Principle based Audit Approach
(Audit Term of Reference)

Wiekram Tewarie

Agenda

Deel I

- Aard IT audit (onderzoeken)
- Probleem, Praktijk en gevolg

Deel II

- Onderzoeksmodel
- Beeld van voorlopige oplossingsrichting *(Model vorming)*
- Epiloog

Aard IT Audits (onderzoeken)

- **Jaarrekening controle**
  - *Reikwijdte*: Vaste onderdelen (UC, AC, GC), eventueel aangevuld met additionele en gerichte onderdelen (financiële datamigratie)
  - *Doel:* Afgeven van “redelijke mate van zekerheid” omtrent de financiële verantwoording
- **IT assurance onderzoeken i.o.v. belanghebbenden** (ministerie en Raad van Bestuur)
  - *Reikwijdte*: behelst het totale IT gebied,
  - Verschillende vormen van IT management (geheel of gedeeltelijk uitbesteed)
  - *Doel*: Afgeven van “redelijke mate van zekerheid” omtrent het managen van IT (al dan niet uitbesteed)
- **Ad hoc: Bijzondere onderzoeken**
  - IT-fraude
  - Beveiligingsonderzoeken
  - Beschikbaarheidsonderzoeken

Probleem, Praktijk en Gevolg

- **Probleem**
  - Geen standaardmethoden of raamwerken voor het opstellen van referentiekaders. (*Paans, Moonen, Lindgreen)*
  - Niet gebaseerd op formele structuren en subjectief
- **Gebruikelijk beoordelingsinstrument**
  - Referentiekader (RFK)
  - Beschikbaar: Best Practices (COBIT), ISO Standaarden (o.a. ISO 17799, ISO 20000), Overige (NIST, StGP, PI)
- **Gangbare methode voor het opstellen van RFK**
  - Selectie uit best practices (lijstje van normen)
  - Set normen opgezet op basis van een “organisatie-specifieke / individu specifieke” aanpak
- **Gevolg**
  - RFK afhankelijk van kennis en kunde van IT Auditors waardoor geen “harde” zekerheid is omtrent de volledigheid
  - Wisselende variaties in indeling van RFK met name aangaande het onderscheid tussen de hoofdnormen en de sub-normen
  - Meningverschillen met leveranciers en belanghebbenden over het RFK
  - Risico’s van onnodige inspanning voor het opstellen van RFK’s

Onderzoek

- **Ontwikkel een formele methode voor het opstellen van referentiekaders**

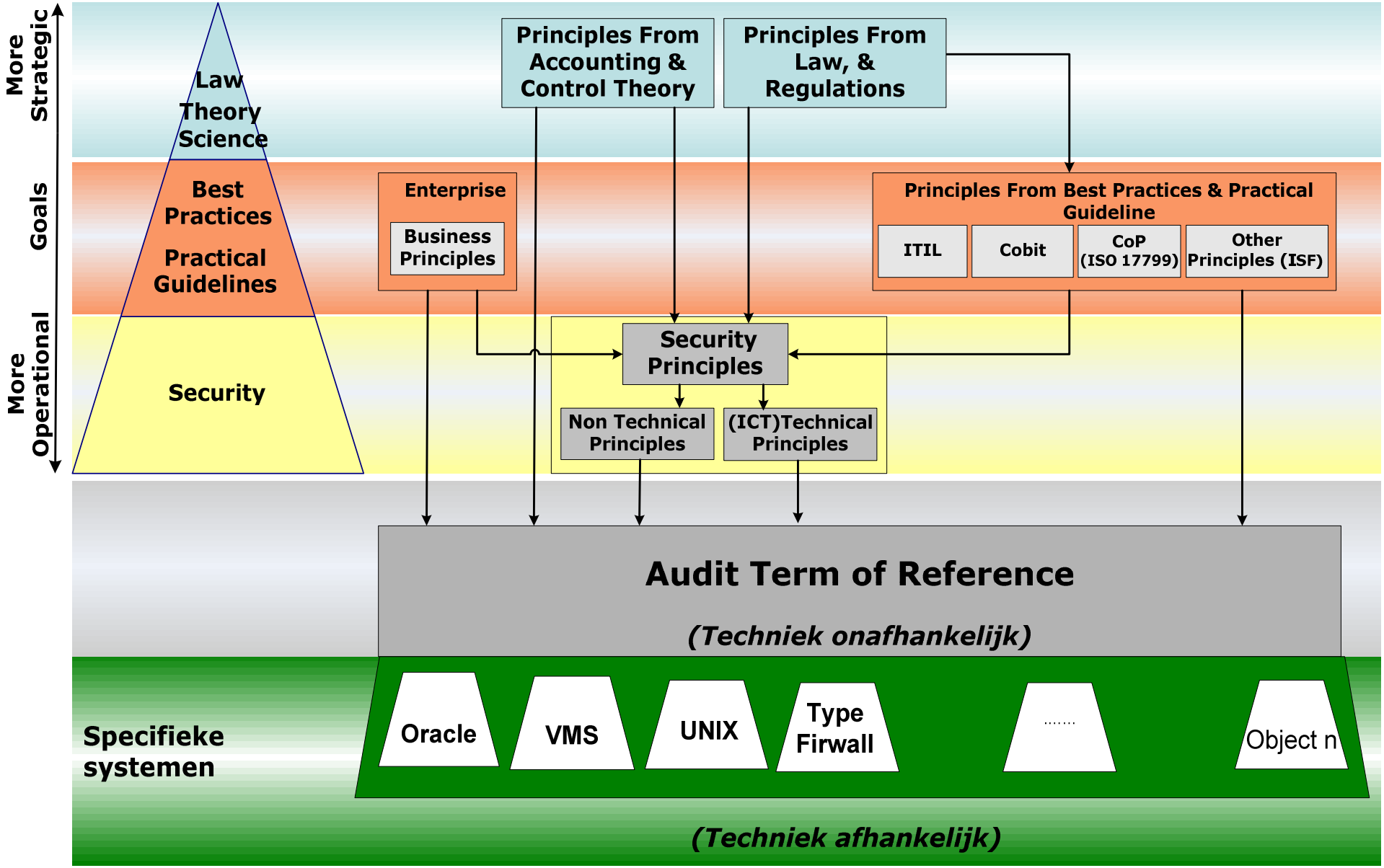
- **Doel van de methode:**

  Theoretisch onderbouwd model te ontwikkelen waarmee op effectieve en efficiënte wijze samenhangende referentiekaders kunnen worden ontwikkeld

Oplossingsrichting

- ***Principle based***
  - **Principles : "*fundamental truth*",**
  - **Hoger abstractie niveau, algemeen onderkend en is naast grondslag voor RFK 's een communicatie-instrument met stakeholders,**
  - **Door koppelingen van audit onderwerpen aan principes kunnen audits meer in Business-IT context worden uitgevoerd,**

Onderzoeksmodel



Voor– en nadelen
Principle-only en Rules-based (1)

