Informationsbehov vid säkerhetsanalyser

En systematisk genomgång av etablerade metoder för IT-system

Teodor Sommestad, Johan Bengtsson,
Jonas Hallberg

FOI-R--3723--SE

September 2013

FOI

Teodor Sommestad, Johan Bengtsson,
Jonas Hallberg

Informationsbehov vid säkerhetsanalyser

En systematisk genomgång av etablerade metoder för IT-system

Bild/Cover: Totalförsvarets forskningsinstitut

Titel	Informationsbehov vid säkerhetsanalyser: En systematisk genomgång av etablerade metoder för IT-system
Title	Information needs in security analyses: A systematic review of established methods for IT systems
Rapportnr/Report no	FOI-R--3723--SE
Månad/Month	September
Utgivningsår/Year	2013
Antal sidor/Pages	39 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E36048
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Denna rapport försöker ge svar på vilken information som, enligt etablerade säkerhetsanalysmetoder, ska ligga till grund för säkerhetsanalyser av IT-system. En studie har genomförts för att identifiera vad etablerade metoder inom området anser ska användas som grund vid genomförandet av säkerhetsanalyser. De initiala sökningarna efter relevanta metoder resulterade i 74 metoder. Av dessa 74 metoder uppfyllde 12 metoder urvalskriterierna samt angav vilken information som bör ligga till grund för genomförandet av säkerhetsanalyser.

Endast en sjundedel av den information som krävs är säkerhetsspecifik information. Metodernas tyngdpunkt ligger således på mer generell information. Med generell information avses exempelvis information om olika typer av strukturer, såsom verksamhetsstruktur och strukturer för tekniska system. Oftast efterfrågas information som relaterar till verksamheten. Överlag prioriteras inte information om vilken information som finns i eller hanteras av ett system. Inte heller prioriteras information om beteende eller information om tekniska lösningar.

Ett annat resultat är att det skiljer sig mycket mellan vilken typ av information metoderna anser att säkerhetsanalysen ska baseras på. Några metoder är helt fokuserade på verksamhet medan de flesta tycker att det även behövs teknisk information, framförallt med avseende på teknikstruktur.

Generellt visar resultaten att det finns en stor mängd olika typer av information av vitt skild karaktär som kan ligga till grund för en säkerhetsanalys.

Nyckelord: Säkerhetsanalys, IT-system, risk

Summary

This report aims at answering which information, according to established methods, should be the basis for security risk analyses of IT systems. A study was performed to identify what established methods use as the basis for the analysis. The initial search for relevant methods resulted in 74 methods. 12 of the 74 methods met the specified selection criteria and stated the information needed to perform the analysis.

Only one seventh of the required information is security-specific information. Thus the emphasis of the methods is on more general information. General information could for example refer to information about different types of structures, such as business structures and structures for technical systems. The most frequently requested information is business related. The overall priority is not on information about the information contained in or processed by a system. Information about behavior or information about technical solutions is not emphasized.

Another result is that the type of information used by the different methods varies. Some methods are completely focused on business whereas most also include technical information, particularly with regard to the structure of technical solutions.

Overall, the results show that there is a large variety of different types of information of widely different character that can be used as the basis of information security risk analysis.

Keywords: Information security risk analysis, IT system, risk

Förord

Insamling och analys av underlag för den typ av studier som genomförts som grund för denna rapport kräver en stor arbetsinsats av flera personer. Vi vill tacka Matus Korman på avdelningen Industriella informations- och styrsystem, ICS, vid Kungliga tekniska högskolan, KTH, för det arbete han har genomfört vid den insamling och analys som ledde fram till de resultat som presenteras i denna rapport.

Innehåll

1 Inledning

I denna rapport används *säkerhetsanalys* (Försvarsmakten, 2013a) som det samlande begreppet för de aktiviteter som genomförs för att identifiera skyddsvärda tillgångar och hot samt bedöma risker som är kopplade till IT-system. Att samla in, strukturera och bedöma all den information som är relevant för att genomföra en säkerhetsanalys är en omfattande uppgift. Det kan till och med vara svårt att avgöra vilken information som är lämplig att samla in.

Syftet med denna rapport är att beskriva vilken typ av information som enligt etablerade säkerhetsanalysmetoder behövs för att genomföra en säkerhetsanalys. I denna inledning ges en kort beskrivning av metoder för att analysera informationssäkerhetsrisker följt av en sammanfattning av hur säkerhetsanalyser genomförs inom Försvarsmakten. Därefter detaljeras rapportens syfte och slutligen ges en översikt av rapportens resterande delar.

1.1 Allmänt om säkerhetsanalyser

Det finns många förslag på metoder för hur informationssäkerhetsrisker ska analyseras och bedömmas. Många av dessa förslag har dokumenterats i form av guider, manualer eller böcker. På en övergripande nivå går analysarbetet ut på att samla in information om relevant verksamhet och miljö för att kunna bedöma sårbarheter, skydd, hot, konsekvenser och risker. Baserat på detta skall beslut sedan fattas om eventuella åtgärder.

I sin doktorsavhandling skriver Johansson (2005) att en informationssäkerhets-bedömning bör a) utgå från en teori som är accepterad för att vara trovärdig och b) ta hänsyn till datainsamlingskostnaden för att vara effektiv. Alltså kan det antas att det som primärt styr vad en guide, manual eller bok säger ska samlas in är den teori som skaparna till metoden förlitar sig på, hur mycket arbete författarna tror att det krävs för att samla in olika typer av information och hur mycket arbete de anser ska läggas ner på en säkerhetsanalys.

Vilken typ av information som behövs beror alltså på vilken teori som ligger till grund för att avgöra vad som är säkert och osäkert. Vissa faktorer kan anses vara av största vikt för en säkerhetsanalys (exempelvis gränssnitt mellan datornätverk) medan andra kan anses vara helt oviktiga (exempelvis Tokyobörsens nuvarande index). Till skillnad från många andra områden finns det inom informations-säkerhetsområdet få dokumenterade teorier som är avsedda att bedöma risker. Därmed finns inte heller någon konsensus om vilka teorier som utgör bäst grund för bedömning av informationssäkerhetsrisker. Ofta specificeras inte vilka teorier en säkerhetsanalysmetod baseras på.

Utöver de underliggande teorierna så måste kostnaden för informationsinsamling tas i beaktande vid analyser, vilket leder till att prioriteringar i de flesta fall är

nödvändiga. Viss information har generellt sett en låg insamlingskostnad (exempelvis anställdas ålder) medan annan är dyr att samla in (exempelvis en karta över alla nätverkskablar i organisationen). Viss information kan också vara osäker (exempelvis antagonisters planer) medan annan är väl känd (exempelvis förra årets bokslut).

Det har tidigare gjorts enklare jämförelser mellan olika metoder för att bedöma informationssäkerhetsrisker. Exempelvis jämförde Syalim, Hori, och Sakurai (2009) fyra metoder med avseende på processteg och dokument som inkluderas. Filippini och Schimmer (2012) tog fram övergripande beskrivningar av 21 metoder anpassade för risker med industriella styrsystem. Dessvärre finns ingen översikt i den tillgängliga litteraturen av vilken information som de olika metoderna kräver, trots att detta är centralt för en riskanalysmetod. Det finns inte heller någon analys av hur samstämmiga de etablerade metoderna är med avseende på det informationsunderlag de kräver.

