Risicomanagement krijgt vaste plaats in ITIL 3

ICT-risico- en -securitymanagement ontwikkelt zich van specialisme tot normaal beheerst proces

In de afgelopen vijf jaar is het beheer van moderne ICT-omgevingen sterk geprofessionaliseerd. Het beheer van andermans infrastructuur plus het leveren van ICT-services, als ware het water uit de kraan, is een wereldwijde miljardenindustrie geworden. De tools waarmee het beheer wordt uitgevoerd, zijn veel krachtiger geworden, waardoor dit mede mogelijk wordt. Op het gebied van security management hebben ze ook veel meer functionaliteit gekregen. Het optimaal gebruik hiervan vereist wel dat ook de processen rond het ICT-beheer ingericht zijn voor security management. De auteurs van dit artikel beschrijven hands-on waar security management effectief op te nemen is in de ICT-beheerprocessen.

Paul Overbeek, Jacques Cazemier en Louk Peters

Dit artikel is als volgt opgebouwd: eerst worden enkele trends in security en ICT beschreven, vervolgens komt security management in 'ITIL classic' aan bod, en tot slot wordt ingegaan op security management in ITIL versie 3.

Trends in ICT-beheer en beveiliging

Techniek en integratie
Gelukkig is te constateren dat de technische beveiliging in nieuwe ICT-producten steeds beter wordt. Zelfs notoire onveilige leveranciers komen nu, onder druk van politiek en publieke opinie, met onmiskenbaar veiligere producten. Veelal is beveiliging direct al geïntegreerd in het product. Er wordt ook meer gewerkt op basis van beveiligingsarchitecturen, hoewel hier nog veel winst is te behalen. Voor specifieke beveiligingsservices in zo'n architectuur, denk aan identity en access management, zijn producten beschikbaar die niet leveranciersgebonden zijn.

Naast dit goede nieuws is ook een minder gunstige ontwikkeling: de toenemende ballast aan historische ICT-producten die in de lucht te houden is. Beveiliging moet over de hele linie gelijkwaardig zijn. In een omgeving waarin de integratie van beveiliging zeer divers is, is dat een probleem. Denk hierbij aan afhankelijkheden tussen beter en minder goed beveiligde componenten, zoals een onveilige applicatie op een veilig besturingssysteem. Het risicomanagement zal deze situatie toch moeten faciliteren, bijvoorbeeld door segmentering van de infrastructuur.

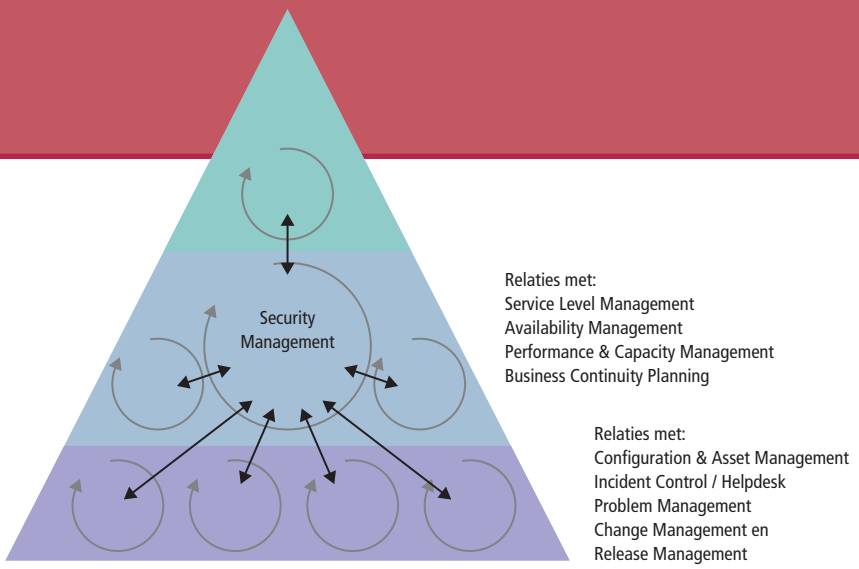
Aantoonbare compliance – ITIL versie 3
Er is inmiddels een veelheid aan methoden en technieken voor beheersing ontstaan. Dit mede onder druk van de toenemende wet- en regelgeving, en omdat klanten niet langer genoegen nemen met 'zeg wat je doet en doe wat je zegt'; ze willen dit ook aangetoond zien. Die veelheid aan methoden en technieken rond security, risk en compliance management vraagt veel van organisaties. Daarom ontstaan er weer tools die voor integratie zorgen, en 'paraplu-methoden'. ITIL versie 3 is zo'n combinatie van best practices voor beheersing van ICT en compliance.

