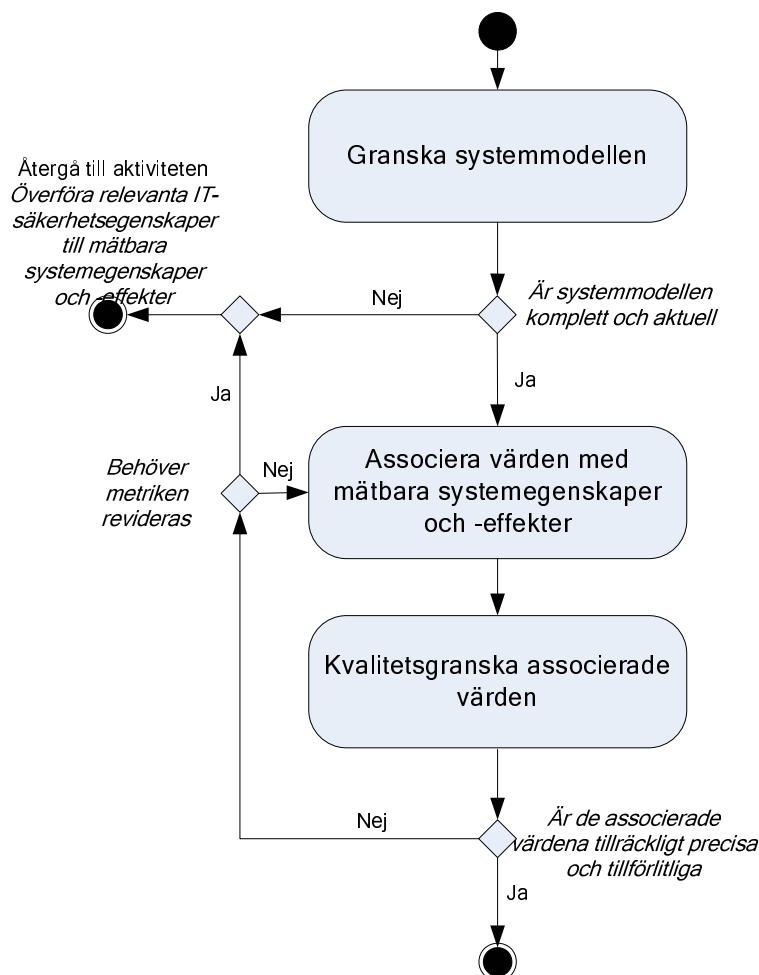
Denna delaktivitet syftar till att fastställa att systemmodellen är komplett och aktuell avseende de systemegenskaper och -effekter som ska mätas. Systemmodellen måste inte nödvändigtvis innehålla all data som behövs, men den ska i så fall tydligt indikera var och hur dessa data kan samlas in.

Associera värden med mätbara systemegenskaper och -effekter

Delaktivitetens genomförande beror på vilka egenskaper och -effekter som adresseras. En indelning i huvudangreppssätt ges av de fem huvudansatserna till värdering (observation av systemeffekter, testning av systemeffekter, granskning av systemegenskaper, granskning av egenskaper hos systementiteter samt granskning av systemstruktur) samt av vilka systemaspekter som adresseras (organisatoriska, humana, tekniska, operativa och kontextuella) (Hallberg o.a., 2006). Bygger exempelvis värderingen på en strukturanalys av systemets inre, ger detta ett markant annorlunda mätförfarande än vad en värdering baserad på analys av endast in- och ut-signaler från systemet ger. Huvudprincipen är dock att värden tas från systemmodellen eller samlas in baserat på systemmodellen och associeras med de mätbara systemegenskaperna och -effekterna i beräkningsmodellen.

Kvalitetsgranska associerade värden.

