



Modellen, Raamwerken en Methode's

'In Control' of 'Under Control'?

De *auditor* in het informatiebeveiligingsbos.

Leon Kuunders (lkuunders@trusted-id.nl)

Modellen, Raamwerken en Methode's



- Definities
- Modellen
- Raamwerken
- Methode's
- Controle / Conclusie
- Overzicht

A close-up, slightly blurred photograph of a person's hand holding a pen and writing on a document. The document is held in a binder with visible rings. The image is semi-transparent, allowing the text to be clearly visible. The background is a light, neutral color.

This page intentionally left blank.

Modellen, Raamwerken en Methode's

Model:

- ✓ Een abstract, conceptueel denkbeeld dat processen, variabelen en relaties verbeeld zonder specifieke richtlijnen voor implementatie.

Abstract: "niet door aanschouwing verkregen maar door redenering afgeleid"

Conceptueel: als in concept, ontwerp

Modellen, Raamwerken en Methode's

Raamwerk (Framework):

- ✓ Een elementair denkbeeld dat aannames, concepten, waardes en richtlijnen vastlegt, en daarbij instructies geeft voor de implementatie.

Modellen, Raamwerken en Methode's

Methode:

- ✓ Een doelgericht denkbeeld dat specifieke richtlijnen, procedure's en regels vastlegt voor implementatie van een taak of functie.

Modellen, Raamwerken en Methode's

Standaard:

- ✓ Een specificatie opgesteld middels een open, geformaliseerd ontwikkeltraject, waarbij de inbreng is beoordeelt en na stemming is opgenomen.