1.2 Säkerhetsanalys av IT-system inom Försvarsmakten

Att identifiera och hantera informationssäkerhetsrisker är viktigt för alla IT-system i Försvarsmakten, från administrativa stödsystem (som diariesystem) till insatsledningssystem (som SLB). Enligt Försvarsmaktens interna bestämmelser (FIB 2006:2) ska det genomföras hot-, risk- och sårbarhetsanalyser för alla IT-system som planeras användas i Försvarsmaktens verksamhet. Inom Försvarsmakten har det genom åren tagits fram ett flertal skrifter som beskriver arbetsprocesser för de olika analyserna samt vilka typer av analysresultat som förväntas.

Effektivare hot-, risk- och sårbarhetsanalyser är ett projekt som löper under åren 2011-2013 och finansieras inom ramen för Försvarsmaktens Forskning och Teknikutveckling (FoT). Fokus för projektet är att effektivisera de hot-, risk- och sårbarhetsanalyser som genomförs inom ramen för arbetet med att ta fram säkerhetsmålsättningar för IT-system.

I *Direktiv för Försvarsmaktens informationsteknikverksamhet* (DIT 04) (Försvarsmakten, 2004) presenteras Försvarsmaktens IT-livscykelmodell som beskriver hur det är tänkt att Försvarsmakten ska arbeta med IT-system. Hela vägen från att ett behov uppstår till att ett infört IT-system slutligen avvecklas beskrivs. I denna livscykelmodell beskrivs auktorisationsprocessen som främst berör de första stegen av IT-livscykelmodellen. Dessa initiala steg handlar om att gå från ett identifierat behov till ett anskaffat system. En del av detta arbete är att analysera vilka risker Försvarsmakten tar genom att införa ett planerat IT-system. Detta görs i form av hot-, risk- och sårbarhetsanalyser. Resultaten från dessa analyser är en viktig del av den säkerhetsmålsättning som tas fram för varje IT-system.

För att stödja arbetet med hot-, risk- och sårbarhetsanalyser har Försvarsmakten tagit fram *Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik* (H SÄK IT) (Försvarsmakten, 2006) som beskriver bakgrunden till varför olika analyser behöver genomföras samt de beroenden som finns mellan de olika typerna av analyser. Försvarsmakten har under de senaste åren arbetat med att ta fram nya handböcker som ger bättre beskrivningar av

- *varför* analyserna ska genomföras
- *vad* som förväntas av analysarbetet
- *hur* de förväntade resultaten ska uppnås.

Tre nya handböcker som berör IT-system har fastslagits under 2013 och förändrar därmed hur Försvarsmakten kommer att arbeta med analyser av IT-system framöver.

Det första nytillskottet är *Processhandbok IT-processen* (Försvarsmakten, 2013b) som har fastställts för att tills vidare användas för pilotarbete och utvärdering av den IT-process som handboken beskriver. DIT 04 och dess IT-livscykelmodell gäller fortfarande, men planen är att på sikt införa en kompletterad version av *Processhandbok IT-processen* som ska ersätta DIT 04.

Det andra nytillskottet är *Handbok Säkerhetstjänst Informationssäkerhet* (H SÄK Infosäk) (Försvarsmakten, 2013c) som fastslagits för tillämpning från och med andra september 2013. Fastslagandet av H SÄK Infosäk innebär att H SÄK IT upphävs. H SÄK Infosäk utgör i huvudsak tolkningar och förklaringar av de författningar som reglerar Försvarsmaktens arbete med informationssäkerhet.

Det tredje nytillskottet är en ny version av *Handbok Säkerhetstjänst Grunder* (H SÄK Grunder) (Försvarsmakten, 2013a) som bland annat beskriver tillvägagångssättet för att genomföra säkerhetsanalyser. Analyserna genomförs i följande fem steg.

1) Identifiera och prioritera skyddsvärda tillgångar.
2) Bedöm säkerhetshot på en femgradig skala.
3) Bedöm sårbarhet på en femgradig skala för varje kombination av skyddsvärd tillgång och hot.
4) Bedöm risk med stöd av en riskmatris kopplad till sannolikhet och konsekvens.
5) Prioritera och hantera risker.

1.3 Syfte och avgränsningar

Denna rapport försöker ge svar på vilken information som, enligt etablerade säkerhetsanalysmetoder, ska ligga till grund för säkerhetsanalyser av IT-system. Den litteraturgenomgång som presenteras har sökt svar på följande frågor:

1) Hur hanteras situationer med flera systemägare enligt etablerade säkerhetsanalysmetoder?
2) Vilken generell IT-relaterad information är till hjälp i riskbedömningar enligt etablerade säkerhetsanalysmetoder?
3) Vilken säkerhetsspecifik information är viktig enligt etablerade säkerhetsanalysmetoder?
4) Vilka roller och organisationer behöver konsulteras för att göra en riskbedömning enligt etablerade säkerhetsanalysmetoder?
5) Hur väl överensstämmer olika etablerade säkerhetsanalysmetoders förslag?

Flera betydande avgränsningar har gjorts i denna studie. Litteraturgenomgången är begränsad till dokument skrivna på svenska eller engelska som författarna har tillgång till. Detta innebär att litteratur som inte gjorts offentlig (dvs. inte finns refererad på Internet), enbart finns tillgänglig på andra språk eller måste köpas in inte har tagits med. Genomgången är också begränsad till vad författarna anser vara etablerade säkerhetsanalysmetoder. Av detta följer att metoder utgivna av andra än myndigheter och standardiseringsorgan endast i undantagsfall har inkluderats. Till exempel exkluderas en icke-etablerad metod som CySeMoL (Sommestad, Ekstedt, & Holm, 2013) trots att den tydligt specificerar vad som skall samlas in och är transparent med orsaken till detta (dvs. specificerar den bakomliggande teorin).

1.4 Rapportstruktur

I kapitel 1, rapportens inledning, ges inledningsvis en allmän beskrivning av säkerhetsanalyser samt vilka utmaningar som finns inom området. Därefter följer en övergripande beskrivning av säkerhetsanalyser inom Försvarsmakten och slutligen beskrivs syfte och avgränsningar relaterade till den genomförda studien som beskrivs i denna rapport.

Kapitel 2 beskriver den genomförda litteraturgenomgången. Beskrivningen är uppdelad på fyra avsnitt som beskriver de olika aktiviteterna som genomförs under en systematisk litteraturgenomgång.

Resultaten från den genomförda studien återges i kapitel 3. Resultat återges för var och en av de frågor som ställts upp. De olika metoderna jämförs för att exempelvis visa på deras samstämmighet.

Rapporten avslutas med kapitel 4 där studiens resultat diskuteras. I detta kapitel förklaras vilka slutsatser som går att dra utifrån studiens resultat samt hur dessa relaterar till Försvarsmaktens arbete med säkerhetsanalyser av IT-system.

2 Litteraturgenomgången

För att svara på de fem frågorna i avsnitt 1.3 gjordes en systematisk genomgång av relevant litteratur. En systematisk litteraturgenomgång syftar till att identifiera, utvärdera och tolka all den forskning och litteratur som relaterar till en eller flera väl specificerade frågor (Kitchenham, 2004). För att öka transparensen och repeterbarheten görs detta enligt ett fördefinierat protokoll som beskriver systematiken. Nedan beskrivs detta protokoll i avsnitten *sökstrategi*, *urvalskriterier*, *extrahering av data* samt *syntes och sammanställning*.