Med fastställda metriker underlättas kvalitetsgranskningen. De uppmätta värdenas tillförlitlighet ska vid granskningen sättas i relation till dessa metriker. Situationer kan då uppstå där den valda metriken inte på ett adekvat sätt beskriver verkligheten, eller att det inte är möjligt att mäta aktuell systemegenskap eller -effekt med tillräcklig noggrannhet. En bedömning bör då göras av huruvida metriken alternativt aktuell systemegenskap eller -effekt ska revideras. Om inte tillräcklig tillförlitlighet kan uppnås hos mätvärden, återgå till föregående delaktivitet och revidera mätförfarandet. Om metriken behöver revideras krävs en återgång till aktiviteten *Överföra relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter* för att efter behov revidera metriken och systemegenskapen eller -effekten.



Figur 7: IT-säkerhetsvärderingens fjärde aktivitet; mäta valda systemegenskaper och -effekter.

4.4.8 Tillämpningsexempel

Inom organisation X används en uppsättning krav avseende IT-systemets funktioner för användarautentisering som mätbara systemegenskaper. Mätningen utgörs av att kraven associeras med värden för det studerade systemet. Värdet 0 motsvarar att

kravet inte alls är uppfyllt, medan värdet 1 motsvarar att kravet är helt uppfyllt. Värden mellan 0 och 1 används för krav som är delvis uppfyllda.

4.5 Beräkna IT-säkerhetsvärden

Under denna aktivitet beskrivs hur uppmätta säkerhetsvärden kombineras till sammansatta säkerhetsvärden för att, slutligen, resultera i värden för de relevanta IT-säkerhetsegenskaperna.

4.5.1 Motivering

Behov av säkerhetsvärdering eftersträvar i allmänhet att yttra sig om säkerhet hos hela system. Detta innebär att värderingar av delsystem eller entiteter i system behöver sammanställas. Om ett större antal generella systemegenskaper har värdesatts, innebär detta oftast också att sammanställning till ett mindre antal egenskaper behöver göras för att uppnå en mera systemövergripande värdering. I båda dessa fall behövs en sammanställning till den typ och nivå av värdering som intressenterna eftersträvar, vilket ska motsvaras av de relevanta IT-säkerhetsegenskaperna.

4.5.2 Viktiga aspekter

Sammanställning av värden innebär komprimering av information, eventuellt förlust av relevant information. När sammanställning kan göras utan att information av betydelse förloras, medför detta förenklingar som framhäver säkerhetsvärderingens centrala resultat. Förlust av information av central vikt för värderingen måste dock undvikas.

4.5.3 Ingångsvärden

Nödvändiga ingångsvärden till aktiviteten utgörs av:

- mätvärden associerade med mätbara systemegenskaper och -effekter samt
- beräkningsmodell.

4.5.4 Resultat

Aktiviteten resulterar i:

- sammansatta säkerhetsvärden för de relevanta IT-säkerhetsegenskaper som inte är direkt mätbara.

4.5.5 Ingående delaktiviteter

I aktiviteten beräkna säkerhetsvärden ingår endast en delaktivitet:

- implementera beräkningsmodellen samt
- sammanställ säkerhetsvärden för relevanta IT-säkerhetsegenskaper

4.5.6 Verktyg

Givet en formellt formulerad beräkningsmodell kan denna aktivitet helt automatiseras, såsom i verktyget NTE (Bengtsson & Brinck, 2007). Om det inte finns något specialdesignat verktyg, kan generell programvara för beräkningar, exempelvis av kalkylark, användas.

4.5.7 Genomförande

Genomförandet av aktiviteten (Figur 8) beskrivs utgående från dess delaktiviteter.