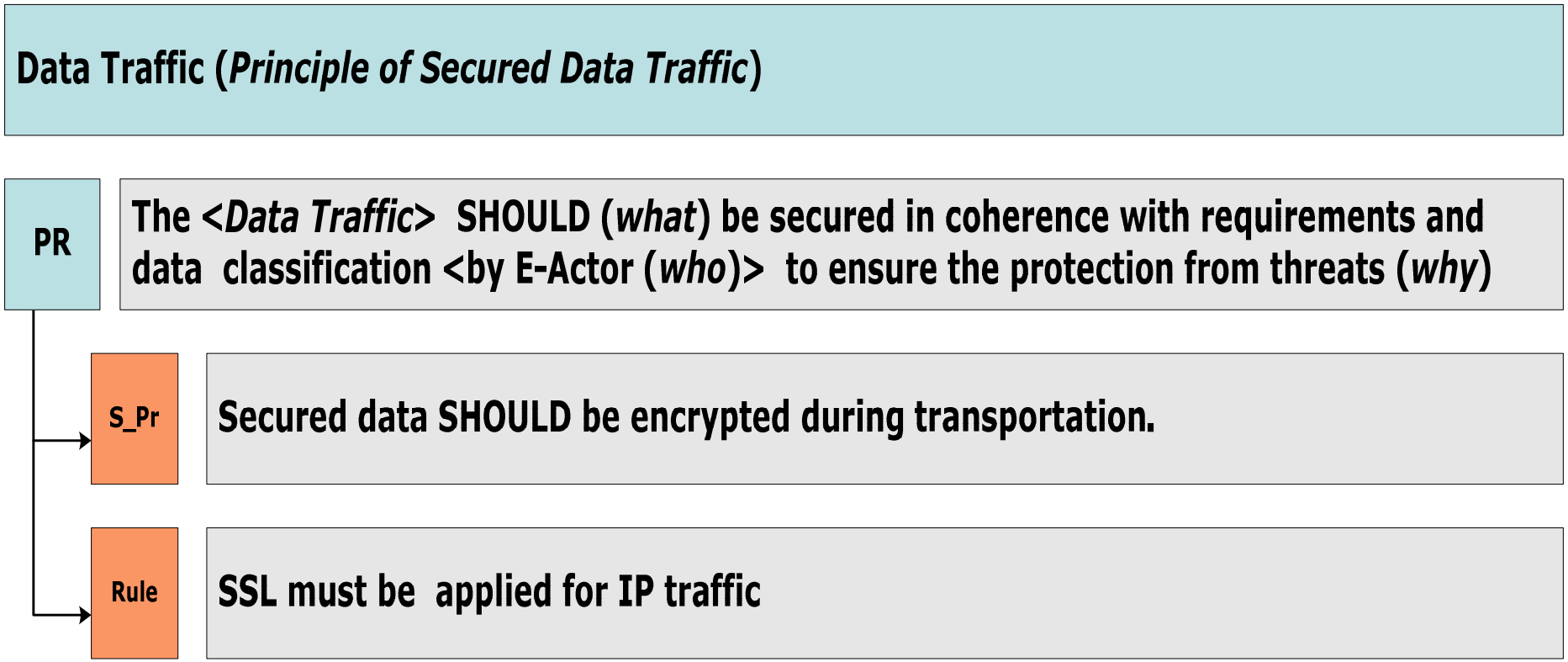
- **Voordelen *Principle based***
  - **Beschikbaar hebben van algemeen onderkende en aanvaarde uitgangspunten (concepten) voor gebruikers *(auditors, security deskundigen, architecten, ontwerpers en bouwers)***
  - **Verschaft aan Stakeholders een duidelijker inzicht van het te hanteren meetinstrument en de wijze waarop het resultaat geïnterpreteerd moet worden (*SEC*)**
  - **Bevordert hergebruik en herhaalbaarheid**
  - **Vergroot de consistentie tussen oordelen**
  - **Biedt ervaren auditors een structuur aan om de detail informatie te koppelen aan formeel overeengekomen concepten zodat overdracht van kennis beter verloopt**

- **Voordeel *Rules-based***
  - **Concreet**

Voor– en nadelen
Principle only en Rules-based (2)

- **Nadeel *Principle-based***
  - ***Principle only* levert moeilijkheden op t.a.v. afdwingbaarheid vanwege de abstractheid**
- **Nadeel *Rules-based***
  - ***Rules-based* standaards leiden vaak de aandacht af van de werkelijke problemen en is onderhoudsintensief**

Specifiek Voorbeeld

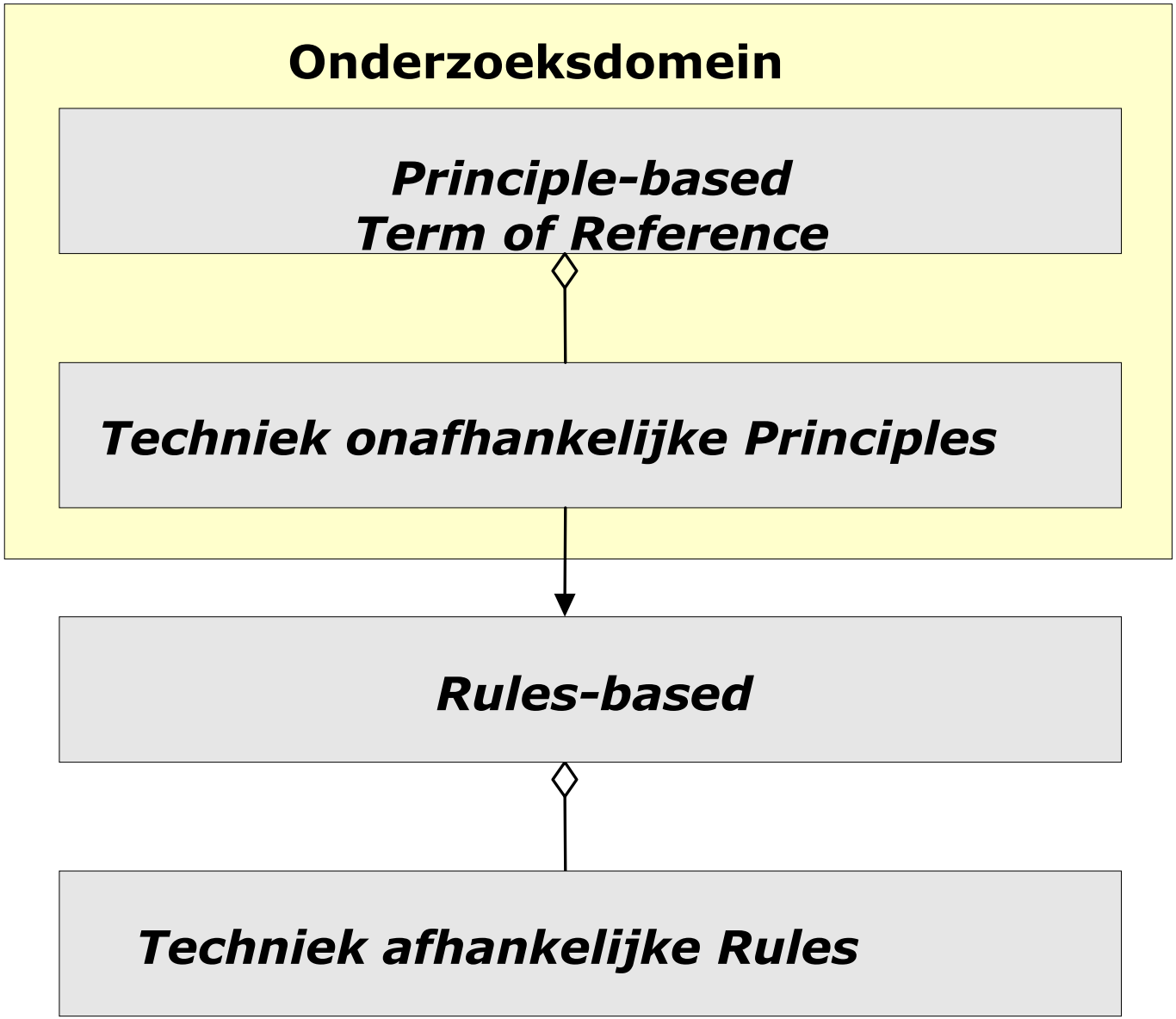


Security Exhange Commision (SEC)

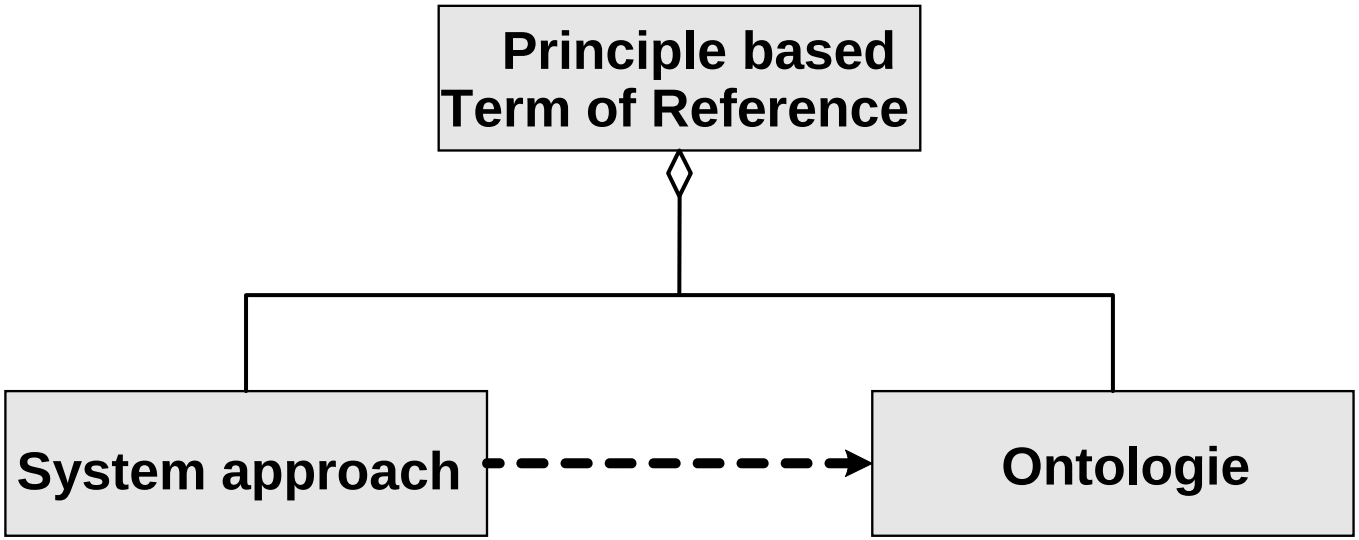
- **Standaards *should be* developed on *Principle based* or *Objectives-oriented* basis**