Voor de ontwikkeling van security en risk management is de druk van de compliance-trend een belangrijke steun in de rug.

Dossier security management

Security management wordt steeds meer geïntegreerd in service management, is de boodschap van het openingsartikel in dit *dossier*. Dat blijkt onder andere uit de nieuwe versie van ITIL, waarin informatiebeveiliging duidelijk zijn plaats heeft veroverd. Het blijft echter lastig om het onderwerp op de agenda te houden, zeker op directieniveau. Daarom heeft een Amerikaanse drankenfabrikant besloten om security als merk neer te zetten, en met succes. Tot slot een interview met ICT-dienstverlener Surfnet, die een opensource-spamfilter verbeterde en nu als dienst gaat aanbieden binnen het onderwijs.

- Risico- en security management in ITIL 3 (p. 10)
- Informatiebeveiliging, maak er een merk van! (p. 16)
- Spambestrijding op z'n Nederlands (p. 22)



Figuur 1 Relaties tussen het ITIL-proces Security Management en de andere processen

Maar nu komt het erop aan de verwachtingen waar te maken. Het inpassen van risicomanagement in de ICT-processen is daarbij een kritieke succesfactor.

'ITIL classic'

Het beheer van grote ICT-infrastructuren is doorgaans gestructureerd volgens ITIL of op basis van tools die ITIL ondersteunen. Het ITIL-proces Security Management zorgt voor de structurele inpassing van beveiliging in de beheerorganisatie. Dat proces is mede gebaseerd op de Code voor Informatiebeveiliging en de Amerikaanse tegenhanger van deze standaard.

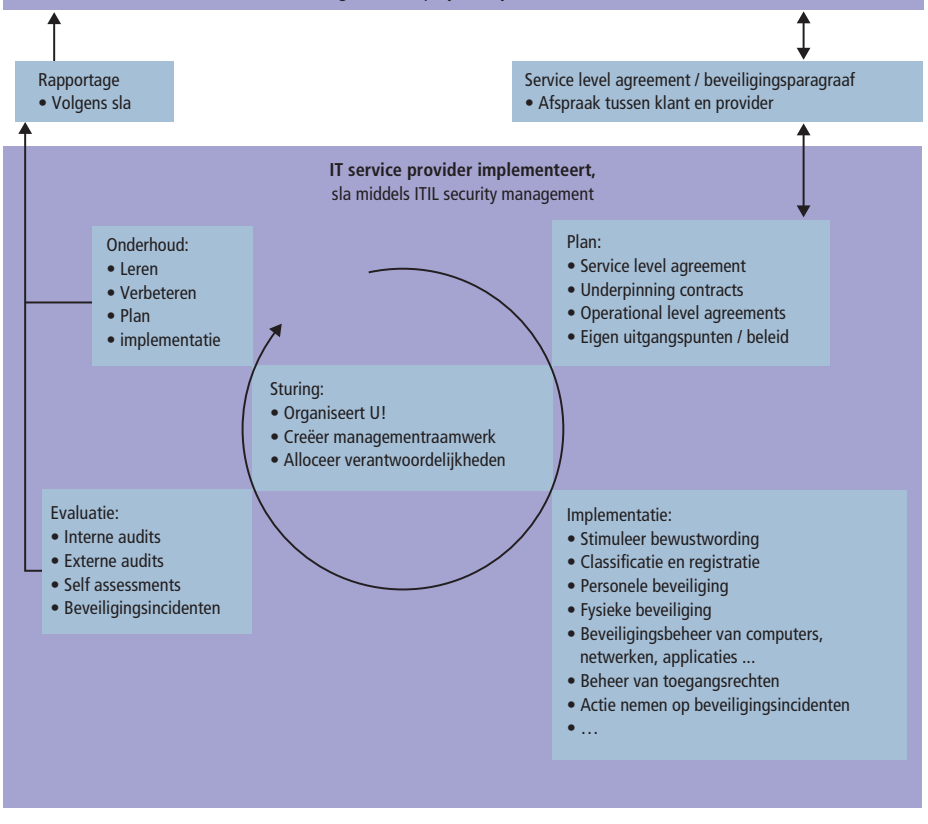
Moderne beheertools bieden ruime mogelijkheden voor security management. In praktijk wordt daar niet volop gebruik van gemaakt, omdat de processen eromheen daar niet op zijn ingericht. Welke beveiligingsactiviteiten zijn praktisch in te passen in de verschillende ITIL-processen van 'ITIL classic', de huidige gebruikte versie van ITIL?