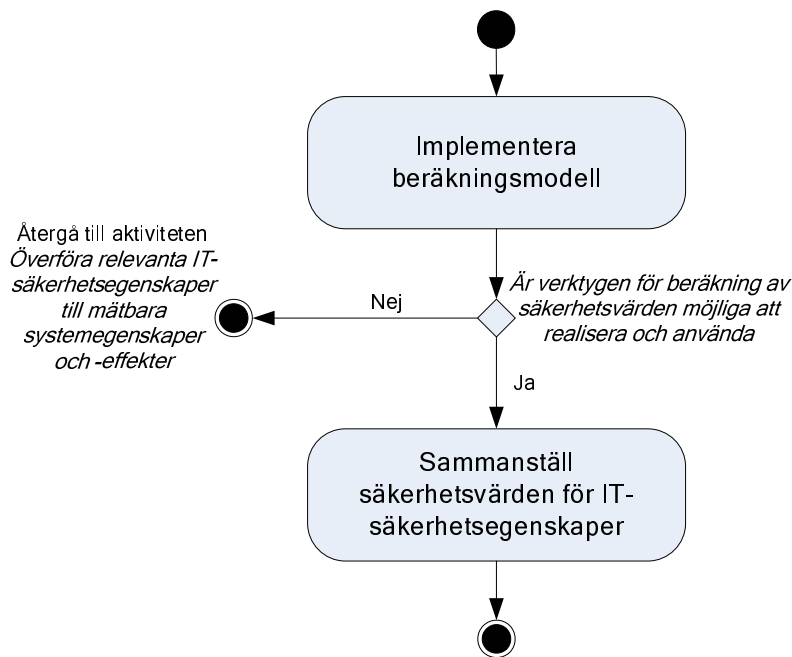
Implementera beräkningsmodellen

Ta fram verktyg vilka implementerar den beräkningsmodell som togs fram under aktiviteten *Överföra relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter*. Om verktygen är alltför kostsamma att realisera eller använda kräver detta en omarbetning av beräkningsmodellen.

Sammanställ säkerhetsvärden för relevanta IT-säkerhetsegenskaper

Beräkna, med hjälp av framtagna verktyg, utgående från uppmätta säkerhetsvärden, vilka i någon mån kan beskrivas som löv i beräkningsmodellen, säkerhetsvärden för de relevanta säkerhetsegenskaperna baserat på beräkningsmodellen. Beroende på modellen kan dessa beräkningar vara:

- så pass rättframma att de kan utföras manuellt,
- relativt invecklade och kräva speciellt stöd (programvara) eller
- baserade på simuleringar och kräva stöd för dessa.



Figur 8: IT-säkerhetsvärderingens femte aktivitet; beräkna IT-säkerhetsvärden.

4.5.8 Tillämpningsexempel

Inom organisation X anses säkerhetsegenskapen ”skydd mot obehörig tillgång till organisationens IT-system” vara relevant. Denna relevanta säkerhetsegenskap har brutits ner till flera mätbara systemegenskaper och -effekter, vilka har mätts. Vid mätningen har en del av de mätbara systemegenskaperna och -effekterna, som består av en uppsättning krav avseende IT-systemets funktioner för användarautentisering, tilldelats värden i intervallet $[0, 1]$. Därigenom kan ett säkerhetsvärde för användarautentiseringen beräknas, hur specificeras av den framtagna beräkningsmodellen (se avsnitt 4.3.8). Utifrån detta och andra beräknade eller uppmätt säkerhetsvärden beräknas säkerhetsvärden för de relevanta säkerhetsegenskaperna enligt beräkningsmodellen.

4.6 Tolka IT-säkerhetsvärden

Denna aktivitet syftar till att tolka vad framtagna säkerhetsvärden för de relevanta IT-säkerhetsegenskaperna innebär inom ramen för det studerade systemet och därigenom värdera dessa egenskaper.

4.6.1 Motivering

För att uppmätta och beräknade säkerhetsvärden ska innebära något för den verksamhet i vilket det studerade systemet befinner sig, måste en tolkning ske, vilket ger värderingsprocessens slutresultat i form av värderade relevanta säkerhetsegenskaper.

4.6.2 Viktiga aspekter

Tolkning av säkerhetsvärden får varken bli för avgränsad eller alltomfattande. Även om man skulle lyckas beskriva relationen mellan intressenter, behov av säkerhetsvärdering och de relevanta säkerhetsegenskaperna, så krävs fortfarande en balansgång för att tolkningen ska resultera i en ändamålsenlig värdering.