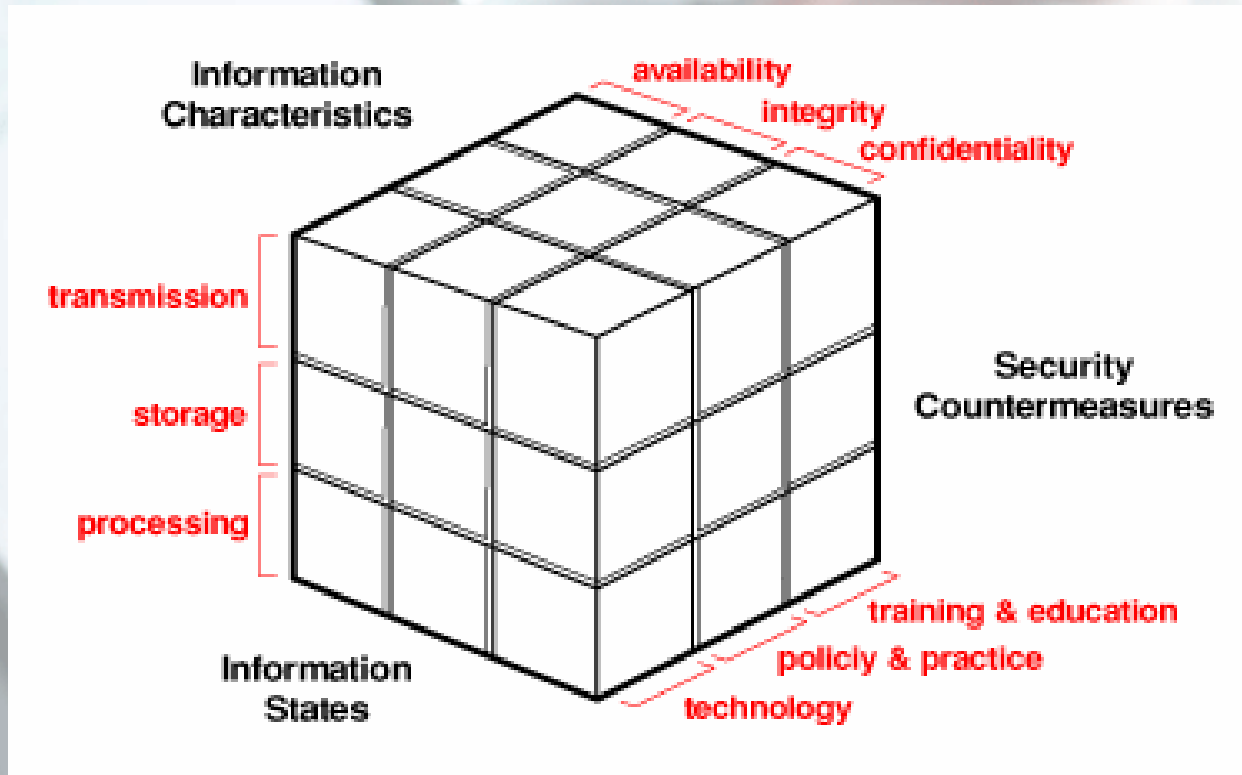
Modellen, Raamwerken en Methode's

M1: The McCumber Cube (1991)

- Information Systems Security: Comprehensive Model
 - focus op 'Information States', 'Critical Information Characteristics' en 'Security Measures'
 - http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf
 - abstract
 - geen richtlijnen

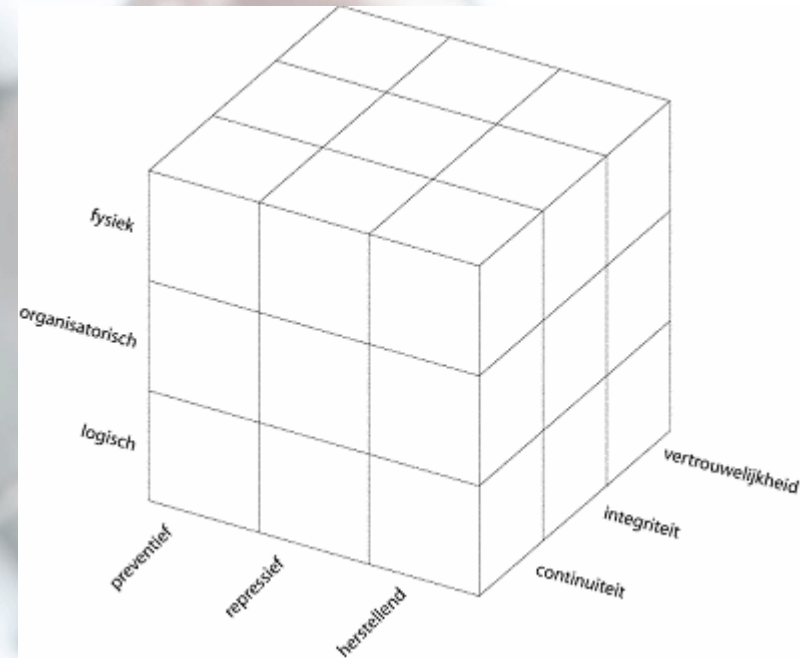
Modellen, Raamwerken en Methode's

The McCumber Cube



Modellen, Raamwerken en Methode's

De McCumber Cube gebruikt door RCC (nu PinkRocade).



“Een zijde ingevuld door vertrouwelijkheid, integriteit en continuïteit. De andere zijde ingevuld door maatregelen die je kunt treffen: fysieke, organisatorische en logische, c.q. programmeerbare maatregelen. En kenmerken van die maatregelen kunnen dan zijn dat ze preventief zijn, repressief of herstellend. Dan heb je $3 \times 3 \times 3 = 27$ minikubusjes. En elk van die kubusjes bevat vervolgens een pakket maatregelen waarmee een bepaald facet van de informatiebeveiliging wordt aangepakt.” (uit interview met Albert Brouwer, CvIB.nl)

Modellen, Raamwerken en Methode's

Wat zijn Raamwerken

- Engels "Framework"
- Nederlands b.v. "Schema's"

Richtlijnen voor maatregelen, zonder op een specifieke taak te richten.

(Een elementair denkbeeld dat aannames, concepten, waardes en richtlijnen vastlegt, en daarbij instructies geeft voor de implementatie.)