ITIL en Security Management

ITIL gaat uit van een procesmatige benadering van het beheer. Het *doel* van het proces Security Management is tweeledig:

- enerzijds het realiseren van de beveiligingseisen in de verschillende service level agreements (de afspraken met de klant) en andere externe vereisten in contracten, wetgeving en eventueel intern of extern opgelegd beleid;
- anderzijds het realiseren van een zeker basisniveau van beveiliging. Dit is nodig om de eigen continuïteit van de beheerorganisatie te waarborgen. Het is ook nodig om tot vereenvoudiging van het Service Level Management voor informatiebeveiliging te komen. Immers, het beheer is bij een groot aantal verschillende sla's veel complexer dan bij een beperkt aantal.

Het proces Security Management heeft relaties met de meeste andere ITIL-processen. In de andere ITIL-processen vinden namelijk de activiteiten plaats voor beveiliging (zie figuur 1).



Figuur 2 Proces Security Management

ITIL-proces	Beveiligingsactiviteiten
Service Level Management	Beveiliging opnemen in servicecatalogus (basisniveau van beveiliging en additionele beveiligingsservices) Afspraken maken over beveiliging in beveiligingsparagraaf sla Afspraken maken over beveiliging in underpinning contracts Intern de afspraken borgen in processen Rapportage en verantwoording afleggen
Configuration & Asset Management	Classificatie/rubricering van Configuration Items (CI's) bijhouden Procedures koppelen aan classificaties van CI's
Incident Management	Identificeren van beveiligingsincidenten en kwetsbaarheden Procedure voor beveiligingsincidenten volgen
Problem Management	Verbanden tussen beveiligingsincidenten leggen Bewaken van de securityarchitectuur
Change Management	RFC's beoordelen op risico's voor de services Basisbeveiligingsniveau en eventuele additionele beveiligingsmaatregelen bewaken bij doorvoeren Changes Bewaken procedure voor Testen-Acceptatie-Overdracht
Release Management	Sluit aan op Change Management. Zorgt tevens voor communicatielijnen en het voorbereid zijn op problemen.
Availability Management	Werkt samen met Security Management aan beschikbaarheid/continuïteit. Wordt ondersteund door Performance & Capacity management.
Business Continuity Planning	Werkt eveneens met Security Management samen aan continuïteit in het geval van calamiteiten

Tabel 1 Beveiligingsactiviteiten in andere ITIL-processen

Naam handboek	Beschrijft lifecyclefase:
Service Strategy	Bepalen van aan te bieden IT-diensten in functie van de bedrijfsactiviteit
Service Design	Ontwerpen van de IT-dienst op basis van de strategie
Service Transition	Invoeren van de IT-dienst
Service Operation	Uitvoeren van de IT-dienst
Continual Service Improvement	Bijsturen van de dienstverlening

Tabel 2 De vijf handboeken ITIL versie 3

Het Security Management coördineert en voert de regie over de beveiligingsactiviteiten. Daarvoor wordt een normale procescyclus ingericht (zie figuur 2).

Binnen het proces wordt, zoals de figuur ook laat zien, een veelheid aan activiteiten uitgevoerd. Voorbeelden zijn:

- ontwikkelen beveiligingsbeleid en richtlijnen;
- organisatie en verantwoordelijkheden voor informatiebeveiliging;
- OTAP-proces voor beveiliging;
- beveiliging van toegang door derden;
- classificatie en beheersing van informatie en IT-middelen;
- personele beveiliging;
- opleiding en training;
- afhandeling beveiligingsincidenten en monitoren zwakheden;
- treffen disciplinaire maatregelen;
- stimuleren van beveiligingsbewustzijn;
- organiseren veilig beheer;
- toegangsbeveiliging (*access control*);
- onafhankelijke beoordeling (IT-audit).