Tolkningen avser de relevanta säkerhetsegenskaperna i den kontext det studerade systemet utgör. Beroende på aktuell säkerhetsmetrik innebär det att tolkningen av ett och samma säkerhetsvärde kan skilja stort mellan olika studerade system. Riskvärdering ligger dock utanför denna aktivitet (och säkerhetsvärdering som helhet), varför tolkningen av säkerhetsvärden är oberoende av den kontext som det studerade systemet befinner sig i.

Rutiner för säkerhetsvärdering är fortfarande en bristvara, men än mera är rutiner för tolkning av säkerhetsvärden en bristvara. Sannolikt krävs det erfarenhet som byggs upp via användning av värderingsprocesser för att skapa en bas av vedertagna rutiner för tolkning av säkerhetsvärden.

4.6.3 Ingångsvärden

Nödvändiga ingångsvärden till aktiviteten utgörs av:

- uppmätta och beräknade säkerhetsvärden för de relevanta säkerhetsegenskaperna.

4.6.4 Resultat

Aktiviteten resulterar i:

- värdering av relevanta IT-säkerhetsegenskaper.

4.6.5 Ingående delaktiviteter

I aktiviteten tolka säkerhetsvärden ingår följande delaktiviteter:

- välj rutin för tolkning av säkerhetsvärden samt
- fastslå tolkning av säkerhetsvärden.

4.6.6 Verktyg

Som stöd för tolkningen kan följande verktyg användas:

- metriker anpassade till det studerade systemet och behoven av säkerhetsvärdering samt
- rutiner för tolkning av säkerhetsvärden.

4.6.7 Genomförande

Genomförandet av aktiviteten (Figur 9) beskrivs utgående från dess delaktiviteter.

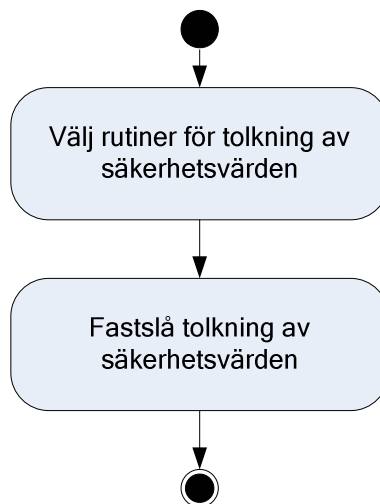
Välj rutin för tolkning av säkerhetsvärden

Med utgångspunkt i värden för de relevanta IT-säkerhetsegenskaperna och till dessa associerade metriker, väljs för sammanhanget relevanta rutiner för tolkning av dessa säkerhetsvärden. Beroende på metrikerna och deras koppling till intressenternas behov framträder följande huvudkategorier av tolkningssituationer. Om aktiviteterna "Fastslå relevanta IT-säkerhetsegenskaper" och "Överföra relevanta IT-säkerhetsegenskaper till mätbara systemegenskaper och -effekter" genomförs helt enligt handboken, är endast den första av huvudkategorierna nedan aktuell. I många fall kan dock svårigheten med att formulera metriker leda till att någon av de senare två huvudkategorierna blir aktuell.