2.1 Sökstrategi

Litteraturgenomgången syftade till att svara på de frågor som presenterades i avsnitt 1.3. Under sökningen gjordes antagandet att etablerade metoder skulle refereras på Internet och därmed gå att identifiera genom internetsökningar. Indexeringstjänsterna Google och Google Scholar användes för att identifiera dokument som innehåller begrepp som *security assessment*, *security analysis method, security analysis, risk assessment*, *risk analysis method* och *risk analysis*. Utöver detta användes också resultat från tidigare litteraturstudier för att identifiera relevanta metoder (ENISA, 2007; Fenz & Ekelhart, 2011; Filippini & Schimmer, 2012; Johansson, 2005; Macedo, 2009; Sommestad, 2012; Syalim et al., 2009). Sökningarna resulterade i totalt 74 metoder som inkluderades för vidare analys.

2.2 Urvalskriterier

Efter sökningen gick författarna igenom de identifierade dokumenten och bestämde under gemensamma möten vilka metoder som skulle inkluderas. Huvudkraven för att en metod skulle inkluderas var att:

- dokumentet specificerar en fullständig metod för att bedöma informations-säkerhetsrisker kopplade till IT-system
- metoden är tillgänglig för granskarna på antingen svenska eller engelska
- metoden är etablerad och tillämpad i flera fall.

Exempel på metoder som exkluderats:

Österreichisches Informationssicherheits-handbuch exkluderades för att den bara finns på tyska.

Sandia Risk Assessment Methodology exkluderades för att det inte var en metod för informationssäkerhet.

Simple to apply risk analysis (SARA) exkluderades för att den kostar £27000.

Huruvida en metod var etablerad eller ej bedömdes av författarna baserat på andras beskrivningar av metoden (exempelvis på bloggar och hemsidor), vem som har publicerat dokumentet (exempelvis om det var en guide utgiven av en myndighet) samt antalet referenser och länkar som fanns till dokumentet i fråga från vetenskapliga publikationer och på Internet i allmänhet. Varje dokument granskades av två personer. Trots att bedömningen är förhållandevis subjektiv rådde stor samstämmighet mellan granskarna. Totalt mötte femton metoder de kriterier som har ställts upp.

2.3 Extrahering av data

Flera av dokumenten som inkluderades är över 100 sidor långa med detaljerade beskrivningar av de steg som ingår i processen. Den genomförda litteraturgenomgången syftade till att svara på specifika frågor och därför var endast en delmängd av innehållet av intresse. Ett dataextraheringsark utarbetades och användes för att granskarna, på ett spårbart och entydigt sätt, skulle kunna identifiera de relevanta delarna. Extraheringsarket hade fält för

- metainformation (exempelvis antalet sidor i dokumentet)
- målgrupp för dokumentet (exempelvis tilltänkt användare)
- dokumentation av resultatet (exempelvis hur sårbarheter ska beskrivas)
- den indata och utdata som anges i metodens precessbeskrivning, dvs. de begrepp som detaljerar vilken information som behövs enligt metoden.

För att säkerställa att extraheringen genomfördes på ett tillförlitligt sätt gjordes den av två granskare för varje dokument. Efter extrahering jämfördes resultaten (exempelvis vilken systeminformation som metoden krävde) från de två granskarna.

I de fall metoden innehöll flera redundanta beskrivningar togs ett gemensamt beslut om vilken data som skulle extraheras. De avsnitt som valdes återges i Appendix B. För 12 av de 15 metoder som uppfyllde urvalskriterierna specificerades indata och utdata i processbeskrivningen.

Exempel på begrepp som extraherades:

Asset, Asset/resource criticality, Vulnerability, Emerging threats, IT budgets, Application architecture, Staff threat profile, Asset data flows, The system topology, Service Providers, Audit Reports, Legal Files (Contracts, MOU).

2.4 Syntes och sammanställning

I många fall är målet med en systematisk litteraturgenomgång att komma fram till en så kallad metaanalys där olika studiers kvantitativa resultat vägs samman för att skapa ett mer träffsäkert medelvärde. I fall som detta, där forskningen och

litteraturen handlar om kvalitativa frågor (och saknar kvantitativa data) beskrivs istället resultatet i form av tabeller och figurer (Kitchenham, 2004).

Syntesen i denna litteraturgenomgång gjordes i flera steg. I det första steget gjordes en koppling mellan de extraherade begreppen och koncept som är generella i IT-systemsammanhang. Som facit på vilka koncept som är relevanta för beslutsfattare inom IT-domänen i största allmänhet användes modelleringsspråket Archimate. Archimate är en standard som utges av The Open Group som och som, inklusive officiella utökningar, definierar 40 koncept som enligt skaparna ska vara relevanta för beskrivning och planering av IT-förändringar (Appendix A). Enligt den officiella beskrivningen[1] erbjuder Archimate ”*a common language for describing the construction and operation of business processes, organizational structures, information flows, IT systems, and technical infrastructure”*. På en högre abstraktionsnivå delas de 40 Archimate-koncepten in i 11 grupper.

Modelleringsspråket Archimate:

Archimate beskriver 40 koncept och relationerna mellan dessa. De beskriver *Passiv Struktur*, *Beteende* och *Aktiv Struktur* för *Verksamheter*, *Applikationer* och *Infrastruktur*. Utöver detta finns utökningar för att beskriva mål och krav. Exempel på centrala begrepp är: *Business Process*, *Business Actor*, *Application Component*, *Application Collaboration*, Node, *Infrastructure Service* och *Driver*.

Två granskare kopplade varje extraherat begrepp mot koncepten i Archimate. Granskarna kopplade varje begrepp mot ett eller flera av Archimates 40 koncept och angav på skalan 1 (låg) till 3 (hög) hur säkra de var i sina bedömningar. Om det extraherade begreppet ansågs vara alltför brett för att kopplas mot Archimate kunde detta anges som en kommentar. Granskaren kunde även ange ifall viktig information gick förlorad om ett extraherat begrepp kopplades mot ett koncept i Archimate. På grund av den stora variationen i terminologi och abstraktionsnivå var det i många fall svårt att på ett konsekvent sätt koppla begreppen mot Archimates 40 koncept. Efter att de två granskarna var för sig hade kategoriserat en metods begrepp mot koncepten i Archimate diskuterades likheter och skillnader för att nå konsensus. Följande ger en indikation på hur säkra granskarna var i sina enskilda bedömningar och hur samstämmiga (eller olika) granskarnas syn var på hur begreppen skulle kopplas.Av de kopplingar som gjordes var 42 procent gjorda med hög konfidens, 35 procent med medelhög konfidens och 24 procent med låg konfidens.

- När en granskare angav att ett begrepp var alltför allmänt eller brett så hade även den andra granskaren gjort det i 6 procent av fallen och osäker (lägsta konfidensnivån) i 13 procent av fallen.

[1] http://www.opengroup.org/subjectareas/enterprise/archimate

- När en av granskarna var riktigt säker på hur ett begrepp skulle kopplas (dvs. satte en trea på ett eller flera koncept) så hade också den andra granskaren markerat minst ett av dessa Archimate-koncept i 60 procent av fallen och minst en av de aktuella grupperna av Archimate-koncept i 73 procent av fallen.
- När granskarna var oense även kring vilken Archimate-grupp som ett begrepp hörde till hade åtminstone en av granskarna den lägsta konfidensnivån i kopplingen i 64 procent av fallen.