- ***Karakteristieken van een standaard zijn:***
  - **Gebaseerd op een conceptueel raamwerk**
  - **Biedt een redelijke mate van structuur voor inhoud en relaties tussen principes om consistent te kunnen worden toegepast**
  - **Structuur moet zodanig zijn dat uitzonderingen op de standaard geminimaliseerd worden**

Opzet “standaard” binnen IT Auditing



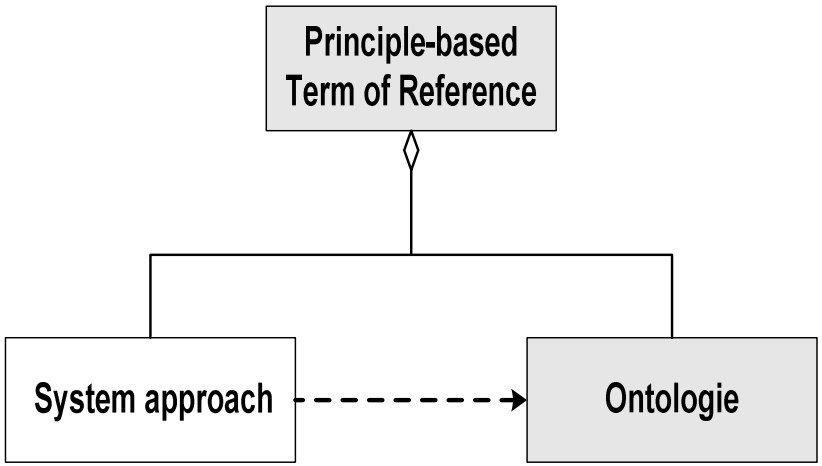
Principle based Term of Reference



- Holistisch aanpak
- Systematiek
- Structuur (Layered Pattern)
- Principes gericht op Structuur

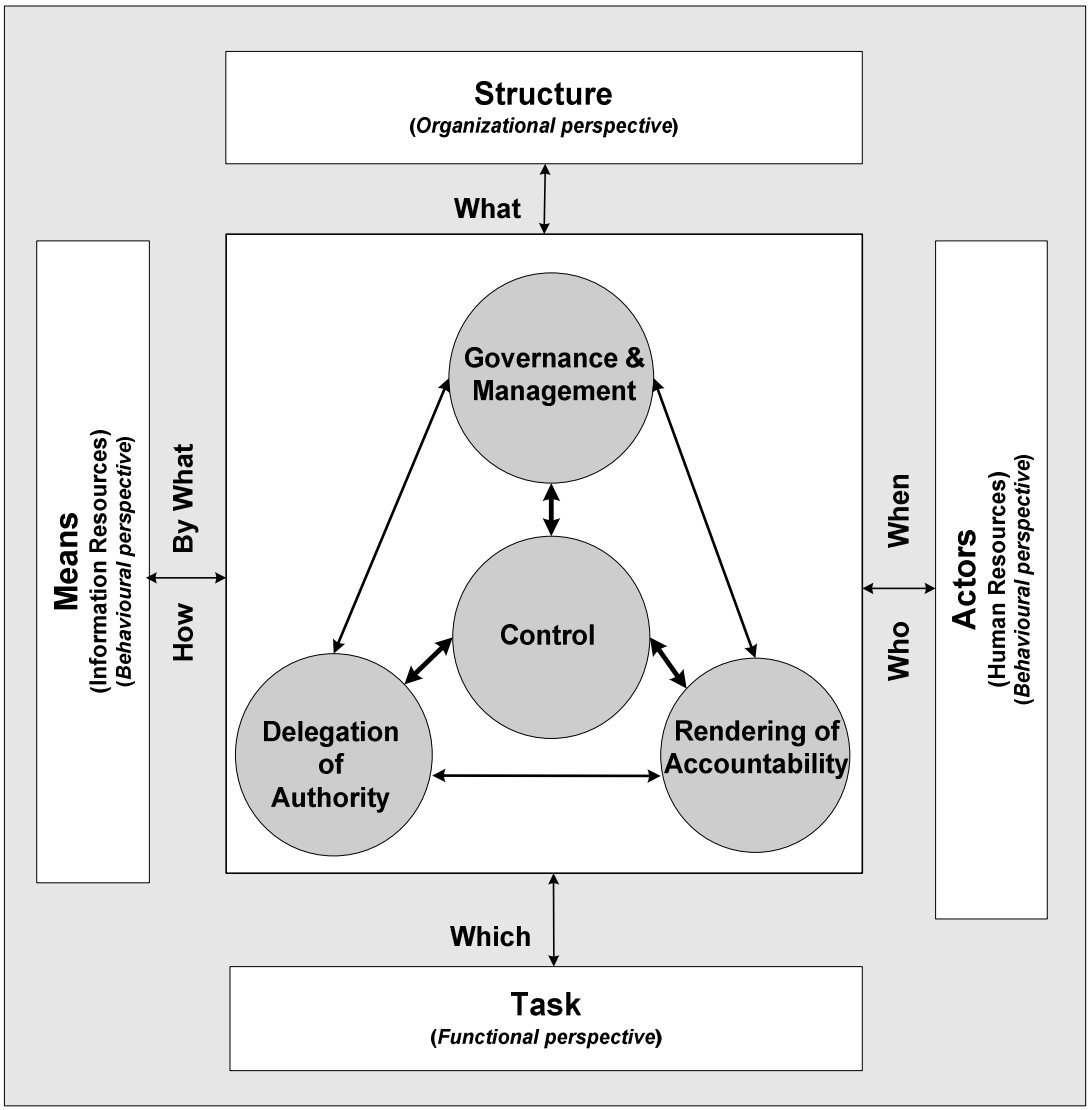
- Taxonomie van objecten
- Relaties tussen en combinaties van objecten
- Content per Layer
- Sentences (Relaties & Associatie)
- Corresponderende Layer Principes

System approach



- *Structuren* zijn afgeleid uit**:**
  - **Starreveld (GDAC model)**
  - **De Leeuw (ETSCO-model)**
  - **Henderson & Venkatramen (SAM)**

Starreveld (GDAC)