- Metrikerna motsvarar direkt intressenternas behov och säkerhetsvärdena för de relevanta säkerhetsegenskaperna kan direkt kommuniceras till intressenterna.
- Metrikerna är väl formulerade och värdena rättframma att förstå, men värderingen av de relevanta säkerhetsegenskaperna i den kontext som systemet utgör är inte klar. Det vill säga säkerhetsvärdena är inte globala för systemet, inte anpassade efter systemets komplexitet eller andra egenskaper etc. Exempelvis kan detta vara fallet för säkerhetsvärden som anger antalet virusinfektioner, intrång, informationsläckor etc. i ett system under en viss tidsperiod. Värdena är tydliga, men deras tolkning och värderingen av systemets säkerhetsegenskaper viruskydd, intrångsskydd, sekretesskydd etc. är inte klar. Här kräver tolkningen stöd av över tid uppbyggda erfarenheter och rutiner.
- Metrikerna är ofullständiga och uttydandet av vad de representerar är oklart. Till exempel är detta fallet med metriker där storheten är en generell säkerhetsegenskap, såsom intrångsskydd, skalan går från 0 till 1 och det inte finns några rutiner för hur värdena ska uttydas. Här kräver uttydandet av säkerhetsvärdena stöd av över tid uppbyggda erfarenheter och rutiner. När väl säkerhetsvärdena är tydda, faller tolkningen in under en av de två ovanstående punkterna.

Fastslå tolkning av säkerhetsvärden

Med hjälp av valda rutiner för tolkning av säkerhetsvärdena värderas de relevanta IT-säkerhetsegenskaperna. Baserat på denna värdering fastslås resultatet av processen för IT-säkerhetsvärdering.



Figur 9: IT-säkerhetsvärderingens sjätte aktivitet; tolka IT-säkerhetsvärden

4.6.8 Tillämpningsexempel

Inom organisation *X* anses säkerhetsegenskapen "skydd mot obehörig tillgång till organisationens IT-system" vara relevant. Ett säkerhetsvärde i intervallet $[0, 1]$ har beräknats för systemet.

Om det finns en metrik som ger en tydlig tolkning associerad med det framtagna värdet, utgör detta värde (tillsammans med motsvarande värden för de övriga relevanta säkerhetsegenskaperna) resultatet av värderingen. Om metrikerna är ofullständiga och uttydandet av vad de representerar är oklart, måste detta hanteras för att möjliggöra en tolkning av säkerhetsvärdet. Detta kan hanteras genom att jämföra med värden som erhållits för andra system, såsom det ideala systemet, ett riktigt dåligt system eller tidigare versioner av det studerade systemet. De levererade säkerhetsvärdena ska också vara oberoende av andra systemegenskaper än de som påverkar systemnivån, till exempel systemets storlek, det vill säga de ska tolkas i den kontext som systemet utgör.

De levererade säkerhetsvärdena kan sedan ligga till grund för beslut som påverkar systemets IT-säkerhetsnivå, till exempel huruvida behörighetskontrollen ska skärpas eller ej.

5 Referenser

- ACSA (2002), *Proc. Workshop on Information Security System Scoring and Ranking*. Applied Computer Security Associates, <http://www.acsac.org/measurement/proceedings/wissr1-proceedings.pdf>
- Andersson, R., Hunstad, A., & Hallberg, J. (2003). *Evaluation of the security of components in distributed information systems*. Linköping, Scientific report. FOI-R--1042--SE. Swedish Defence Research Agency.
- Andersson R. & Hallberg J. (2006). System security assessment – a concept demonstrator. FOI Memo 1798. Linköping, Sweden.
- Bengtsson, M. (2007). *Mathematical Foundation Needed for Development of IT Security Metrics*. Examensarbete under framtagande.
- Bengtsson, J. & Brinck, P. (2007). *Using NTE with XMASS*. Arbetsdokument. FOI, Linköping.
- Common Criteria (2006). *Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, Version 3.1, Revision 1*. September 2006. CCMB-2006-09-002.
- Flanagan, J. C. (1954). The Critical Incident Technique. *Psychological Bulletin*, 51, 327-58.
- Forman, E. & Selly, M. (år okänt). *Decision by Objectives*.
- Försvarsmakten (2004). *Krav på säkerhetsfunktioner – Grunder*. 10 750: 78976. 2004-12-20.
- Geer, D. (2006). *Measuring Security*. Lecture Notes, Training program M3. 15th USENIX Security Symposium, Vancouver, Canada. July 31-August 4, 2006.
- Hallberg, N. (1999). *Incorporating User Values in the Design of Information Systems and Services in the Public Sector: A Methods Approach*. [Dissertation No. 596] Linköping Studies in Science and Technology.
- Hallberg, J., Hunstad, A., Bond, A., Peterson, M., Pålsson, N., (2004), *System IT Security Assessment*, FOI-R—1468—SE, Defence Research Establishment, Linköping, Sweden.
- Hallberg, N., Andersson, R., & Westerdahl, L. (2005) *Quality-driven process for requirements elicitation: the case of architecture driving requirements*. Linköping, FOI 2005, (FOI-R--1576--SE).
- Hallberg, J., Hallberg, N., Hunstad, A. (2005). *Behovsanalys avseende värdering av IT-säkerhet*. Vetenskaplig rapport, FOI-R--1820--SE. FOI, Linköping, Sweden.
- Hallberg, J., Hallberg, N., Hunstad, A., (2006), *Crossroads and XMASS: Framework and Method for System IT Security Assessment*, FOI-R—2154—SE, Defence Research Establishment, Linköping, Sweden.
- Jaquith, A. (2007). *Security Metrics—Replacing, Fear, Uncertainty, and Doubt*. Addison-Wesley.
- Kano, N. (1995). Upsizing the Organization by Attractive Quality Creation. In G.K. Kanji (Ed.), *Proceedings of the First World Congress on Total Quality Management* (pp. 60-72). London: Chapman & Hall.

