VUro RE

vrije Universiteit amsterdam

NOREA
de beroepsorganisatie van IT-auditors

Van principes naar normenkaders

Jan Dros Belastingdienst/Amsterdam

Gerrit Wesselink UWV

Inhoud

- Inleiding
- Beschrijving scriptiecontext
- Onderkende principes
- RBAC
- Levenscyclus van systemen
- Conclusies en aanbevelingen

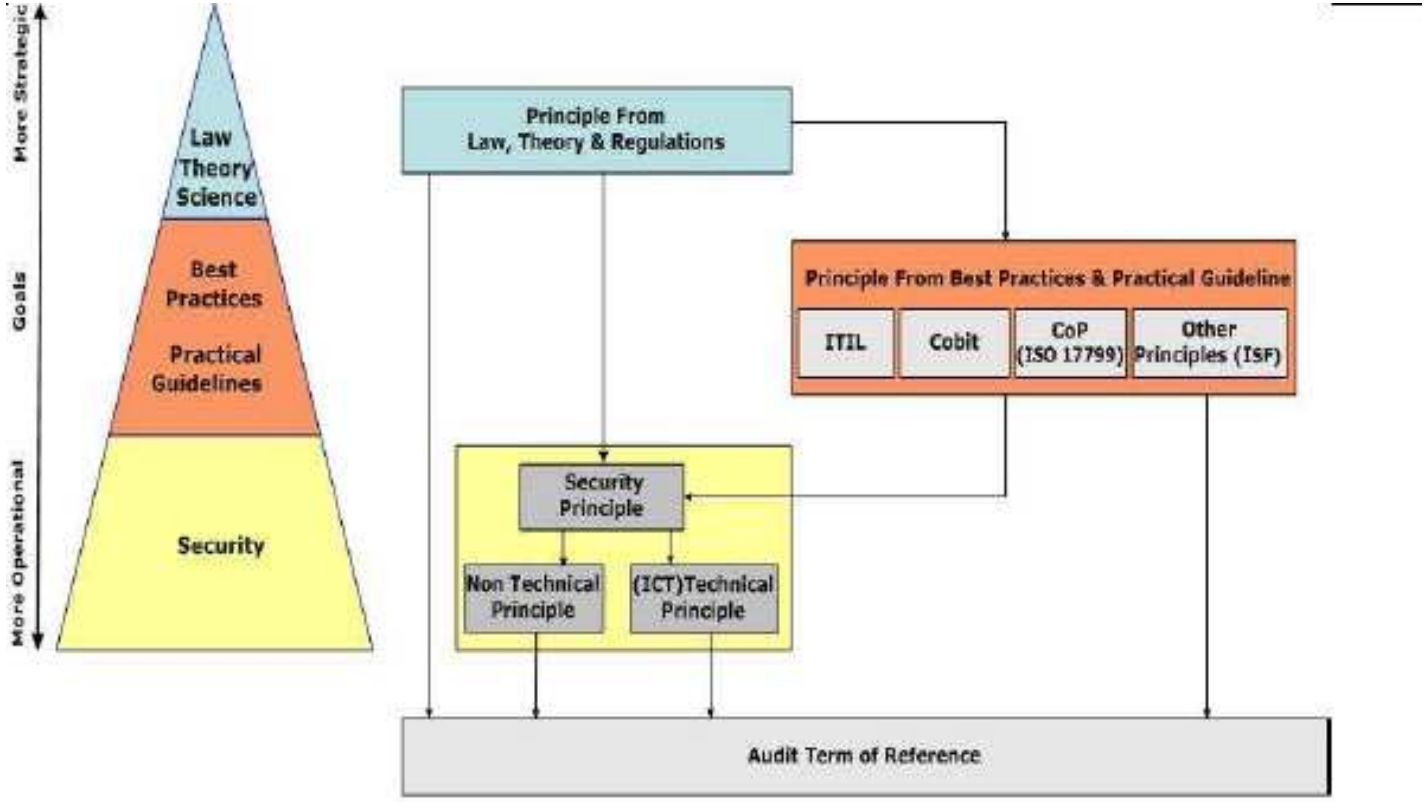
Inleiding

- Scriptie
- Aanpak
- Waarom scriptie m.b.t. normenkaders
- Principle based

Context van het onderzoek (1)

De scriptie van “Principes naar normenkaders” is uitgevoerd in de context van het promotieonderzoek “effectiviteit en efficiëncy van IT-audits”, door Drs.ing. Wiekram Tewarie RE.