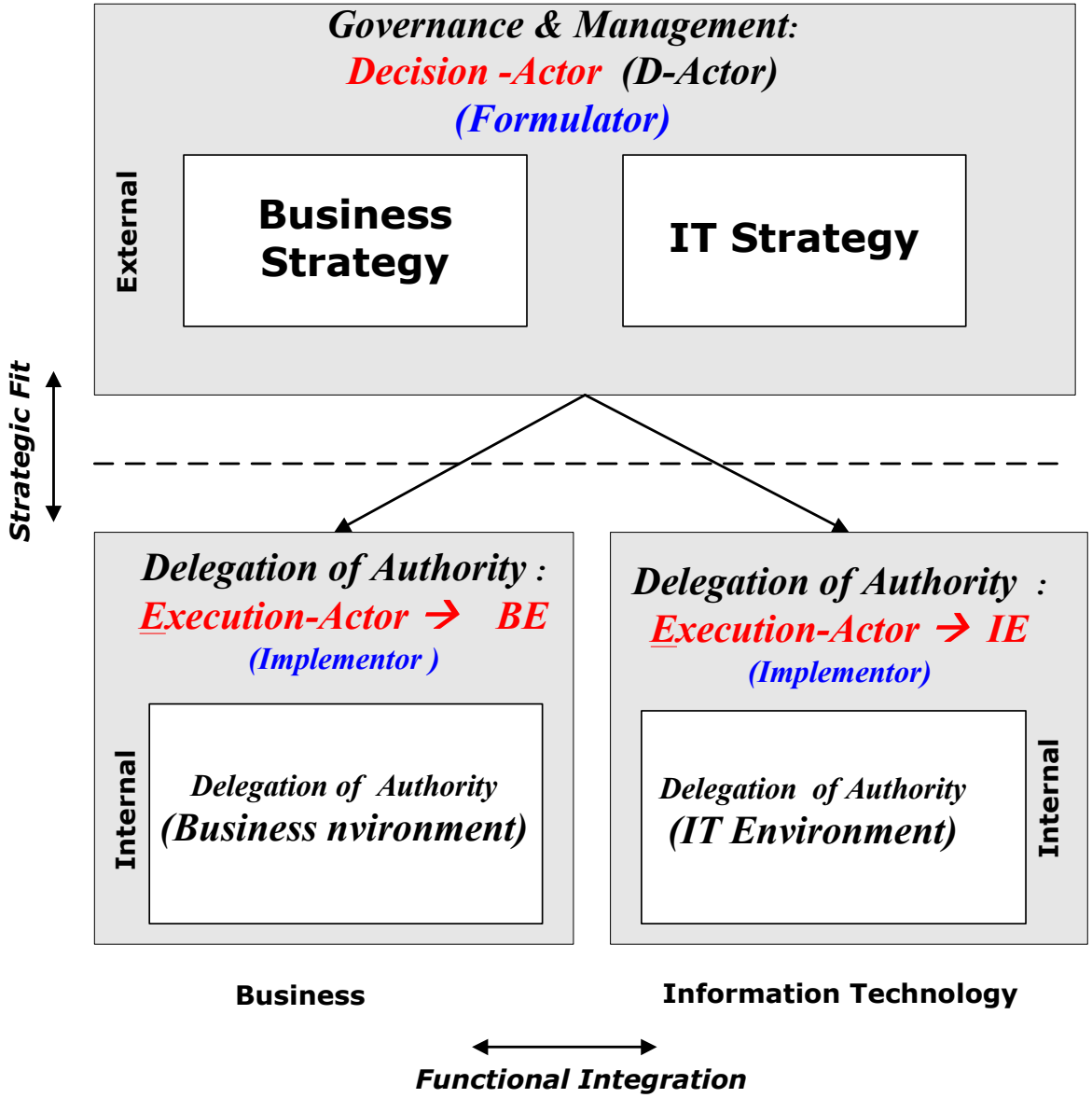
Governance & Management : **PoGM**

Delegation of Authority : **PoDA**

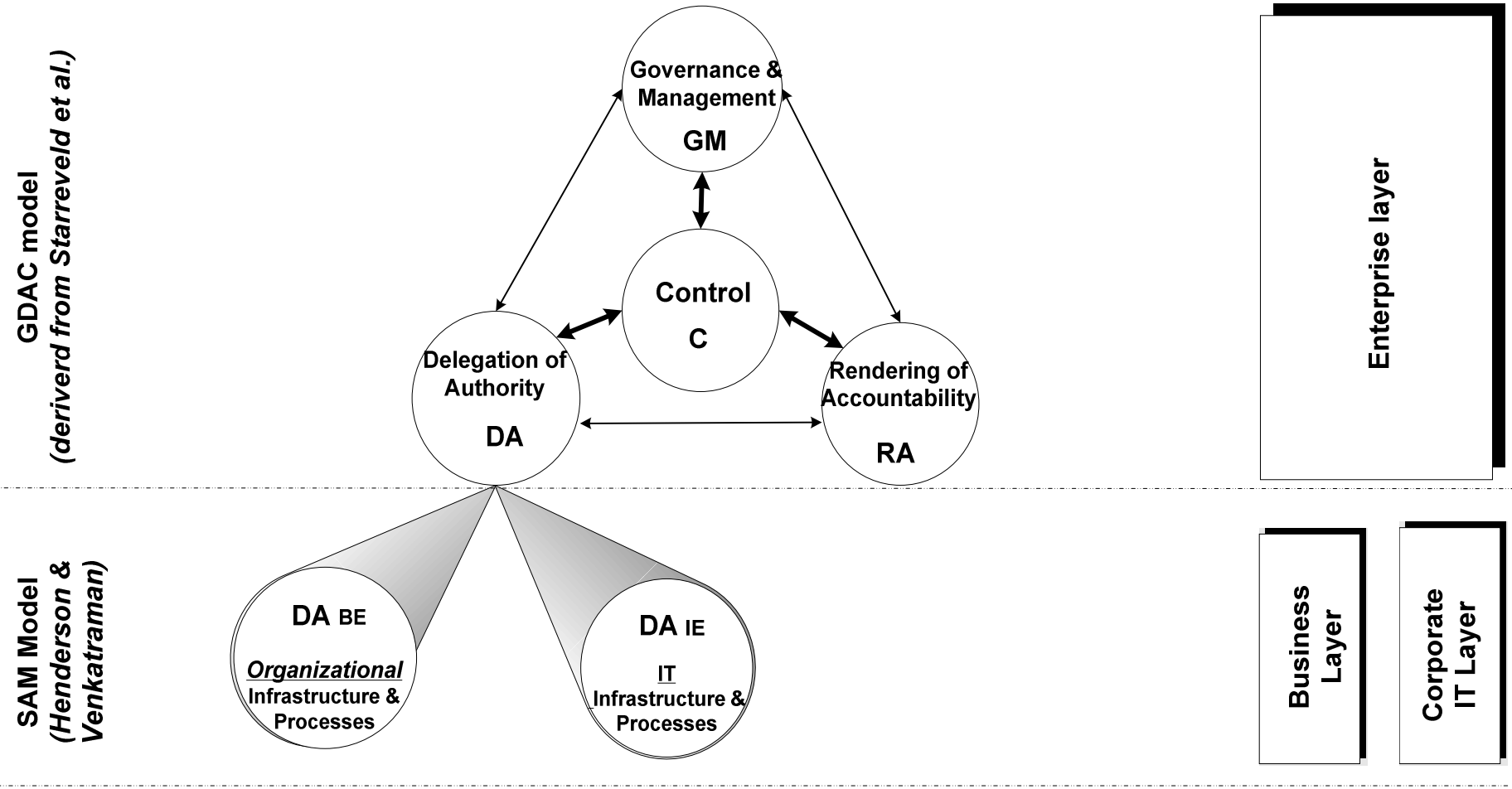
Rendering of Accountability : **PoRA**

Control : **PoC**

H & V : SAM → (BE & IE)


Governance & Management:
Decision -Actor (D-Actor)
(Formulator)
External
Business Strategy
IT Strategy
Strategic Fit
Delegation of Authority :
Execution-Actor → BE
(Implementor)
Internal
Delegation of Authority
(Business nvironment)
Delegation of Authority :
Execution-Actor → IE
(Implementor)
Delegation of Authority
(IT Environment)
Internal
Business
Information Technology
Functional Integration