Det kan tilläggas att det ofta fanns en uppenbar koppling mellan de koncept som granskarna valt i de fall granskarna var oense. Det finns exempelvis en tydlig koppling mellan *Contract* och *Requirement*, mellan *Application interface* och *Application interaction,* mellan *Business collaboration* och *Business interaction* och mellan *Business object* och *Data Object*. Det kan även tilläggas att vissa begrepp har en oklar relation till informationssäkerhet och IT och således var svåra att koppla. Ett exempel på detta är *Furniture*.

De begrepp som i konsensus klassificerats som säkerhetsspecifika sorterades in i grupper. Sorteringen gjordes för att reducera antalet begrepp (109 stycken) till färre begrepp (11 stycken) som fångade de ingående begreppens gemensamma drag.

3 Resultat

I detta kapitel ges först en översikt av de inkluderade metoderna. Därefter besvaras de fem forskningsfrågorna (se avsnitt 1.3) i tur och ordning. Sist sammanfattas resultatet.

3.1 Inkluderade metoder

Den systematiska litteraturgenomgången resulterade i 15 riskhanteringsmetoder som uppfyllde urvalskriterierna. Metoderna varierar avseende exempelvis omfattning, inriktning och hur analysresultaten kvantifieras. I Tabell 1 ges en överblick av dem. I Appendix B finns information om vilka delar som begrepp extraherades från. I Appendix C beskrivs metodernas definition av risk.

Tabell 1: Metoder som mötte de kriterier som ställts upp.

ID	Namn (referens)	Antal sidor	Livs-cykel[2]
ISO27005	ISO/IEC 27005 Information technology – Security techniques – Information security risk management (ISO/IEC, 2011)	76	P&B
FAIR	Factor Analysis of Information Risk (Jones, 2005)	76	P&B
RMF	NIST Risk Management Framework (NIST, 2012)	1142	P&B
MAGERIT	Methodology for Information Systems Risk Analysis and Management (Ministerio de Administraciones Públicas, 2006)	267	P&B
Grundschutz	BSI-Standard 100-3 Risk analysis based on IT-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik, 2008)	23	P&B
TARA	Threat Agent Risk Assessment (Rosenquist, 2009)	114	P
MEHARI	MEthode Harmonisée d'Analyse de RIsque (Club de la Sécurité de l'Information Français, 2011)	46	B
TRITF	The Risk IT Framework (ISACA, 2009)	107	P&B
ISRAM	Information Security Risk Analysis Method (Karabacak & Sogukpinar, 2005)	13	P
CORAS	CORAS (Lund, Solhaug, & Stølen, 2011)	456	P&B
TSRMG	The Security Risk Management Guide (Microsoft Solutions for Security and Compliance & Microsoft Security Center of Excellence, 2006)	129	P&B
TRA-1	Harmonized Threat and Risk Assessment Methodology (Communications Security Establishment & Royal Canadian Mounted Police, 2007)	290	P&B
OCTAVE	The Operationally Critical Threat, Asset, and Vulnerability Evaluation (Carnegie Mellon University, 2001)	1113	B
MG-3	A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems (Communications Security Establishment (CSE), 1996)	73	P&B
HMG IA	HMG IA Standard No. 1 Technical Risk Assessment (National Technical Authority for Information Assurance, 2009)	114	P&B

[2] Syftar på om ett IT-system är planerat (P) eller befintligt (B).

3.2 Situationer med flera systemägare

Endast sex metoder tar upp problematiken som kan uppstå när system med flera systemägare eller verksamhetsägare analyseras. Av dessa gör endast fyra det på ett sätt som inkluderar förslag på hur situationen kan hanteras. Tabell 2 sammanfattar innehållet.

Tabell 2: Sammanfattning av förslag på hur situationer med flera systemägare ska hanteras (endast de som tar upp problemet finns med i tabellen).

ID	Förslag
ISO27005	Att en ägare skall identifieras för varje tillgång för att säkerställa ansvar. En gräns måste dras för vad som inkluderas i granskningen/analysen. Ägarna av tillgången bör kunna hjälpa till att identifiera hot.
RMF	Problemet nämns endast som något att ta hänsyn till. Förslag på hur detta ska göras ges ej.
CORAS	Olika parter nämns och diskuteras. Riskanalysen berör dock endast de organisationer som analysen görs på uppdrag av.
TSRMG	En holistisk ansats bör tas fram då det som är bäst för en affärsenhet inte behöver vara bäst för den organisation som den ingår i. Vissa enheter kommer instinktivt att vilja driva processen åt ett håll som gynnar deras del av organisationen.
TRA-1	Metoden slår fast att det vid analyser av sammankoppande IT-system kan finnas en tendens att utöka och bredda riskanalysen till att täcka alla sammankopplade delar. För att undvika överväldigande uppgifter rekommenderas det att riskanalysen delas upp i moduler som var och en tar fasta på ett visst nätverkssegment, en viss applikation eller en viss affärsfunktion.
MG-3	Riskanalysens gränser måste definieras i termer av ett fysiskt IT-system och logiska analysgränser. När sammankopplingar till externa IT-system finns måste alla gränssnitts karakteristik beskrivas noggrant. Beställaren av analysen och riskanalytikern definierar omfattningen av analysen, som beskrivs genom att definiera: • **Fokus**. Om det är något som ska prioriteras i analysen. Exempelvis särskilda tillgångar, hotagenter eller systemaspekter. • **Bredd**. Hur många delar av systemdesignen som ska tas med. Exempelvis kan det beslutas att ett nätverk är så säkert att det inte behöver inkluderas i analysen. • **Djup.** Detaljnivån som krävs i riskanalysen. Olika nivåer kan användas för olika delar av systemet. Detaljnivån ökar i regel ju längre fram i livscykeln systemet befinner sig.

3.3 Generell IT-relaterad information som krävs

Generell IT-relaterad information är i denna studie den information som täcks in av modelleringsspråket Archimate. Archimate är skapat för att vara ett grundläggande stöd vid skapandet av företagsövergripande arkitekturer för IT-lösningar.

Efter att granskarnas enskilda resultat hade sammanställts aggregerades antalet tillfällen då de olika koncepten för generell IT-relaterad information hade använts i de olika metoddokumenten. Totalt hade 748 kopplingar gjorts mellan Archimate-koncept och de begrepp som extraherats från metod-beskrivningarna. Tabell 3 anger hur ofta olika Archimate-koncept använts och vilka delar av Archimate som dessa återfinns i.

Som tabellen visar är det främst verksamhetsinformation som efterfrågas av metoderna. Av de begrepp som efterfrågas har 43 procent en koppling till verksamheten. *Motivation*, och då främst koncepten *utvärderingar*, *krav* och *begränsningar*, är också vanligt förekommande. Likaså inkluderas *teknikstruktur* (som koncepten *nätverk* och *enheter*) ofta i säkerhetsanalysen – över hälften av begreppen har en koppling till strukturella koncept.

Sammanställningen visar också att vissa delar verkar vara av ringa intresse när metoderna ska användas. De tre Archimate-grupper som fångar beteende utgör endast 16 procent av de extraherade begreppen. Archimate-koncept som används för att beskriva implementations- och migrationsprojekt har endast varit aktuella nio gånger, dvs. för cirka en procent av begreppen.