Context van het onderzoek



Gehanteerde kenmerken principe

- Beïnvloed de ondernemingsstrategie, en drijfveer voor gedrag en organisatie;
- Eenvoudig overdraagbaar;
- Robuust;
- Herkend en gedragen door management.

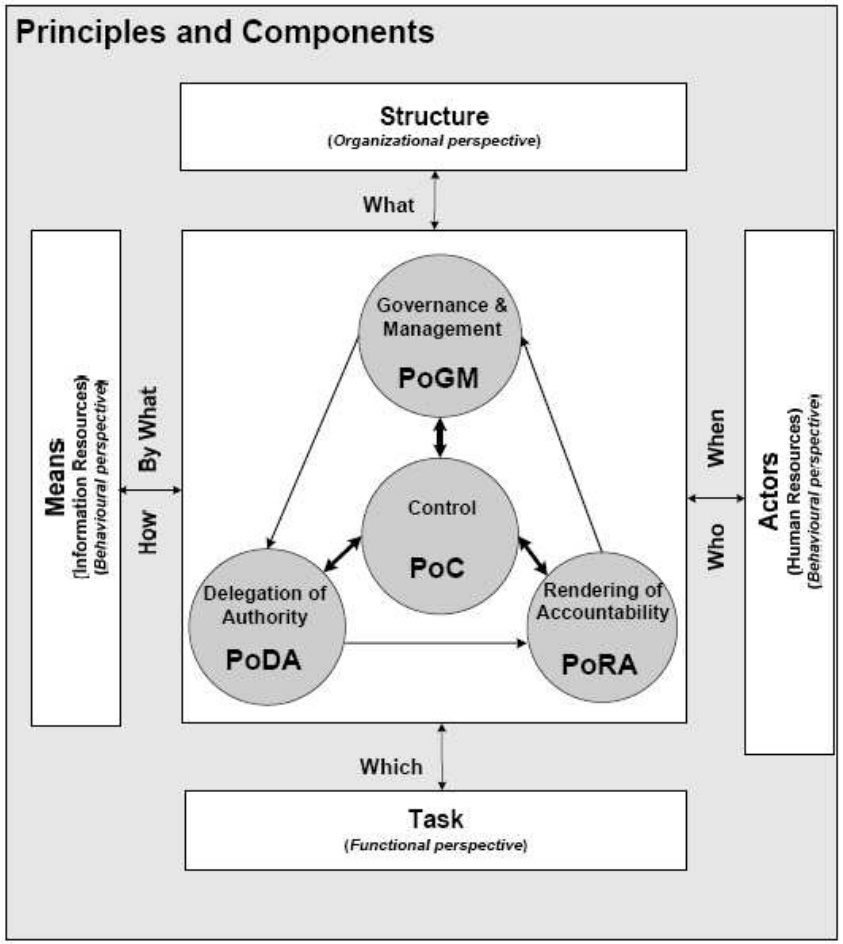
Onderzoeksvraag

Beredeneer welke principes ten grondslag liggen aan de “Best Practices en Practical Guidelines”. Volgens welke principes hebben de originele auteurs deze documenten opgesteld.

Onderzoeksvraag / verdieping

Zoek in de “Best Practices en Practical Guidelines” naar gemeenschappelijke kenmerken aan de hand waarvan principes opgesteld kunnen worden.

GDAC Model


Principles and Components
Structure
(Organizational perspective)
What
Means
(Information Resources)
(Behavioural perspective)
By What
How
Governance & Management
PoGM
Control
PoC
Delegation of Authority
PoDA
Rendering of Accountability
PoRA
When
Who
Actors
(Human Resources)
(Behavioural perspective)
Which
Task
(Functional perspective)

Gekoppeld aan Starreveld

- PoGM, Governance en Management, besturen in enge zin;
- PoDA, Delegation of authority, het doen functioneren van een organisatie;
- PoRA, Rendering Accountability, het afleggen van verantwoording;
- PoC, Control, het (doen) beheersen

Bestudeerde documenten

- Cobit 4.0 (ITGI);
- Standard of Good Practice 4.1 (ISF);
- Code of Practice (ISO/IEC17799:2005)

Rule based qua opzet, zeer uitgebreid.