Modellen, Raamwerken en Methode's

S1: Cobit “Control Objectives for Information and related Technology”

- <http://www.isaca.org/cobit/>
- Geeft een aanpak voor het ontwerpen, implementeren en testen van “IT controls”.
- Bevat kritische succesfactoren, sleutelindicatoren en prestatieindicatoren.
- Geeft richtlijnen voor het uitvoeren van een audit.
- Bevat vier “domeinen”: Planning & Organisatie, Acquisitie en Implementatie, Oplevering & Ondersteuning en Monitoring.

Modellen, Raamwerken en Methode's

S1: Cobit “Control Objectives for Information and related Technology”

- Verbeterd de controle op IT middelen.
- Geen Informatiebeveiliging Framework.
- Bevat 1 verwijzing naar informatiebeveiliging uit de 34 richtlijnen.

Informatiebeveiliging is holistisch van aard.

Cobit is exclusief IT gericht.

Modellen, Raamwerken en Methode's

S2: Common Criteria for Information Technology Security Evaluation

- ISO/IEC 15408, CC
- <http://www.commoncriteriaportal.org/>
- Maakt beschrijven van beveiligingsprincipes in software en hardware mogelijk.
- Wordt gebruikt door fabrikanten om de beveiligingsvoorwaarden van producten te beschrijven.
- Kern “Evaluated Assurance Levels” (gebaseerd op business processen) en “Protection Profile” (de beveiligingsvoorwaarden).

Modellen, Raamwerken en Methode's

S3: COSO Enterprise Risk Management – Integrated Framework (1987)

- The Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management – Integrated Framework.
- <http://www.coso.org/>
- Geeft een integrale aanpak voor de organisatiebrede implementatie van risico-management.
- Categoriën: Strategie, Operationeel, Rapportage, Naleving.
- Top-down aanpak (consistent met Sox).
- Gaat uitgebreid in op het identificeren en beheersen van bedrijfsrisico's.

Modellen, Raamwerken en Methode's

S3: COSO Enterprise Risk Management – Integrated Framework (1987)

- In lijn met ISO/IEC 17799.
- Bevat geen richtlijnen voor het bepalen en verminderen van risico's.
- Geeft hulp voor het bepalen en integreren van complementaire methode's.

Modellen, Raamwerken en Methode's

S4: Information Security Management Maturity Model

- Geeft richtlijnen voor het verbeteren van een Information Security Management Systems (ISMS).
- <http://www.isecom.org/projects/ism3.shtml>
- Gebruikt het Capability Maturity Model.
- Doel is het voorkomen en verminderen van (beveiligings)incidenten.
- Vier uitgangspunten: Documentatie (generiek), Strategisch Management, Tactisch Management en Operationeel Management.

Modellen, Raamwerken en Methode's

S4: Information Security Management Maturity Model

- Leent veel uit andere schema's of raamwerken zoals ISO/IEC 17799.
- Geeft geen richtlijnen voor de implementatie van een ISMS.
- Kan worden ingezet voor het testen van de effectiviteit van een geïmplementeerd ISMS.

Modellen, Raamwerken en Methode's

S5: INFOSEC Assurance Capability Maturity Model (IA-CMM)

- <http://www.iatrp.com/iacmm.cfm>
- Geeft handreikingen voor het selecteren en implementeren van verbeteringsstrategiën van het informatiebeveiligingsniveau.
- Maakt gebruik van definities uit SSE-CMM (Security Software Engineering – Capability Maturity Model, ISO/IEC 21827).
- Controle gebieden: 'Provide Training', 'Coordinate with Customer Organization', 'Specify Initial INFOSEC Needs', 'Assess Threat', 'Assess Vulnerability', 'Assess Impact', 'Assess INFOSEC Risk', 'Provide Analysis and Results'

Modellen, Raamwerken en Methode's

S6: ISF Standard of Good Practice

- The Information Security Forum Standard of Good Practice
- <http://www.isfsecuritystandard.com/>
- Benadert informatiebeveiliging vanuit een zakelijk perspectief.
- Focust op de afspraken die nodig zijn om zakelijke risico's die aan kritische informatiesystemen zijn gekoppeld te beheersen.
- Vijf aspecten: Beveiligingsmanagement (bedrijfsbreed), Kritische 'Business' Applicaties, Computer Installaties, Netwerk en Systeem Ontwikkeling.