- Kensing, F. & Halskov Madsen, K. (1991). Generating Visions: Future Workshop and Metaphorical Design. In J. Greenbaum & M. Kyng (Eds.). *Design at Work: Cooperative Design of Computer Systems* (pp. 155-168). Hillsdale, New Jersey: Lawrence Earlbaum.
- Kulak, D. & Guiney, E. (2000). *Use Cases: Requirements in Context*. New York: Addison-Wesley Pub Co.
- Lippiatt, B. & Fuller, S. (2007). *An Analytical Approach to Cost-Effective, Risk-Based Budgeting for Federal Information System Security*. National Institute of Standards and Technology. NISTIR 7385.
- Nationalencycledin. Artikel om informationssystem. www.ne.se. Besökt 2007-06-15.
- McClelland, S. B. (1994a) Training Needs Assessments Data-gathering Methods: Part 2, Individual Interviews. *Journal of European Industrial Training*. 18, 2, pp 27-31.
- McClelland, S. B. (1994b) Training Needs Assessments Data-gathering Methods: Part 3, Focus Groups. *Journal of European Industrial Training*. 18, 3, pp 29-32.
- Oman, P., Krings, A., Conte de Leon, D., & Alves-Foss, J. (2004). Analyzing the Security and Survivability of Real-time Control Systems. *Proceedings of the 5th IEEE Workshop on Information Assurance*. West Point, NY, June 2004.
- Object Management Group, OMG. (2001). *Unified Modeling Language Specification, Version 1.4*.
- Seddigh, N., Piedad, P., Matrawy, A., Nandy, B., Lambadaris, J., & Hatfield, A. (2004). Current Trends and Advances in Information Assurance Metrics. Second Annual Conference on Privacy, Security and Trust, October 13-15, 2004.
<http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf>
- SIS. (2003). *Terminologi för informationssäkerhet*. SIS HB 550, utgåva 2. 2003-08-29.
- Swanson, M., Bartol, N., Sabato, J., & Hash, J. (2003). *Security metrics guide for information technology systems*. Technical Report NIST Special Publication 800-55, National Institute of Standards and Technology, July 2003.
<http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf>.
- Vaughn, R., Henning, R., & Siraj, A. (2003). Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy. *Proceedings of the Hawaii International Conference on System Sciences (HICSS-36)*, Waikoloa, Hawaii, January 6-9, 2003.
- Ölvingson, C., Hallberg, N., Timpka, T., and Greenes R. A (2002) Using the critical incident technique to define a minimal data set for requirements elicitation in public health, *International Journal of Medical Informatics*, vol 68, no1-3, pp 165 – 174.