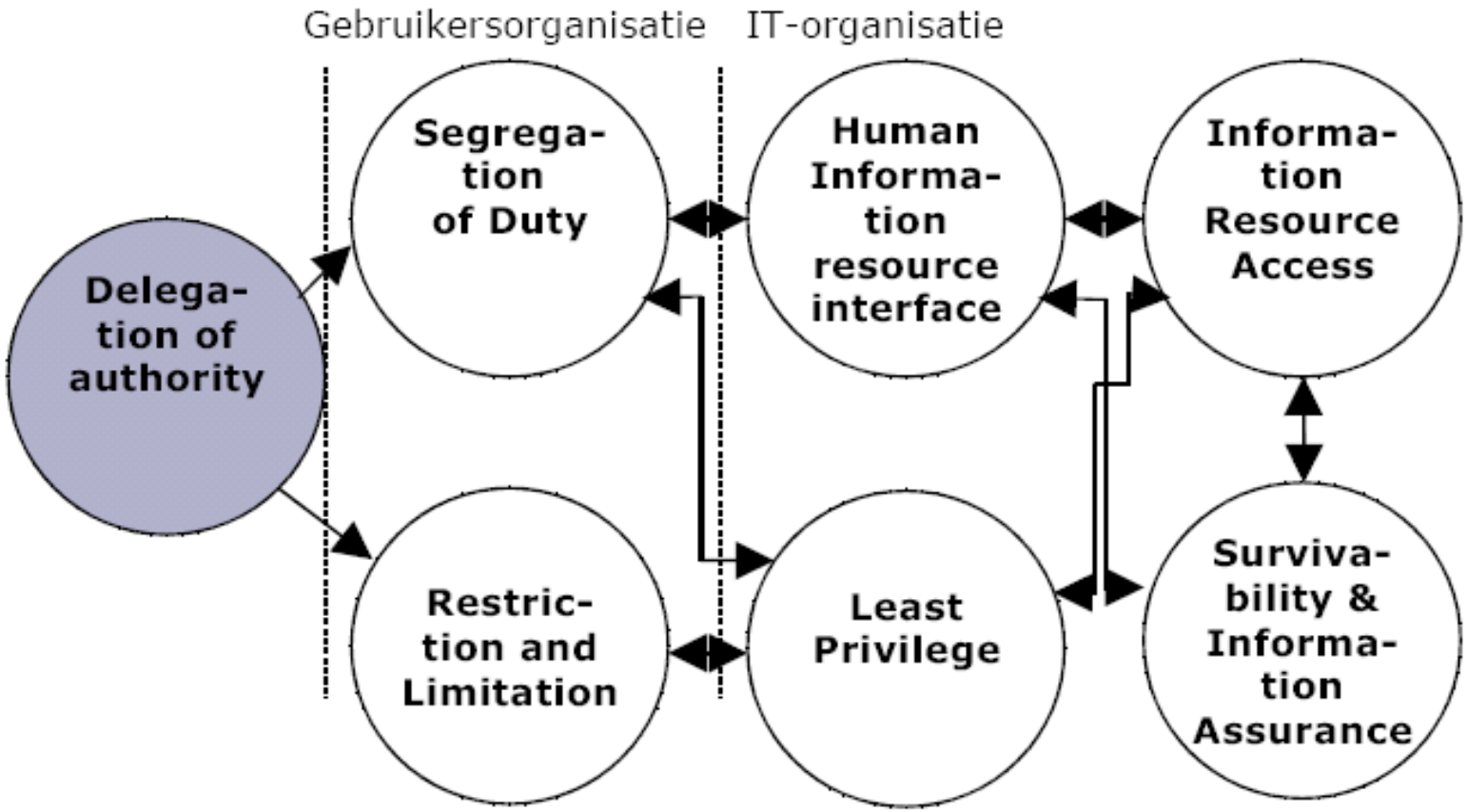
Onderkende principes

- 10 principes, waarvan 2 getoetst
- Principe van functiescheiding
  Getoetst met behulp van een normenkader van PI
- Principe van Levenscyclus van systemen
  Getoetst aan een praktijksituatie