Tabell 3: Generell IT-relaterad information som extraherats ur dokumenten kopplad till Archimate-grupper och Archimate-koncept. Antalet och andelen förekomster av begrepp anges inom parentes. (Vår svenska översättning av Archimate.)

Archimate-grupp (antal; andel)	**Archimate-koncept (antal)**
Motivation (126; 17%)	Intressent (6) Drivkraft (18) Utvärdering (35) Mål (2) Princip (6) Krav (24) Begränsning (35)
Implementation & migration (9; 1%)	Platå (0) Gap (5) Leverabel (1) Arbetspaket (3)
Verksamhetsinformation (77; 10%)	Produkt (3) Värde (27) Representation (14) Kontrakt (11) Verksamhetsbetydelse (22)
Verksamhetsstruktur (186; 25%)	Verksamhetsgränssnitt (3) Affärssamarbete (4) Verksamhetsobjekt (59) Verksamhetsroll (46) Verksamhetsaktör (55) Plats (19)
Verksamhetsbeteende (58; 8%)	Verksamhetstjänst (7) Verksamhetshändelse (19) Verksamhetsfunktion/process/interaktion (32)
Applikationsstruktur (89; 12%)	Applikationsgränssnitt (14) Applikationssamarbete (13) Dataobjekt (34) Applikationskomponent (28)
Applikationsbeteende (27; 4%)	Applikationstjänst (11) Applikationsinteraktion/funktion (16)
Teknikinformation (15; 2%)	Artefakt (15)
Teknikstruktur (133; 18%)	Infrastrukturgränssnitt (9) Nod (18) Kommunikationsväg (13) Systemmjukvara (24) Apparat (41) Nätverk (28)
Teknikbeteende (28; 4%)	Infrastrukturtjänst (19) Infrastrukturfunktion (9)

3.4 Information specifik för informationssäkerhet

Bland de begrepp som extraherades fanns det många som ansågs vara säkerhetsspecifika. Eftersom Archimate är ett brett modelleringsspråk och avsett att användas för flera IT-relaterade typer av problemställningar är inte säkerhet i fokus. För att beskriva vilken säkerhetsspecifik information som säkerhetsanalysmetoderna kräver har en kortsortering genomförts med de säkerhetsspecifika begreppen. Syftet med kortsorteringen var att gruppera liknande begrepp och därigenom erhålla grupper som illustrerar vilken säkerhetsspecifik information som anses vara nödvändigt underlag vid genomförandet av säkerhetsanalyser för IT-system. Kortsorteringen genomfördes av en granskare och resulterade i 11 grupper (Tabell 4).

Tabell 4: Identifierade grupper för säkerhetsspecifika begrepp, antal begrepp de innehåller, de metoder som begreppen kommer ifrån samt exempel på begrepp som ingår i gruppen.

Grupp	Antal begrepp	Metoder	Exempel
Incident- och analyshistorik	11	TRITF ISO27005 MAGERIT	• Erfarenhet av hot • Incidenter i organisationen
Tillgångar	16	TRITF MEHARI TSRMG MAGERIT OCTAVE RMF	• Kritiska tillgångar • Resultat av säkerhetskategorisering av information och IT-system • Etablerade skalor för felfunktionsvärden
Hot	5	TRITF ISO27005 TSRMG OCTAVE	• Orsaker eller händelser som kan ha negativ påverkan på tillgångar • IT-riskproblem • Hot mot kritiska tillgångar
Sårbarheter	5	ISO27005 OCTAVE	• Lista med sårbarheter relaterade tillgångar, hot och säkerhetsåtgärder • Katalog med mjukvarusårbarheter • Organisatoriska sårbarheter
Säkerhetsåtgärder	32	Grundschutz TRA-1 TRITF ISO27005 MAGERIT OCTAVE MG-3 RMF	• Existerande säkerhetsåtgärder • Dokumentation av säkerhetsåtgärder • Verksamhetsnytta kopplad till IT-risker
Omfattning	14	Grundschutz TRITF ISO27005 MEHARI OCTAVE RMF	• Omfattning och gränser för riskanalysen • Säkerhetsmål • Typer av risker som ingår i analysen
Utvärderingar	3	TRITF	• Test av förmåga att fortsätta leverera
Metod	2	MEHARI OCTAVE	• Förståelse för analysmetoden
Krav	13	Grundschutz TRITF MEHARI OCTAVE RMF	• Säkerhetskrav för använda tillämpningsprogram • Katalog med legala krav och regelverkskrav relaterade till leverans av IT-tjänster • Säkerhetskrav för kritiska tillgångar
Externa parter	5	ISO27005 MEHARI	• Beroenden av externa parter • Kritiska externa leverantörer av mjukvara
Säkerhetsstrategi och organisation	8	TRITF MEHARI MAGERIT RMF	• Toleransnivå för IT-risker • Informationssäkerhetspolicy • Fördelning av ansvar för säkerhet

3.5 Roller och organisationer av relevans

När en säkerhetsanalys ska genomföras behöver vissa roller och vissa organisationer involveras. Vilka dessa är påverkas av vilka indata metoden kräver. Exempelvis finns i de allra flesta organisationer vissa roller som kan verksamheten och andra som kan de tekniska systemen. Ett sätt att identifiera roller och organisationer som behöver involveras, och till vilken grad detta bör ske, är därför att utgår från vilken information som behövs och involvera lämpliga roller och organisationer med detta som utgångspunkt. Vilken typ av information som behövs enligt de etablerade metoderna står i Tabell 3.

Tabell 5 utgör en sammanställning av informationskällor som förespråkas i de olika metoddokumenten. Notera att endast nio metoder anger relevanta informationskällor.

Tabell 5. Informationskällor som metoderna tar upp.

Metod	Föreslagna informationskällor
ISO27005	• Informationsdirektör, informationssystemsansvarig, lokalansvarig, verksamhetsansvarig och användare som föreslagna säkerhetsåtgärder implementeras för. • Existerade dokumentation om kontroller och riskbehandlingsplaner.
FAIR	• Ämnesexperter (juridik, verksamhets IT-drift, etc.) sägs kunna förbättra uppskattningarna betydligt.
MAGERIT	• Inventarierlistor, modeller och annan organisatorisk information, de som är ansvariga, styrgruppen, specialister på skyddsåtgärder och kataloger över skyddsåtgärder.
ISRAM	• Enkäter skickade till chefer, direktörer, teknisk personal, och vanliga användare.
CORAS	• Kunden och dess representanter är huvudkällan till information.
TSRMG	• Verksamhetsägare ska bestämma tillgångars värde; informationssäkerhetsgruppen ska bestämma sannolikheten för påverkan på verksamhetstillgångar; IT-ingenjörer ska designa tekniska lösningar och uppskatta utvecklingskostnader; IT-driften ska designa verksamhetsdelen av lösningen och uppskatta verksamhetskostnader. • Följande källor tas också upp: verksamhetens nya drivkrafter, tidigare riskbedömningar, revisioner, tidigare incidenter, ”bulletins”, industrievent och allmänna säkerhetsriktlinjer.
TRA-1	• Program- och verksamhetschefer för att värdera anställda, tillgångar och tjänster; projektledare och deras anställda för att översätta verksamhetskrav till tekniska krav; lokalansvariga och informationschefer tillsammans med deras anställda kan bidra med information om delade utrymmen och teknisk infrastruktur; avdelningars säkerhetsansvariga (av olika slag) kan ge råd och vägledning avseende hotmiljö och skyddsalternativ. • Utöver detta listas en stor mängd roller och titlar av relevans i dokumentets appendix A och B.
OCTAVE	• Källorna skiftar mellan processens steg. Huvudkällorna är högsta ledningen för att få ”enterprise knowledge”; verksamhetsaområdesansvariga för att få ”operational area knowledge”; anställda för att få ”staff knowledge”.
MG-3	• Systemspecialister för att ge sårbarhetsinformation; användarrepresentanter för att kunna bedöma risken de utgör; säkerhetsingenjörer för att ge rekommendationer om skydd. • Dessutom påpekas att sårbarhetsinformation kan fås från: tidigare analyser, databaser och listor, produktutvärderingar eller myndigheters bedömningar och sårbarhetsregister.