Rapportage is een belangrijk onderdeel van de activiteiten. Dit vindt plaats om verantwoording af te leggen over de geleverde beveiligingsdiensten en om relevante informatie te verstrekken over beveiliging aan de klanten. Rapportage wordt veelal expliciet afgesproken. De klant moet een correct beeld krijgen van de efficiëntie van de inspanningen (bijvoorbeeld met betrekking tot realisatie van de beveiligingsmaatregelen) en van de beveiligingsmaatregelen zelf. Ook krijgt de klant een rapportage over de beveiligingsincidenten.

Veel van de activiteiten die in het proces Security Management worden aangestuurd of gecoördineerd, worden uitgevoerd binnen andere ITIL-processen. In tabel 1 is een samenvatting opgenomen van beveiligingsactiviteiten in die andere processen. Beveiliging en beheer zijn twee begrippen die dicht bij elkaar staan. Het een kan niet zonder het ander: beveiliging is afhankelijk van beheer en beheer kan niet zonder goede beveiliging. Omdat met het gebruik van ITIL een beheerst proces ontstaat, zullen er ook minder fouten in beheer en beveiliging ontstaan. En dat is een groot winstpunt voor beveiliging.

ITIL versie 3

Hiervoor is 'ITIL classic' oftewel ITIL versie 2 beschreven. Recentelijk is de nieuwe versie, versie 3, beschikbaar gekomen. ITIL v2 kende een procesaanpak; ITIL v3 vertrekt vanuit een service lifecycle model. Niet het invoeren van een bepaald proces (bijvoorbeeld Incident Management) staat centraal, maar de zorg dat de IT-diensten (services) continu beter worden doordat de ondersteunende IT beter en betrouwbaarder wordt. Voor elke IT-dienst zijn vijf fases gedefinieerd. Voor iedere fase bestaat een apart ITIL-handboek (zie tabel 2).

Behalve deze verschuiving naar de servicelifecycleaanpak zijn de belangrijkste algemene veranderingen:

- een versterking van de financiële component van het ICT-beheer. Financial Management is opgewaardeerd en begrippen als return on investment (roi), total cost of ownership (tco) en activity based costing (ABC) hebben een veel belangrijkere positie gekregen;
- het gebruik van sourcingmodellen;
- nastreving van een veel sterkere oriëntatie op de bedrijfsprocessen;
- werken aan planmatige, continue verbetering van de beheerprocessen (hieraan wordt een apart boek gewijd);
- het uitgangspunt is niet meer een min of meer statische ICT-omgeving;

- onderkenning van ook processen, applicaties en informatie als configuratie-items (ci's);
- Incident Management is uitgesplitst in Event Management, Incident Management (afhandeling events) en Request Fulfilment.
- aandacht voor onder andere Service Portfolio Management, Service Catalogue Management, Supplier Management, Service Validation & Testing, Transition Planning, Knowledge Management, Service reporting (zie tabel 3).

De belangrijkste veranderingen ten aanzien van Security Management zijn:
- *Security Management* wordt nu *Information Security Management* genoemd.
- In het boek Service Operation wordt apart aandacht besteed aan Access Management.
- Er is minder aandacht voor beveiligingsmaatregelen.
- Er is meer aandacht voor beveiligingseisen vanuit de business aan een IT-dienst.

ITIL v3 maakt gebruik van een scala aan bestaande methoden en technieken, en beoogt deze geïntegreerd aan te bieden. Net als bij 'ITIL classic' wordt voor het onderwerp Information Security Management een 'best practice guide' gemaakt (zie de auteursinformatie onder aan dit artikel).

Service Strategy
De vijf nieuwe ITIL-boeken worden hier kort beschreven, met hun relevantie voor en impact op beveiliging.
Service Strategy betreft het ontwikkelen van het serviceportfolio, met als doel dit gericht te houden op de zich ontwikkelende behoeften van de klanten van vandaag en de prospects van morgen.
In de servicestrategie ten aanzien van Information Security Management is er aandacht voor:
- identificatie van de security requirements van de klanten van vandaag en morgen en de ontwikkeling daarvan;
- beveiliging als onlosmakelijke eigenschap van een IT-dienst (*warranty*);
- invloed van nieuwe vormen van ICT-gebruik, inclusief applicaties, op security requirements;
- Invloed van trends op security requirements.