Uitwerking functiescheiding (matrix)

	Leiding	**Delegatie**	**Control**	**Accounta-bility**
Wat is de Structuur (S)	•Beleid •Strategie •Delegatie	•Functiescheiding	•Functiescheiding •Beleid •Strategie •Delegatie	•Verantwoordings-rapportage •Controlerapportage
Wat zijn de taken (T)	•Taken •Functies	•Delegatie	<u>Vastlegging</u> •Controle •Restricties en limieten •Normen	•Vastlegging tbv verantwoording •Toegekende restricties •Uitgevoerde taken
Wie zijn de actoren (A)	•Leiding en besluitvor-mers per level	•Uitvoerenden	•IC-actoren	•Verantwoordelijken tbv rapportage
Wat zijn de Middelen (M)	•Informatie producten (beleid) •Technische middelen	•Taken en rollen binnen gebruikersorganisatie en IT organisatie	•Voorschriften •Beleid •Normen	•(niet) geautomati-seerde vastleggingen

Uitwerking functiescheiding (raakvlakken)



Functiescheiding

- Model getoetst aan PI-studie Role Based Access control (RBAC)
- Deze modelmatige benadering stemt in hoofdlijnen overeen met de stappen die PI onderscheidt.
- Conclusie m.b.t. functiescheiding: model is toepasbaar.

Levenscyclus van systemen (matrix)

	Leiding	**Delegatie**	**Control**	**Accounta-bility**
Wat is de Structuur (S)	•Beleid •Strategie •Delegatie •Standaar-den •Bijsturing	•Functiescheiding •Taakomschrijving	•Functiescheiding •Beleid •Strategie •Delegatie	•Contracten •Registratie voorschriften •Rapportage eisen
Wat zijn de taken (T)	•Taken •Functies	•Taken •Procedures	Vastlegging Realisatie Beoordeling	•Vastlegging
Wie zijn de actoren (A)	•Leiding en besluitvor-mers per level	•Uitvoerenden	•IC-actoren	•Verantwoordelijken tbv rapportage
Wat zijn de Middelen (M)	•Methoden •Informatie	•Ontwikkeltools •Software •Middleware •Hardware •Netwerkcomponenten	•Rapportages •Contracten •Verslagen	•Registraties

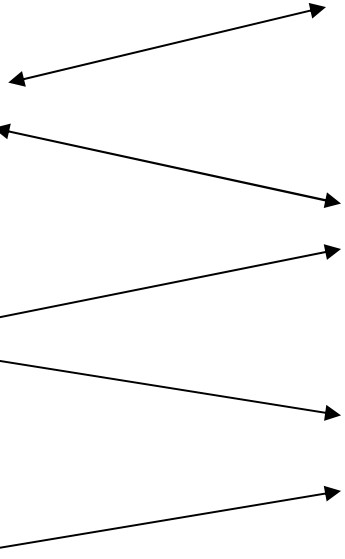
Uitwerking levenscyclus (raakvlakken)

IT Organisatie

- Ontwikkelen
- Onderhoud
- Beëindigen

Gebruikersorganisatie

- Initiatie
- Specificatie
- Gebruik



Levenscyclus van systemen (beëindigen gebruik)

- Getoetst aan praktijksituatie UWV
- Andere structuurbenadering, kostte veel tijd om hier een match te krijgen
- Conclusie: model bruikbaar om normenkader volledig te krijgen

Conclusies scriptie (1)

- Principle based werken bevordert volledige normenkaders en daarmee volledige danwel volkomen onderzoeken

- Principle based werken maakt raakvlakken met ondernemingsdoelstellingen scherper zichtbaar. Toegevoegde waarde van IT-audit is éénvoudiger aan te tonen

Conclusies en aanbevelingen (2)

- De gehanteerde modellen dienen verder uitgewerkt te worden:
  - Er dient een “schakelmechanisme” te komen, een structuur aan de hand waarvan principes geselecteerd worden