3.6 Metoders samstämmighet

Vissa säkerhetsanalysmetoder beskriver detaljerat vilken information som behövs under en säkerhetsanalys, vissa nöjer sig med övergripande formuleringar. Som följd av detta varierade antalet kopplingar till Archimate-koncept för de olika metoderna. För *HMG IA* och *CORAS* gjordes endast 5 respektive 6 kopplingar till Archimate-koncept; i den andra ändan av skalan finns *MAGERIT* med 116 kopplingar till Archimate-koncept. Sammanställningen i Tabell 3 ovan visar hur Archimate-koncepten har använts generellt, men tar inte hänsyn till att tonvikten skiljer sig mellan metoderna. Tabell 6 beskriver vilken Archimate-grupp de olika metodernas begrepp oftast kopplas till. Som tabellen visar är vissa metoder fokuserade på vad som motiverar analyserna (främst *Grundschutz*, *TRITF* och *TSRMG*) medan andra är fokuserade på verksamhetens struktur (som *TRA-1* och *OCTAVE*). Det är också noterbart att några metoder inte alls använder begrepp som hör till Archimate-grupperna som berör applikationer eller teknik. De med jämnast fördelning över Archimate-grupperna är kanadensiska *MG-3* och amerikanska *RMF*.anadensiskaanadensiska

Tabell 6. Antalet kopplingar till Archimate-grupper för de olika metoderna samt andelen av kopplingarna till de olika Archimate-grupperna (anges i procent). Färgerna illustrerar storleken på den relativa vikten.

Archimate-grupp	**Grundschutz**	**TRA-1**	**TRITF**	**CORAS**	**ISO27005**	**MEHARI**	**TSRMG**	**MAGERIT**	**OCTAVE**	**MG-3**	**RMF**	**HMG IA**
Motivation	44%	6%	43%	0%	23%	25%	42%	0%	13%	12%	9%	20%
Implementation & migration	0%	0%	2%	0%	5%	1%	0%	1%	1%	2%	0%	0%
Verksamhetsinformation	33%	6%	15%	67%	5%	8%	3%	9%	16%	2%	13%	0%
Verksamhetsstruktur	0%	36%	19%	33%	20%	30%	16%	25%	42%	16%	11%	20%
Verksamhetsbeteende	0%	3%	20%	0%	11%	8%	26%	4%	4%	5%	4%	0%
Applikationsstruktur	0%	19%	0%	0%	9%	9%	6%	19%	2%	23%	20%	0%
Applikationsbeteende	0%	0%	1%	0%	6%	1%	0%	3%	1%	12%	11%	20%
Teknikinformation	0%	12%	0%	0%	2%	0%	0%	0%	0%	0%	2%	0%
Teknikstruktur	22%	18%	0%	0%	15%	16%	6%	31%	20%	19%	25%	0%
Teknikbeteende	0%	0%	0%	0%	6%	1%	0%	9%	0%	9%	7%	40%

3.7 Sammanfattning av resultat

Under studien identifierades 15 etablerade metoder som specificerar hur risker med IT-system ska analyseras. Tolv av dessa metoder anger vilken information som behöver samlas in för att kunna genomföra en säkerhetsanalys. Nio metoder ger förslag på vilka källor som ska konsulteras. Fyra metoder ger förslag på hur situationer med flera systemägare kan hanteras.

Avseende allmän information föreskriver metoderna framförallt att information om olika typer av strukturer (verksamhet, applikationer och teknik) ska ligga till grund för analysen. Oftast är det information relaterad till verksamhet som efterfrågas. Överlag prioriteras inte information om vilken information som finns eller hanteras, inte heller prioriteras information om beteende eller information om tekniska lösningar. Ungefär en sjundedel av de identifierade begreppen, som beskriver nödvändig information, är säkerhetsspecifika; sex sjundedelar av begreppen är alltså generella.

Ett annat resultat är att det skiljer sig mycket mellan vilken typ av information metoderna anser att säkerhetsanalysen ska baseras på. Några metoder är helt fokuserade på verksamhet medan de flesta tycker att det även behövs teknisk information, framförallt med avseende på teknikstruktur.

Generellt visar resultaten i detta kapitel att det finns en stor mängd olika typer av information av vitt skild karaktär som kan ligga till grund för en säkerhetsanalys.

4 Diskussion

Resultatens reliabilitet och validitet diskuteras i avsnitt 4.1. Därefter ges råd angående befintliga metoder och rekommendationer till Försvarsmakten.

4.1 Reliabilitet och validitet

Frågan om hur säkra resultaten är kan delas upp i två delfrågor:

- Reliabilitet: skulle andra granskare komma fram till samma resultat om de gjorde om studien enligt samma metod?
- Validitet: är resultaten rättvisande och korrekta?

Avseende reliabilitet är författarna av denna rapport ganska säkra på att rätt metoder har inkluderats och att rätt information har extraherats från dessa. Alla granskarna har gjort liknande översiktsstudier tidigare och är väl bekanta med säkerhetsanalyser inom IT- och informationssäkerhet. Tydliga kriterier har dessutom använts för såväl inkludering av metoder som identifiering av begrepp att extrahera. Kopplingen mellan de extraherade begreppen och Archimates koncept är dock mindre tillförlitlig. Punktlistan i avsnitt 2.4 visar att det finns betydande skillnader mellan hur de olika granskarna gjort kopplingar.

Det är egentligen inte konstigt att begreppen är svåra att koppla – skaparna av metoderna har med största sannolikhet inte tänkt i termer av Archimate när de skrev metodbeskrivningarna. Att de begrepp som extraherats från metoderna i många fall är diffusa och otydliga gjorde det också svårt att koppla ihop dem med Archimates koncept. Osäkerheten och olikheterna i granskarnas kopplingar antyder att en annan grupp granskare skulle producera ett annat resultat. Vår bedömning är dock att en ny studie skulle uppvisa samma tendenser. Exempelvis anser vi det sannolikt att en annan grupp granskare också skulle finna att verksamhetsinformation och information om struktur är det som används mest i metoderna.

Denna rapport presenterar primärt beskrivande resultat och det finns därför få slutsatser som behöver validitet. En relevant fråga är ifall beskrivningen är rättvisande. Det vill säga om extraheringen av begrepp som nämns i metodernas textbeskrivningar fångar den information som metodskaparna egentligen tycker är viktig och om den fångar den information som i praktiken behövs om metoden ska tillämpas. Vi anser att det är svårt att göra en rakare tolkning av metodbeskrivningarna än vad som gjorts i denna rapport – att extrahera de begrepp som nämns i metodens steg. Men det är möjligt att extraheringen missade begrepp som finns med i andra delar av metodbeskrivningarna. Därmed finns det utrymme för att komplettera de listor med begrepp som har extraherats.