Modellen, Raamwerken en Methode's

S6: ISF Standard of Good Practice

- Geeft per onderzocht aspect de algemeen toepasbare 'best practices' voor informatiebeveiliging.
- Is gedetailleerd van opzet.
- Kan goed gebruikt worden in combinatie met ISO/IEC 17799 of COSO.

Modellen, Raamwerken en Methode's

S7: ISO 17799 / ISO 27001

- ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management.
- <http://www.iso.org/>
- 17799: richtlijnen voor het ontwikkelen van beveiligingsstandaarden en beveiligingsmanagement bij een organisatie.
- 27001: eisen voor het opzetten, implementeren, gebruiken, controleren, herzien, onderhouden en verbeteren van een gedocumenteerd ISMS binnen de context van de zakelijke risico's.

Modellen, Raamwerken en Methode's

S7: ISO 17799 / ISO 27001

- 17799 geeft richtlijnen voor de invoer van informatiebeveiligingsmaatregelen.
- 27001 geeft richtlijnen voor het managen van informatiebeveiliging en het controleren van het niveau.
- Start bij de business en het identificeren en analyseren van risico's.
- Is gericht op het verminderen van die (zakelijke) risico's.
- Lijkt op COSO wat betreft aanpak.
- Is flexibeler in de implementatie van het ISMS dan COSO.

Modellen, *Raamwerken* en Methode's

S7a: ISO 17799 / ISO 27001 in de zorg: NEN 7510

- Nieuwe norm toegespitst op de zorg vastgesteld door NEN Normcommissie 303001.
- Gebaseerd op de “Code voor Informatiebeveiliging”, de nederlandstalige ISO 17799.
- Uitgebreid met eisen uit ENV 12924 (Medical informatics - Security categorisation and protection for healthcare information systems).
- Toetsbare varianten voor drie organisatievormen: NEN 7511-1 (complexe organisaties), NEN 7511-2 (groepspraktijken), NEN 7511-3 (zelfstandigen).

Modellen, *Raamwerken* en Methode's

NEN 7510 - hoofdstukken

1. Onderwerp en toepassingsgebied
2. Normatieve verwijzingen
3. Termen en definities
4. Structuur van de norm
5. Beveiligingsbeleid
6. Organiseren van informatiebeveiliging
7. Beheer van middelen voor de informatievoorziening
8. Beveiligingseisen t.a.v. personeel
9. Fysieke beveiliging en beveiliging van de omgeving
10. Operationeel beheer van informatie en comm. voorzieningen
11. Toegangsbeveiliging
12. Aanschaf, ontwikkeling en onderhoud van informatiesystemen
13. Continuïteitsbeheer
14. Naleving
15. Beveiligingsincidenten

Modellen, Raamwerken en Methode's

S8: ITIL / BS 15000

- ITIL: Information Technology Infrastructure Library
- BS 15000: Information Technology Service Management Standard
- <http://www.iti1.co.uk/>
- <http://www.bs15000.org.uk/>
- ITIL is een standaard die helpt bij het opzetten van IT Service Management (ITSM) raamwerk.
- BS15000 geeft in deel 1 instructies voor het opzetten van een ITSM en in deel 2 instructies voor certificering van dat systeem.
- Niet specifiek gericht op informatiebeveiliging.

Modellen, Raamwerken en Methode's

S9: New Basel Capital Accord (BASEL-II)

- International Convergence of Capital Measurement and Capital Standards: A Revised Framework
- <http://www.bis.org/>
- Gericht op internationale organisaties uit de banksector.
- Doel is veiligstellen van de integriteit van kapitaal (geldstromen).
- Niet specifiek gericht op informatiebeveiliging.