Relatie: GDAC-SAM

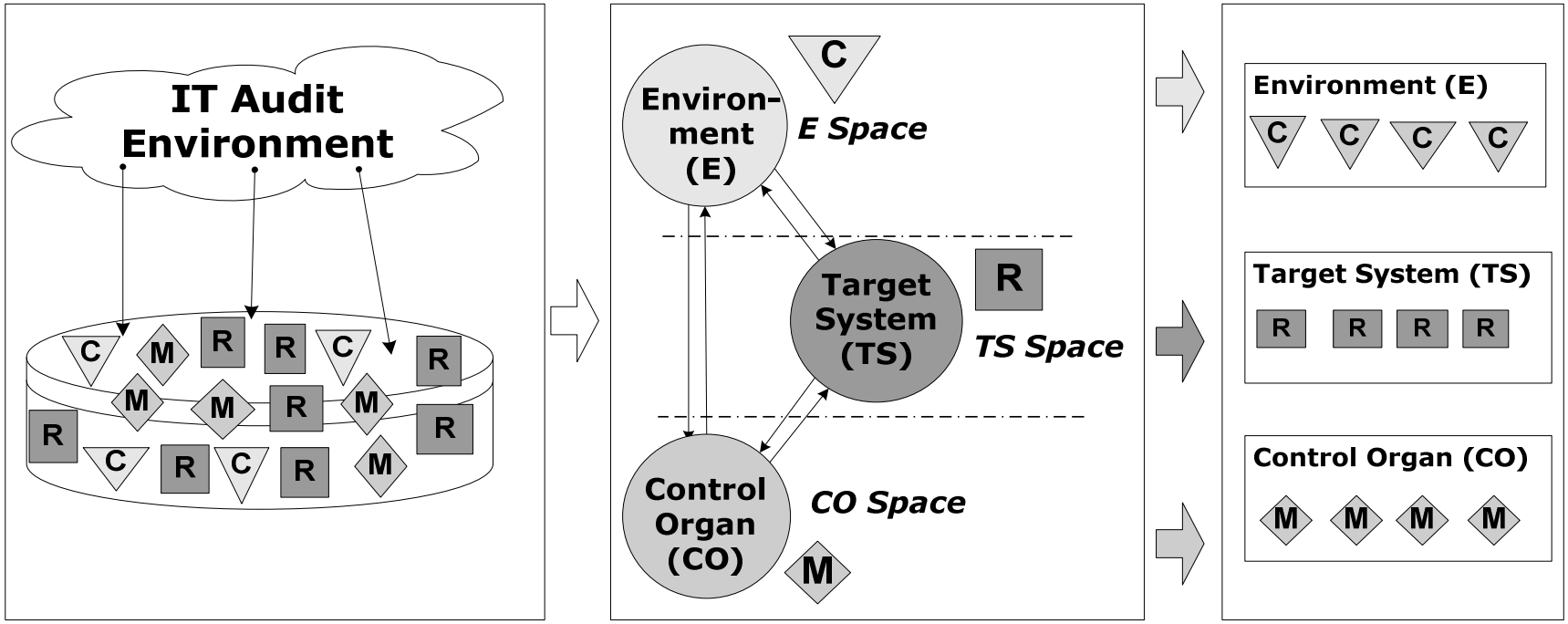


DoA (IE) →ETSCO model

Mix van:
Conditionele,
Configuratie van Resources en
Management aspecten

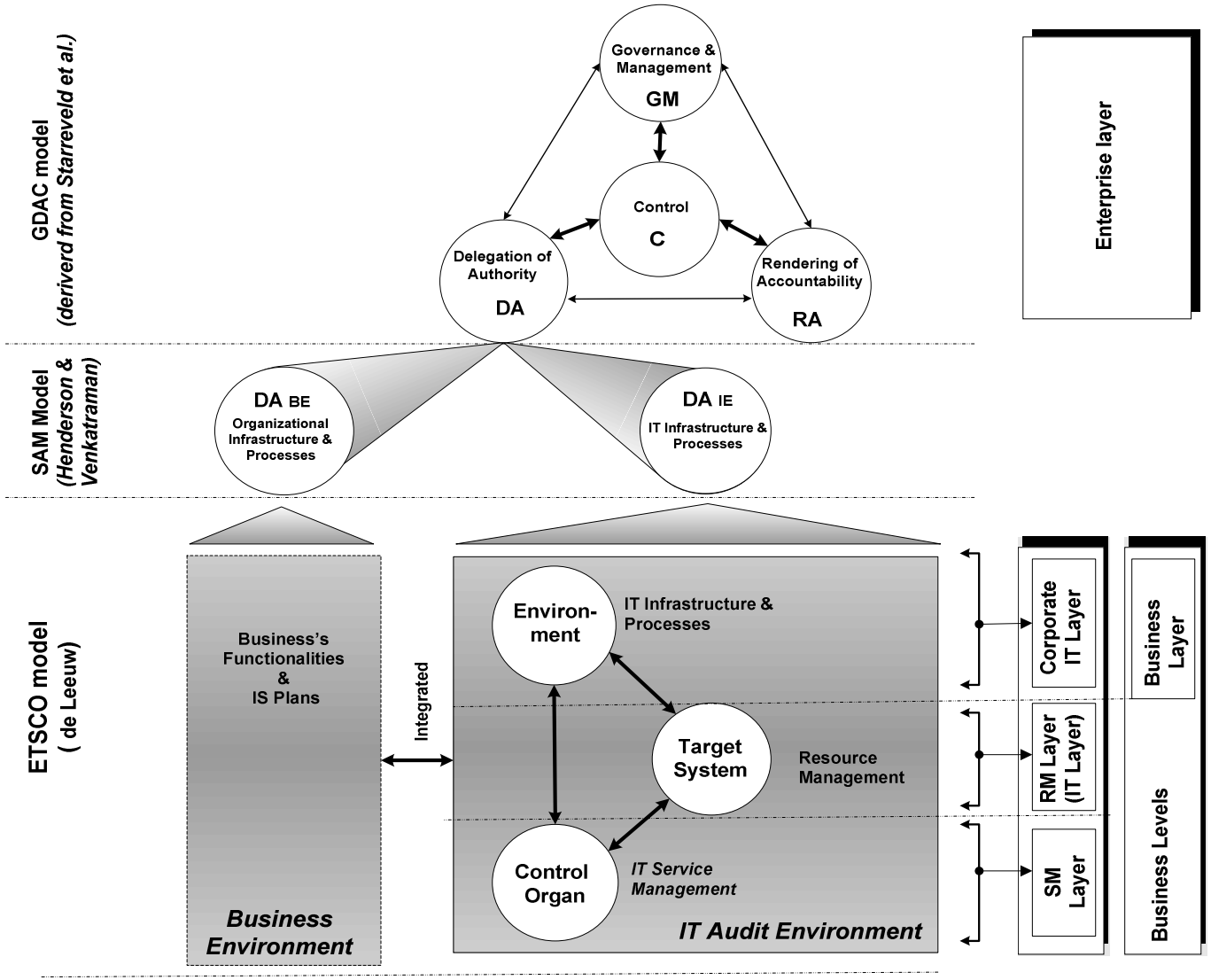
Relaties tussen sub systemen

Scheiding van Beleids-, Inrichting en Beheersingsaspecten

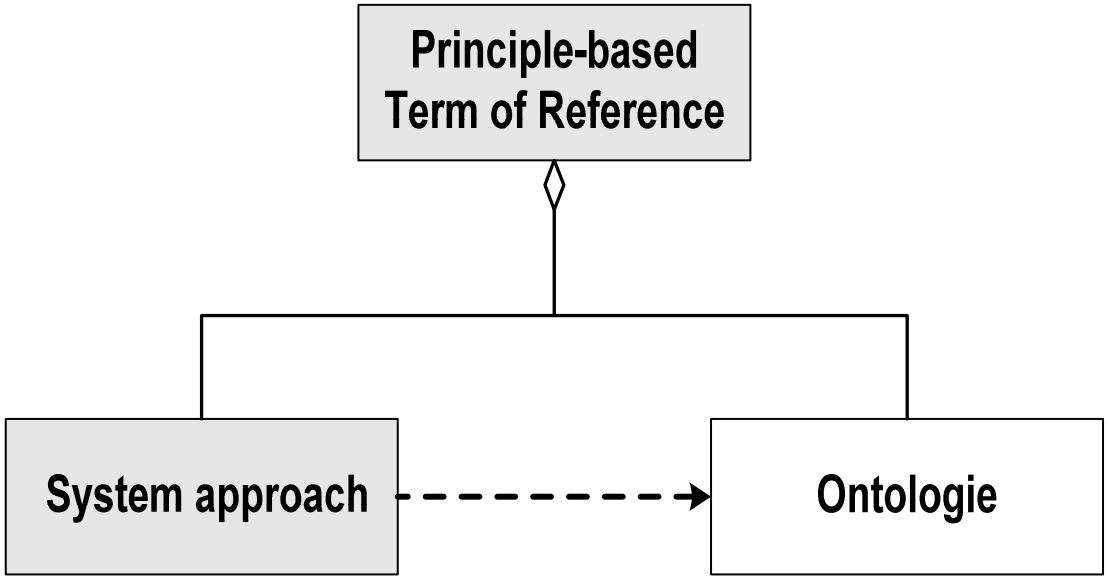


C - Conditional elements
R - Resource elements
M - Management elements

Relatie: GDAC - SAM – ETSCO (GSE)