4.2 Val av metod

Det finns betydande skillnader mellan vilken information de olika metoderna anser ska ligga till grund för analyserna. Ingen av metoderna motiverar sina val och det blir därför svårt att identifiera vilken metod som bäst motsvarar Försvarsmaktens förutsättningar. Att metoderna är etablerade gör inte valet enklare – att bara följa strömmen är inte lätt när den delar upp sig. Författarnas erfarenhet är att de flesta som använder en etablerad metod anpassar denna till sin egen organisation och dessutom förenklar metoderna en hel del. Det stora behovet av att anpassa metoderna till aktuell organisation gör valet av metod mindre viktigt.

Förutom att metoderna är generella avseende vilken information som ska ligga till grund för säkerhetsanalysen ger de även få svar när det kommer till de moment som är erkänt svåra och problematiska. Exempelvis ges inte svar på vilka matematiska operationer som skall genomföras för att med hjälp av informationen kvantifiera konsekvensers allvarlighet eller angrepps sannolikhet. Inte heller finns tydliga beskrivningar av vilken bakgrund eller utbildning de som bedömer risker ska ha. Inget av detta är särskilt förvånande – det finns nämligen ingen forskning som ger bra svar på frågorna.

4.3 Rekommendationer till Försvarsmakten

Försvarsmakten bör fundera över hur specifika metodbeskrivningar och verktygsstöd ska vara med avseende på vilken information som ska ligga till grund för säkerhetsanalyser inom ramen för auktorisations- och ackrediterings-processen för IT-system. Hänsyn bör tas till såväl krav på säkerhetsalysens detaljnivå som andra processer och styrinstrument som finns i Försvarsmakten.

Om träffsäkra och effektiva analyser är målet med säkerhetsanalyserna är en mer standardiserad och checklistebaserad metod att föredra. Det är exempelvis rimligt att hotbilden är densamma för de allra flesta system, men som processen ser ut nu genomförs en ny hotanalys inom ramen för varje säkerhetsanalys. Det är också rimligt att tänka sig att samma typer av tekniska, processrelaterade och människorelaterade sårbarheter återkommer i säkerhetsanalyserna, men ingen beskrivande katalog över dessa finns att tillgå. Krav på Säkerhetsfunktioner (KSF) är härledda från en central och standardiserad uppfattning om hotbilden och går i denna riktning. Med ytterligare standardisering skulle domänexperter kunna fördefiniera så gott som allt utom verksamhetsbeskrivning och värdering av tillgångar. Det skulle då kunna säkerställas att allt som är relevant i befintlig hotbild täcks in i säkerhetsanalyserna och att de beslut som fattas om exempelvis skydd har gjorts av domänexperter.

Mer standardisering är en väg framåt om träffsäkra resultat är det överordnade målet med att genomföra en säkerhetsanalys. Försvarsmakten bör dock fundera

på om andra tänkbara mål också är av vikt. Sådana mål kan exempelvis vara att systemägarna ska bekanta sig med riskerna eller att hitta en optimal lösningsdesign ur ett informationssäkerhetsperspektiv.

5 Referenser

Bundesamt für Sicherheit in der Informationstechnik. (2008). BSI-Standard 100-3 Risk analysis based on IT-Grundschutz. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Carnegie Mellon University. (2001, October). OCTAVE Method Implementation Guide v2.0. *The Journal of medicine and philosophy*. USA: Carnegie Mellon University. doi:10.1093/jmp/jhs081

Club de la Sécurité de l'Information Français. (2011). M EHARI 2010 Processing guide for risk analysis and management. Paris: Club de la Sécurité de l'Information Français.

Communications Security Establishment (CSE). (1996). A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems. Ottawa, Canada: Government of Canada.

Communications Security Establishment, & Royal Canadian Mounted Police. (2007). Harmonized Threat and Risk Assessment (TRA) Methodology. Canada: Communications Security Establishment.

ENISA. (2007). *Methodology for evaluating usage and comparison of risk assessment and risk management items* (pp. 1–61).

Fenz, S., & Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. *Security & Privacy, IEEE*, (April). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5510237

Filippini, R., & Schimmer, M. (2012). *Risk assessment methodologies for Critical Infrastructure Protection. Part I : A state of the art*. Ispra (VA), Italy.

Försvarsmakten. (2004). Direktiv för Försvarsmaktens informationsteknikverksamhet. Stockholm: Försvarsmakten.

Försvarsmakten. (2006). Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik. Stockholm: Försvarsmakten.

Försvarsmakten. (2013a). Handbok Säkerhetstjänst Grunder. Stockholm: Försvarsmakten.

Försvarsmakten. (2013b). Processhandbok IT-processen (Bilaga 1 till HKV 2013-06-28 09 100:60203). Stockholm: Försvarsmakten.

Försvarsmakten. (2013c). Handbok Säkerhetstjänst Informationssäkerhet. Stockholm: Försvarsmakten.

ISACA. (2009). The Risk IT Framework. Rolling Meadows, USA: ISACA.

ISO/IEC. (2011). International Standard ISO/IEC 27005. Switzerland: ISO/IEC. Retrieved from http://link.springer.com/chapter/10.1007/978-3-8348-9870-8_3

Johansson, E. (2005). *Assessment of Enterprise Information Security–How to make it Credible and efficient*. *Information Security*. KTH - The Royal Insitute of Technology. Retrieved from http://en.scientificcommons.org/7645483

Jones, J. (2005). An Introduction to Factor Analysis of Information Risk. Colombia & USA: Risk Management Insight.

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147–159. doi:10.1016/j.cose.2004.07.004

Kitchenham, B. (2004). *Procedures for performing systematic reviews* (Vol. 33). Keele, UK: Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.122.3308&rep=rep1&type=pdf

Lund, M. S., Solhaug, B., & Stølen, K. (2011). *Model-Driven Risk Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-12323-8

Macedo, F. N. R. (2009). *Models for Assessing Information Security Risk*. Instituto Superior Técnico.

Microsoft Solutions for Security and Compliance, & Microsoft Security Center of Excellence. (2006). The Security Risk Management Guide. San Francisco, CA, United states: Microsoft Corporation.

Ministerio de Administraciones Públicas. (2006). MAGERIT – version 2 Methodology for Information Systems Risk Analysis and Management Book I – The Method. Madrid: Ministerio de Administraciones Públicas.

National Technical Authority for Information Assurance. (2009). HMG IA Standard No. 1 Technical Risk Assessment. Cheltenham, United Kingdom: National Technical Authority for Information Assurance.

NIST. (2012). NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments. Gaithersburg, USA: NIST.

Rosenquist, M. (2009). Whitepaper: Prioritizing Information Security Risks with Threat Agent Risk Assessment. USA: Intel Information Technology.