Het doel is de strategie te bepalen ten aanzien van het serviceportfolio voor beveiligingsdiensten alsmede Information Security Management. ITIL v3 schuift nadrukkelijk op naar de business, wil de risico's ook kennen en daarop anticiperen. Ook op beveiligingsgebied is een proactieve opstelling nodig. Strategie kan gepositioneerd worden op 'boardroomniveau', als partner van het management, zet toegevoegde waarde centraal en ontzorgt management en andere stakeholders ten aanzien van compliancevraagstukken.

Service Design
Service Design sluit aan op de in *Service Strategy* bepaalde doelstellingen. Het service design ontwerpt de Information Security Management services, opgelijnd met de bedrijfsdoelstellingen en andere doelstellingen uit *Service Strategy*. Het serviceontwerp houdt rekening met de onderkende risico's, neemt deze risico's weg of maakt de restrisico's expliciet. Ook andere security requirements, denk aan die voortkomend uit wet- en regelgeving, worden in het ontwerp opgenomen.

Typische onderwerpen voor Information Security Management in het service design zijn:
- ontwerp van security services;
- service oriented security architectures;
- lifecycle management van security services en architecture;
- return on security investment (rosi).

In het Service Design is een uitgangspunt: '*if you can't measure it, you can't manage it*'. Vandaar dat er veel aandacht wordt besteed aan het formuleren van *metrics,* ook bekend als *performance-indicatoren*. Andere principes zijn het mee-ontwerpen van het deliverymodel, bijvoorbeeld *sourcing*, *partnering*, *business process outsourcing (bpo)* en *layered service provision*. Delivery models beschrijven hoe partijen met elkaar samenwerken in een keten, en hoe (delen van) services op elkaar steunen en op elkaar worden gebouwd.

Zoals gezegd is lifecycle management ook een ontwerpprincipe. In het ontwerp kan meegenomen worden dat een service op een eenvoudig niveau wordt gelanceerd en vervolgens via een aantal plateaus naar het gewenste niveau doorgroeit. Als voorbeeld: een service kan starten met wachtwoordbeveiliging, later worden gecombineerd met een smartcard, met als optie in de toekomst biometrische technieken toe te voegen.

Continual Service Improvement
Continual Service Improvement (CSI) zorgt voor continue afstemming tussen de (security) requirements van de business en de ICT service provision. Dit proces zorgt voor monitoring van de prestaties van de bestaande processen, verbeteren waar dat nodig en mogelijk is, en het doorvoeren van veranderingen volgens de geplande groeipaden in het lifecycle-ontwerp. Het begrip *plateauplanning* komt hier naar voren: het opwaarderen van processen van de ene naar een volgende stabiele situatie.

Voor beveiliging is CSI een interessant proces: er wordt in gemeten, gereviewd en geaudit. In CSI worden de *metrics* gevolgd, ook voor beveiliging. De beheersing van de beveiliging wordt daardoor ondersteund. In de guide voor het Information Security Management-proces zijn *metrics* per *maturity level* gespecificeerd.
CSI is een complex proces, waarover wordt opgemerkt: '*these activities will not happen automatically*'. De winst ervan ligt namelijk in de toekomst; het proces staat dan ook onder druk van de waan van de dag.

ITIL v2-proces	In ITIL v3-boek: Continual Service Improvement	Service Strategy	Service Design	Service Transition	Service Operation
Service Desk					Service Desk
Configuration Management				Asset & Configuration Management	
Incident Management					Incident Management
Problem Management					Problem Management
Change Management				Change Management	
Release Management				Release & Deploy Management	
Service Level Management			Service Level Management		
Availability Management			Availability Management		
Capacity Management			Capacity Management		
Financial Management for IT services		Financial Management			
IT Service Continuity Management			IT Service Continuity Management		
Security Management			Information Security Management		
Nieuw in ITIL v3	The 7-step improvement process	Service Portfolio Management	Service Catalogue Management	Service Validation & Testing	Access Management
	Control of services	Demand Management	Supplier Management	Transition Planning & Support	Event Management
	Servicereporting		Service Portfolio Management	Knowledge Management	Request Fulfilment

Tabel 3 ITIL v2-processen in ITIL v 3

Service Transition
Service Transition beschrijft de problematiek van het invoeren en wijzigen van IT-diensten. Bij alle processen die in dit boek genoemd worden, zoals Service Asset & Configuration Management, Change Management, Release & Deployment Management en Service Validation & Testing, wordt het beveiligingsaspect meegenomen. Veel van deze aspecten zijn in het eerste deel van dit artikel al genoemd.