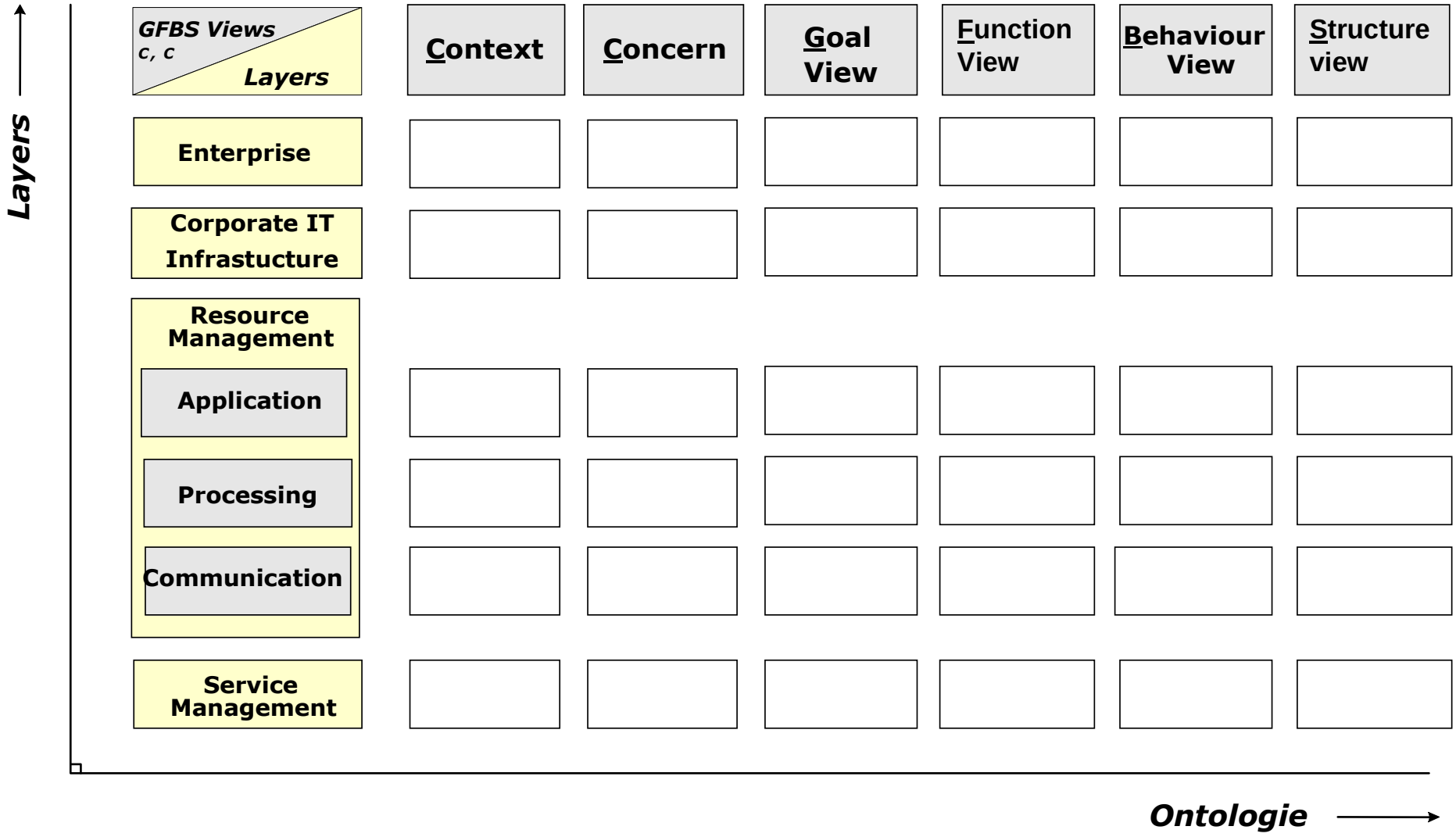


Ontologie

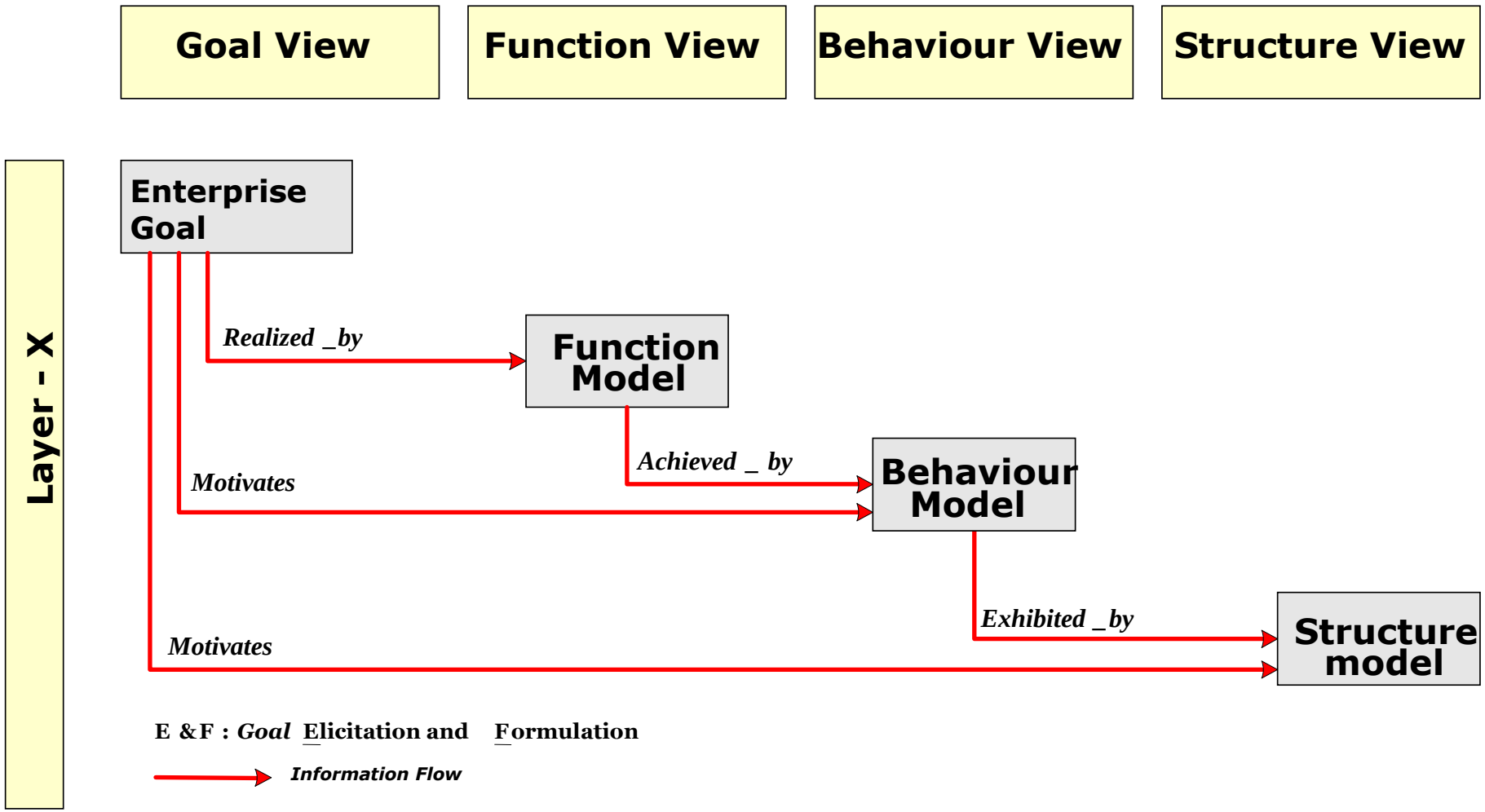


- *Structuur* : (layered pattern) afgeleid uit GSE model
- *Inhoudelijk* : per layer toepassing van ontologie om pattern af te leiden