Modellen, Raamwerken en Methode's

S10: NIST SP 800-14 (1996)

- National Institute of Standards and Technology, Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- <http://www.nist.gov/>
- Geeft een basis voor het vaststellen en herzien van het IT beveiliging programma.
- Oud, maar concepten en generieke richtlijnen zijn nog steeds geldig.
- Gebruikt bij opstellen van BS 7799.
- Vervangen door ISO 17799.

Modellen, Raamwerken en Methode's

S11: Systems Security Engineering Capability Maturity Model (SSE-CMM)

- <http://www.sse-cmm.org/>
- Geeft de eisen voor het implementeren en verbeteren van beveiligingsfuncties in een systeem, of serie van systemen, uit het "Information Technology Security (ITS) domain".
- Bekijkt gebreken of incidenten en onderzoekt welk proces op welke wijze daarvoor verantwoordelijk is, met als doel dat proces aan te passen.
- Verwacht voorspelbaarheid in processen en gedefinieerde controlepunten rondom processen.
- Gericht op de technische bedrijfstak (bouw, ontwikkeling).

Modellen, Raamwerken en Methode's

Een doelgericht denkbeeld dat specifieke richtlijnen, procedure's en regels vastlegt voor implementatie van een taak of functie.

Modellen, Raamwerken en Methode's

E1: INFOSEC Assessment Methodology (IAM)

- <http://www.iatrp.com/iam.cfm>
- Levert een gestandaardiseerde aanpak voor de analyse van de stand van zaken op het gebied van informatiebeveiliging voor geautomatiseerde informatiesystemen.
- Onderdeel van het IA-CMM schema.
- Geeft een beoordeling op hoog niveau van specifiek systeem zodat potentiële kwetsbaarheden (en dus risico's) kunnen worden geïdentificeerd.
- Onderverdeeld in drie fases: pre-assessment (voor-beoordeling), on-site activities, post-assessment (na-beoordeling).
- Niet technisch van opzet.
- Lijkt op een SAS 70 Type II beoordeling.

Modellen, Raamwerken en Methode's

E2: INFOSEC Evaluation Methodology (IEM)

- <http://www.iatrp.com/iem.cfm>
- Methode voor het technisch vaststellen van kwetsbaarheden in systemen en het bevestigen van de actuele stand der zaken van die systemen.
- Onderdeel van het IA-CMM schema.
- Controleert de systemen “hands-on”.
- Drie fases: pre-evaluatie, on-site, post-evaluatie.
- Gebruikt als input de rapporten opgeleverd bij de IAM fases.

Modellen, Raamwerken en Methode's

E3: ISACA Standards for IS Auditing

- Information Systems Audit and Control Association Standards for Information Systems Auditing
- <http://www.isaca.org/>
- Geeft een gedetailleerde methode voor de uitvoering van audits van informatie systemen.
- Beïnvloedt COBIT (ook van ISAS).
- Wordt continue bijgewerkt zodat nieuws regelgeving direct met audits wordt meegenomen.

Modellen, Raamwerken en Methode's

E4: OCTAVESM

- Operationally Critical Threat, Asset, and Vulnerability EvaluationSM
- <http://www.cert.org/octave/>
- Geeft een methode die specifiek focust op het onderzoek naar operationeel risico, beveiligingsmaatregelen technologie.
- Drie fases: “Build Asset-Based Threat Profiles”, “Identify Infrastructure Vulnerabilities”, “Develop Security Strategy and Plans”.
- Levert onderzoek naar risico's op strategische en praktijk gerichte uitgangspunten.
- Gericht op “zelf doen”: een team van eigen analisten wordt getraind en ondersteund door een (externe) specialist.