Sommestad, T. (2012). *A framework and theory for cyber security assessments*. Royal Institute of Technology (KTH). Retrieved from http://kth.diva-portal.org/smash/record.jsf?pid=diva2:561246

Sommestad, T., Ekstedt, M., & Holm, H. (2013). The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures. *IEEE Systems Journal*, (99), 1–1. doi:10.1109/JSYST.2012.2221853

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. In *2009 International Conference on Availability, Reliability and Security* (pp. 726–731). IEEE. doi:10.1109/ARES.2009.75

Appendix A: Archimate-koncept

Koncept	Definition
Business actor	An organizational entity that is capable of performing behavior.
Business role	The responsibility for performing specific behavior, to which an actor can be assigned.
Business collaboration	An aggregate of two or more business roles that work together to perform collective behavior.
Business interface	A point of access where a business service is made available to the environment.
Location	A conceptual point or extent in space.
Business object	A passive element that has relevance from a business perspective.
Business process	A behavior element that has relevance from a business perspective.
Business function	A behavior element that groups behavior based on a chosen set of criteria (typically required business resources and/or competences).
Business interaction	A behavior element that describes the behavior of a business collaboration.
Business event	Something that happens (internally or externally) and influences behavior (business process, business function, business interaction).
Business service	A service that fulfills a business need for a customer.
Representation	A perceptible form of the information carried by a business object.
Meaning	The knowledge or expertise present in a business object or its representation, given a particular context.
Value	The relative worth, utility, or importance of a business service or product.
Product	A coherent collection of services, accompanied by a contact/set of agreements, which is offered as a whole to (internal or external) customers.
Contract	A formal or informal specification of agreement that specifies the rights and obligations associated with a product.
Application component	A modular, deployable, and replaceable part of a software system that encapsulates its behavior and data and exposes these through a set of interfaces.
Application collaboration	An aggregate of two or more application components that work together to perform collective behavior.
Application interface	A point of access where an application service is made available to a user or another application component.
Data object	A passive element suitable for automated processing.
Application function	A behavior element that groups automated behavior that can be performed by an application component.
Application interaction	A behavior element that describes the behavior of an application collaboration.
Aplication service	A service that exposes automated behavior.
Node	A computational resource upon which artifacts may be stored or deployed for execution.

Koncept	Definition
Device	A hardware resource upon which artifacts may be stored or deployed for execution.
Network	A communication medium between two or more devices.
Communication path	A link between two or more nodes, through which these nodes can exchange data.
Infrastructure interface	A point of access where infrastructure services offered by a node can be accessed by other nodes and application components.
System software	A software environment for specific types of components and objects that are deployed on it in the form of artifacts.
Infrastructure function	A behavior element that groups inftastructural behavior that can be performed by a node.
Infrastructure service	An externally visible unit of functionality, provided by one or more nodes, exposed through well-defined interfaces, and meaningful to the environment.
Artifact	A physical piece of data that is used or produced in a software development process, or by deployemnt and operation of a system.
Stakeholder	The role of an individual, team or organization (or classes thereof) that represents their interests in, or concerns relative to, the outcome of the architecture.
Driver	Something that creates, motivates, and fuels the change in an organization.
Assessment	The outcome of some analysis of some driver.
Goal	An end state that a stakeholder intends to achieve.
Requirement	A statement of need that must be realized by a system.
Constraint	A restriction on the way in which a system is realized.
Principle	A normative property of all systems in a given context, or the way in which they are realized.
Work package	A series of actions designed to accomplish a unique goal within a specified time.
Deliverable	A precisely-defined outcomce of a work package.
Plateau	A relatively stable state of the architecture that exists during a limited period of time.
Gap	An outcome of a gap analysis between two plateaus.

Appendix B: Metodernas processbeskrivningar

Metod	Avsnitt som beskriver processen
ISO27005	Kapitel 7 och 8 samt avsnitt 9.2
FAIR	-Inga delar-
RMF	Avsnitt 3.1 och 3.2
MAGERIT	Avsnitt 3.4.1 till 3.4.4
Grundschutz	Kapitel 2 i *BSI Standard 100-3*.
TARA	-Inga delar-
MEHARI	Hela dokumentet *MEHARI 2010 – Processing guide for risk analysis and management*.
TRITF	Kapitel 12, delarna/processerna: RE1, RE2 och RE3
ISRAM	-Inga delar-
CORAS	Den ”input documentation" och "output documentation" som står i tabellerna med namn enligt "Overview of Step X", där X är numret på steget i processen.
TSRMG	Begrepp som nämns och de appendix som refereras i kapitel 3 och 4.
TRA-1	Appendix B-1 Sources of Asset Data, Appendix C-1 Sources of Threat Data och, Appendix D-1 Sources of Vulnerability Data.
OCTAVE	Processbeskrivningen som finns i form av deras dataflödesdiagram och de indata och utdata som nämns där. De går även att finna i delar benämnda "Summary for Process X", där X är processen i fråga.
MG-3	Begreppen som tas upp i följande avsnitt: 2.2.3 System Description, 2.3.1 Analysis Approach, 2.3.1.3 System Decomposition, 2.3.2 Asset Sensitivity Analysis, 2.4.2 Risk Report, 2.7.1.1 Safeguard Groups
HMG IA	Begreppen som tas upp i steg 1av metoden och som nämns i appendix B.

Appendix C: Metodernas riskdefinition

ID	Risk-definition
ISO27005	An effect of uncertainty on objectives.
FAIR	Risk is derived from loss event frequency and probable loss magnitude.
RMF	A measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.
MAGERIT	Estimate of the degree of exposure to a threat appearing to one or more assets, causing damages or prejudices to the organization.
Grundschutz	-
TARA	-
MEHARI	Function of the likelihood and the impact.
TRITF	The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.
ISRAM	Probability of occurrence of security breach*Consequence of occurrence of security breach.
CORAS	The likelihood of an unwanted incident and its consequence for a specific asset.
TSRMG	The combination of the probability of an event and its consequence.
TRA-1	The chance of a vulnerability being exploited.
OCTAVE	A risk is a measure of the expected loss in the absence of any mitigation actions or countermeasures.
MG-3	A measure indicating the likelihood and consequence of events or acts that could cause a compromise of system asset(s).
HMG IA	In general terms information risk can be thought of as the likelihood that a threat will exploit a vulnerability leading to a business impact.

Denna rapport försöker ge svar på vilken information som, enligt etablerade säkerhetsanalysmetoder, ska ligga till grund för säkerhetsanalyser av IT-system. En studie har genomförts för att identifiera vad etablerade metoder inom området anser ska användas som grund vid genomförandet av säkerhetsanalyser. De initiala sökningarna efter relevanta metoder resulterade i 74 metoder. Av dessa 74 metoder uppfyllde 12 metoder urvalskriterierna samt angav vilken information som bör ligga till grund för genomförandet av säkerhetsanalyser.

Endast en sjundedel av den information som krävs är säkerhetsspecifik information. Metodernas tyngdpunkt ligger således på mer generell information. Med generell information avses exempelvis information om olika typer av strukturer, såsom verksamhetsstruktur och strukturer för tekniska system. Oftast efterfrågas information som relaterar till verksamheten. Överlag prioriteras inte information om vilken information som finns i eller hanteras av ett system. Inte heller prioriteras information om beteende eller information om tekniska lösningar.

Ett annat resultat är att det skiljer sig mycket mellan vilken typ av information metoderna anser att säkerhetsanalysen ska baseras på. Några metoder är helt fokuserade på verksamhet medan de flesta tycker att det även behövs teknisk information, framförallt med avseende på teknikstruktur.

Generellt visar resultaten att det finns en stor mängd olika typer av information av vitt skild karaktär som kan ligga till grund för en säkerhetsanalys.

FOI

ISSN1650-1942

www.foi.se