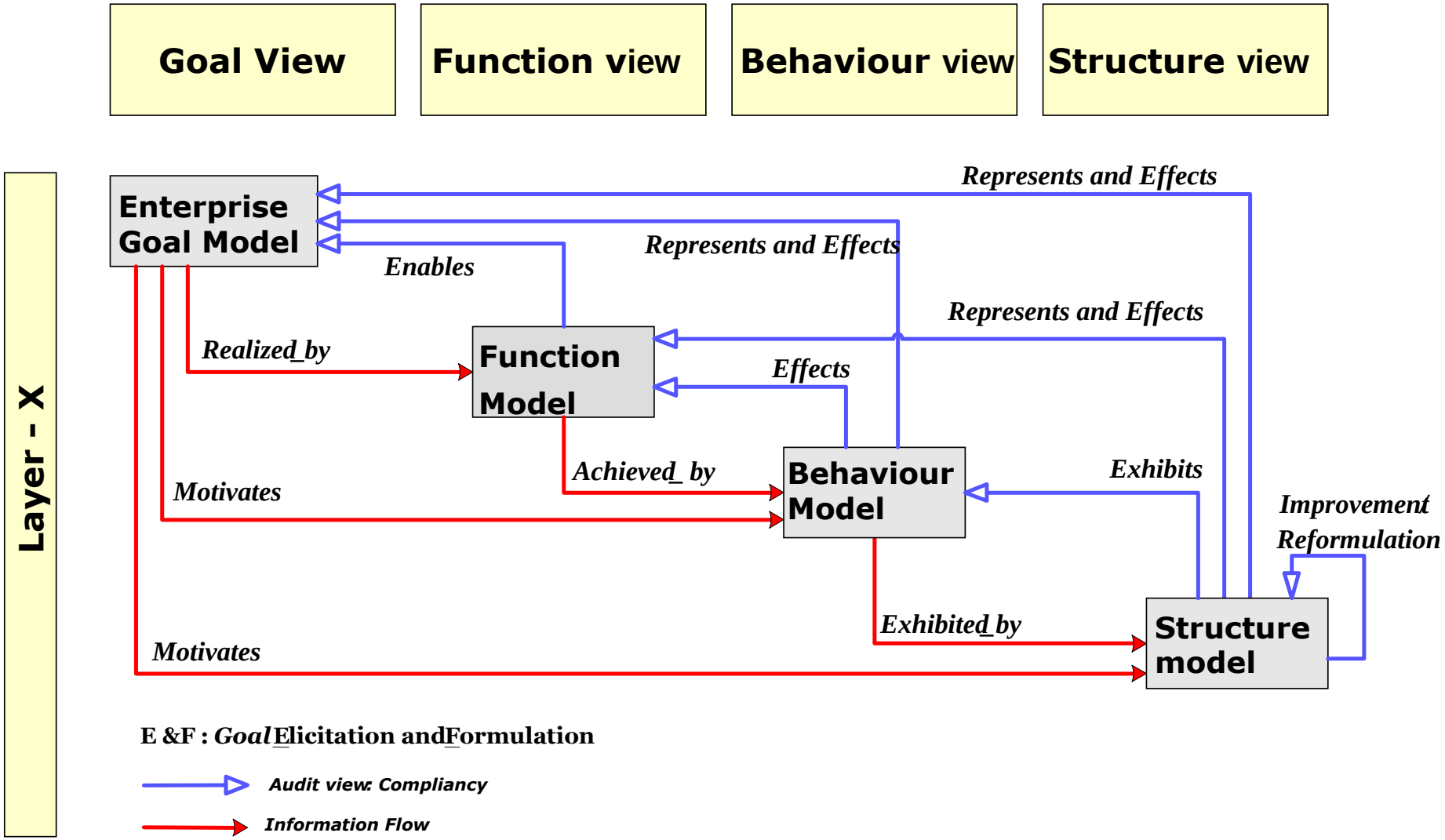
Layers vs Ontologie (GFBS)



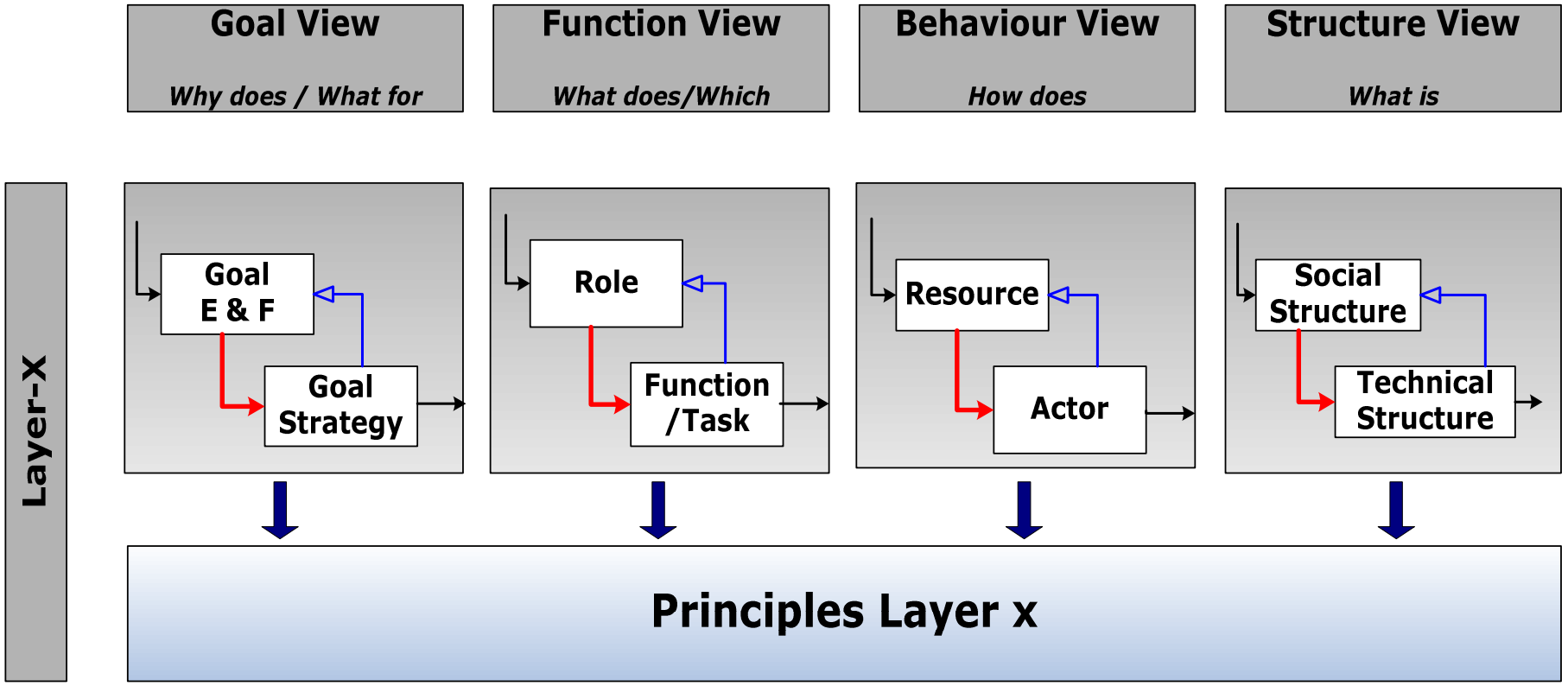
Layer-x vs GFBS view (1)



Layer-x vs GFBS view (2)



Layer-x vs GFBS view (3)