Service Operation
In *Service Operation* gaat het om het uitvoeren van een IT-dienst conform de beveiligingsstandaarden en –procedures die zijn bepaald in het proces Information Security Management conform *Service Design*. Verder wordt in dit boek kort aandacht besteed aan technische hulp bij beveiligingsissues, controle op wat systeembeheerders wel of niet (mogen) doen, screening, training en goede documentatie.
Nieuwe en opvallend is de specifieke aandacht die in dit boek wordt besteed aan Access Management. *Service Operation* hanteert daarbij een beperkte definitie van beheer van toegangsrechten, namelijk het verlenen van rechten aan geautoriseerde gebruikers voor het gebruik van een IT-dienst.

Visie
Hoewel ITIL versie 3 vele voordelen biedt, zijn er ook kanttekeningen te plaatsen:

- Ten eerste is behalve de omvang ook de complexiteit enorm toegenomen. Dat komt mede doordat versie 3 een aantal good practices combineert zonder tot echte integratie te zijn gekomen. De methoden en technieken die nu worden toegevoegd, zijn maar deels specifiek voor ICT.

- Een consequentie van de servicelife-cycleaanpak is dat activiteiten die bij één proces behoren, dus ook security, in verschillende fasen van de cyclus thuishoren. Dat heeft als nadeel dat de activiteiten rond security nu bijvoorbeeld versnipperd zijn over de verschillende boeken en dat het proces niet meer zo zichtbaar is. Dat vermindert de leesbaarheid voor iemand die het complete plaatje over een

bepaald thema tot zich wil nemen. Een ander nadeel is dat dezelfde activiteiten in meerdere boeken worden beschreven, vanuit net een iets ander perspectief. Voor Information Security Management zijn er voldoende kapstokken, maar ingericht zijn ze nog niet.

- Een andere observatie is de rolwijziging. ITIL, voorheen gepositioneerd als het operationeel houden van de ICT, 'trekt een veel grotere broek aan'. Strategie, bedrijfsdoelstellingen, procesoptimalisatie, roi: allemaal onderwerpen die de klassieke ICT-beheerder niet zo direct in zijn bagage heeft. Natuurlijk is een ontwikkeling in deze richting mogelijk, maar is het een natuurlijke ontwikkeling die eenvoudig zal worden geaccepteerd? Het lijkt op de garagist die in plaats van de auto te repareren het fileprobleem aanpakt.

- Het betere is de vijand van het goede. Een praktische implementatie van ITIL versie 3 kan zijn om vooral de verworvenheden van ITIL classic vast te houden. Vervolgens is veel winst te behalen door elementen zoals lifecycle management en de *metrics* conform CSI toe te voegen. Voor Information Security Management zou dit in ieder geval een belangrijke stap voorwaarts betekenen.

Paul L. Overbeek, Jacques A. Cazemier en Louk Peters zijn tevens de schrijvers van ITIL Security Management (versie 2) en zijn nu bezig met de ontwikkeling van de ' best practice guide' getiteld Process Management Guide for Information Security Management with ITIL v3. Dit boek verschijnt in de tweede helft van dit jaar.
Reacties op dit artikel naar Paul.Overbeek@Ois-NL.EU.

Bronnen/literatuur

- www.itsmf.nl: informatie over ITIL versie 3
- ITIL Security Management is gebaseerd op de *Code voor Informatiebeveiliging*: *Code of Practice for Information Security Management*, ISO 27000-serie
- Office of Government Commerce, J. Cazemier, P. Overbeek, L. Peters, *Best Practice for Security Management,* 8th Impression 2004, The Stationary Office
- Overbeek, P., E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder Controle*, Financial Times/ Prentice Hall, tweede druk, 2000, ISBN 90-430-0289-5
- Overbeek P, W. Sipman, *Informatiebeveiliging*, tweede druk, Tutein Nolthenius, 1999, ISBN 90-72194-57-8
- Cazemier, J.A., P.L. Overbeek, L. Peters, *Security Management – IT Infrastructure Library*, CCTA, 1999, ISBN 0-11-330014-X