Modellen, Raamwerken en Methode's

E5: OSSTMM

- Open Source Security Testing Methodology Manual
- <http://www.isecom.org/osstmm/>
- Geeft regels en richtlijnen voor het testen van software.
- Geeft aan hoe en wanneer “events” getest worden.
- Testen gebeurt vanuit een “ongemachtigde” omgeving.
- Gebruikt richtlijnen uit ITIL, ISO 17799, NIST, MITRE.

Modellen, Raamwerken en Methode's

E6: Security Incident Policy Enforcement System

- <http://www.isecom.org/projects/sipes.shtml>
- Geeft een methode voor het opstellen en implementeren van een SIPES.
- Behandelt reacties op incidenten.
- Verouderd, niet compleet.

Modellen, Raamwerken en Methode's

E7: SAS 70

- Statement on Auditing Standards Number 70
- <http://www.sas70.com/>
- Is een samenvatting van “Statements of Auditing Standards from the American Institute of Certified Public Accountants (AICPA)”.
- Was de de facto standaard voor audits voordat in 2002 de Sarbanes-Oxley Act werd aangenomen en de “grote 4” besloten daarvoor COBIT te volgen.
- Twee fases: één richt zich op een documentonderzoek, twee controleert of systemen gehoorzamen aan de gedocumenteerde controles.

Controle, Controle, Conclusie

- Geen enkele methode voldoet aan alle eisen.
- Wetgeving/afspraken schrijven in de regel voor dat men “*common sense*” gebruikt bij het bewaken, openbaren en bewerken van informatie.
- De Payment Card Industry Data Security Standards (PCI DSS) is hiervan een goed voorbeeld.

Controle, Controle, Wetgeving

Sarbanes-Oxley

- http://www.sox-online.com/sarbanes-oxley_news.html
- Tegengaan van illegale boekhoud praktijken.
- Schrijft de implementatie van interne controles voor.
- Schrijft jaarlijkse “controle op de controles” voor.
- Maakt bestuurders persoonlijk verantwoordelijk.
- Voor certificatie dient het COSO raamwerk gevolgd te worden.

Controle, Controle, Wetgeving

Sarbanes-Oxley

- Information Security
 - Policies, Procedures, Standards
 - Risk Assessment
 - Authentication Controls
 - Authorization Controls (including Administrator/Super User level)
 - User Access Administration (Granting, Terminating and Employee Transfers, Contractors)
 - Security Logging and Monitoring Controls
 - Other Technical Configurations
 - Physical Security

Controle, Controle, Wetgeving

Sarbanes-Oxley

- Systems Development and Change Management Controls
 - Request/Approvals
 - Prioritizations
 - Development Standards
 - SDLC
 - Testing, QA, Migration
 - Documentation Maintenance

Controle, Controle, Conclusie

The information security management program should implement commonsense security measures to protect data and systems. These measures should include maintaining information security policies (reiterated), building a secure network, protecting stored and transmitted data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks and systems, and maintaining a business continuity and disaster recovery program that plans for backup, recovery, and contingency planning.

The entire program should be assessed on a regular basis.

'In Control'? Waarmee?

- Cobit is te “eng” in de definitie en kan daardoor niet aan alle wettelijke eisen voldoen.
- COSO ERM kan worden gebruikt maar dient te worden aangevuld met COBIT, OCTAVE, IA-CMM, IAM, IEM, ITIL, of zelfs ISO/IEC 17799.

'In Control'? Waarmee?

- ISO/IEC 17799 is het enige raamwerk dat voldoende flexibel is om 'in control' te zijn.
- Kan eenvoudig worden uitgebreid of ingeperkt.
- Sluit goed aan op andere raamwerken en methode's.

Overzicht presentatie

Modellen	Schema's (Raamwerken)	Methode's
McCumber Cube	Cobit	IAM
	Common Criteria	IEM
	COSO ERM	ISACA IS Auditing Standards
	ISM3	OCTAVA
	IA-CMM	OSSTMM
	ISF Standard	SIPES
	ISO 17799/27001	SAS 70
	ITIL/BS 15000	
	BASEL-II	
	NIST SP 800-14	
	SSE-CMM	