E &F : *Goal* Elicitation and Formulation

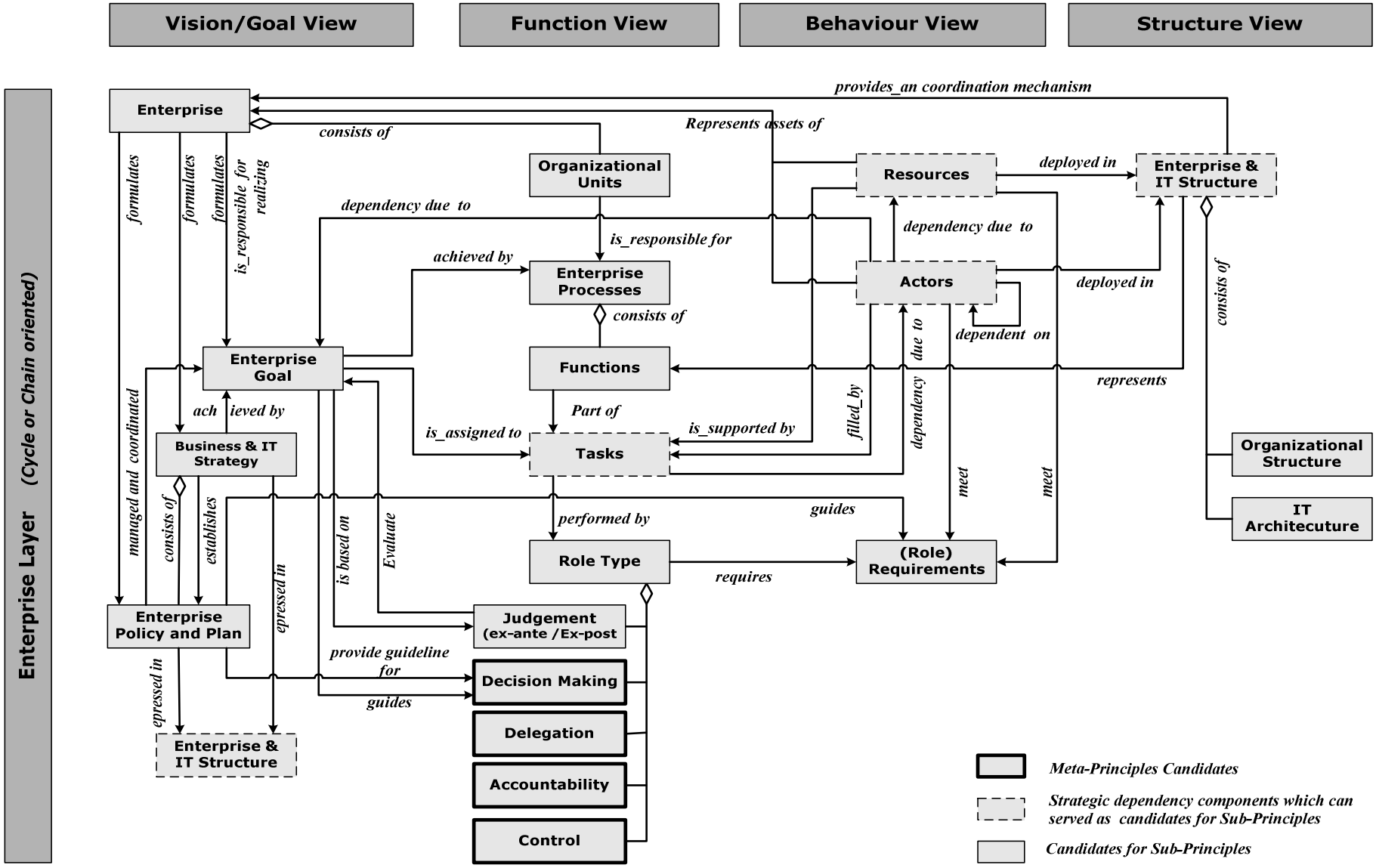
Audit view: Compliancy

Information Flow

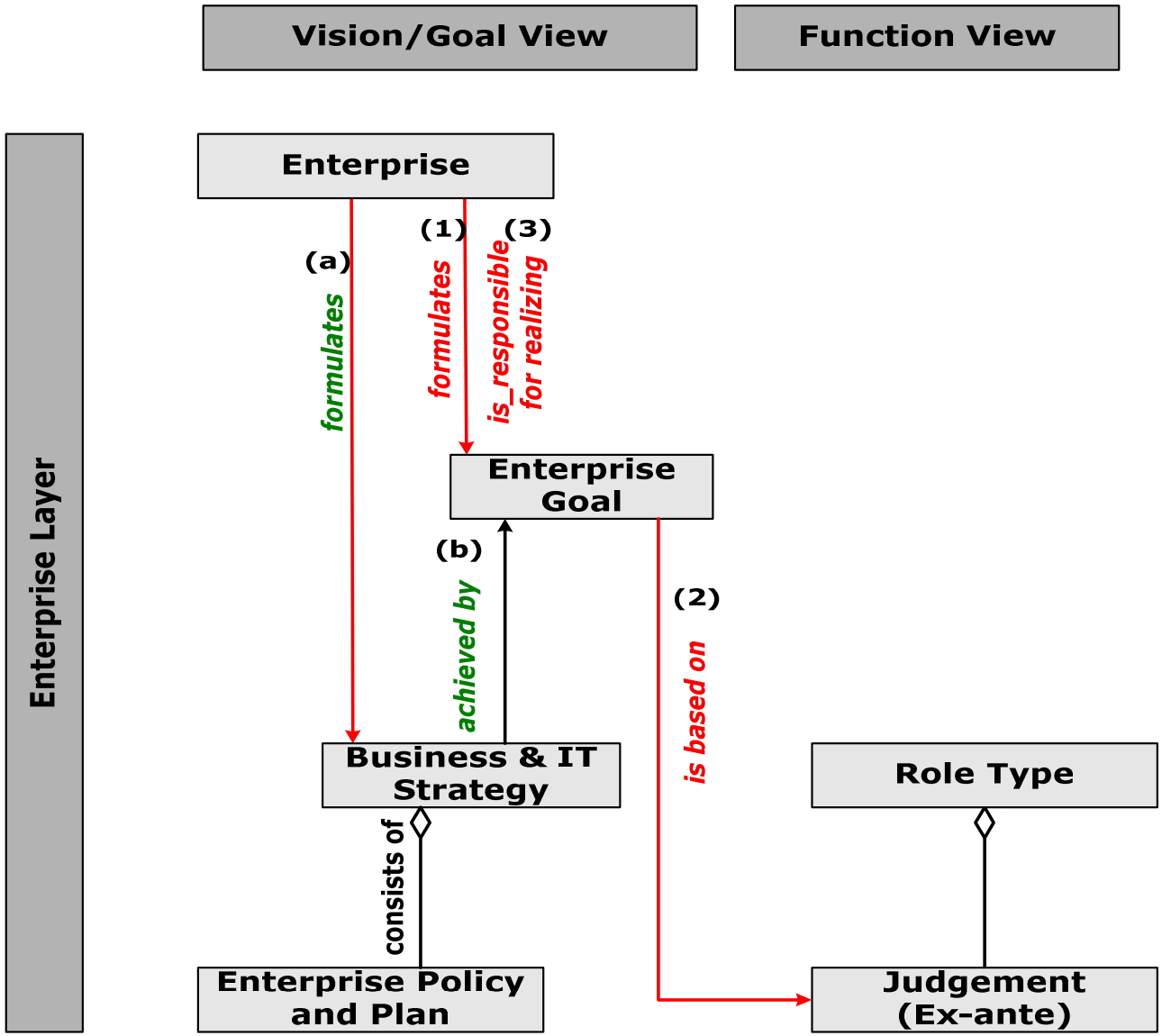
GFBS-Ontologie (Voorbeeld)

Communication Layer (LAN)	
Context	**Het LAN *biedt communicatie* services aan gebruikers waarin Functionele en Non-Functionele requirements zijn verwerkt. De requirements worden uitgevoerd obv LAN Policy.**
Concern	**Onjuiste inrichting en implementatie van het LAN verhindert gebruikers bij het uitvoeren van hun taken. Hierdoor lijdt de organisatie productieverlies.**
Goal View	**Het creëren van een veilige netwerkomgeving die toegang biedt tot applicaties die de primaire en secundaire processen ondersteunen.**
Function View	**LAN dient de functionaliteit te bieden voor gegevenstransport en gegevensuitwisseling tussen gebruiker en applicaties**
Behaviour View	**FR : De features van betrokken LAN - performance (bandbreedte) kunnen worden bereikt NFR : De features van betrokken LAN componenten - beveiligd zijn en beheerd worden.**
Structure	**Het LAN dient gebaseerd te zijn op een logische en fysieke architectuur**

Enterprise layer



Gedeeltelijke Goal View



Enterprise layer - Goal view

Voorbeeld Sentences:

Dependencies and Association are:

- **The Enterprise <*formulates*> the Enterprise Goal <*based on*> “Judgment- ex ante” and is < *responsible for the realization*>**

- **The Enterprise <*formulates*> the Business and IT Strategy, which guide <*achieving*> the Enterprise Goal**

Derived Principles

Corresponding principles:

- ***Principle*: Enterprise SHOULD *formulates* the Enterprise Goal *based on* Judgement ex-ante and is *responsible for the Goal realization.***

- ***Principle*: The Enterprise SHOULD *formulates* the Business and IT Strategy.**

Epiloog

- **Uit de analyses blijkt dat RFK (AToR) te structuren is**
- **Creëert meer samenhang, beter in context met bedrijfsdoelen**
- **Wel effectief, maar efficiency kan bereikt worden mbv Tool ondersteuning**