
SIVA-methode voor de ontwikkeling van auditreferentiekaders

Toepassingen:

- ADR (en NCSC)
 - Cobit : “Light Cobit versie” ?
-

Agenda

SIVA	Toelichting SIVA componenten
------	------------------------------

LTB	Analyse van een set LTB auditelementen en resultaten
-----	--

Cobit	“Light Cobit versie”
-------	----------------------

NCSC	Herziening van Webapplicatierichtlijnen 2012
------	--

Vragen in de praktijk

- Is mijn referentiekader/normenkader volledig?
- Ben ik goed bezig?
- Heb ik de juiste elementen meegenomen?

The logo for SIVA, consisting of the letters 'SIVA' in a bold, orange, sans-serif font, centered within a dark blue square.

**ISACA**[®]
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

Ontwikkeifasen van een referentiekader

1. Analyseren en identificeren

2. Clusteren

3. Ordenen

4. Bewerken

5. Formuleren

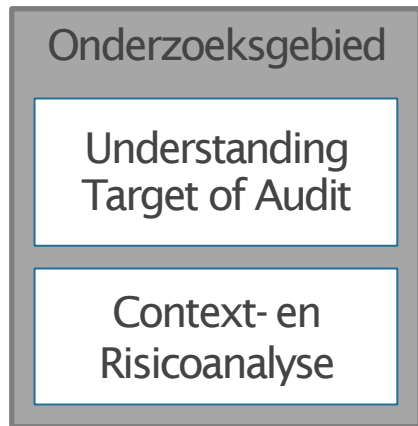
Brainstorm-/ Creatieve fase

Zoeken
naar
ontbrekende elementen
en
samenhang

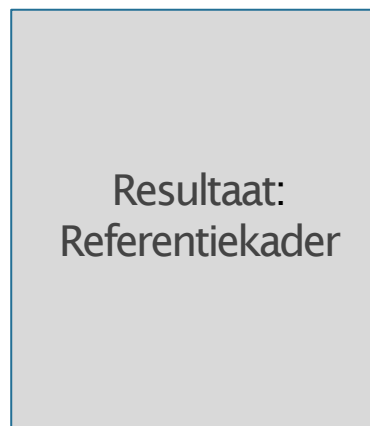
Definiëren van
Hoofd- en Subnormen

Hulpmiddelen: Raamwerk

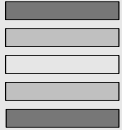
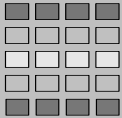
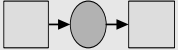

Fase 1



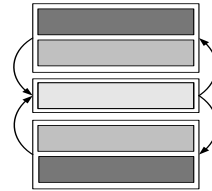
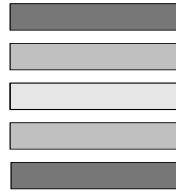
Fases 2-5



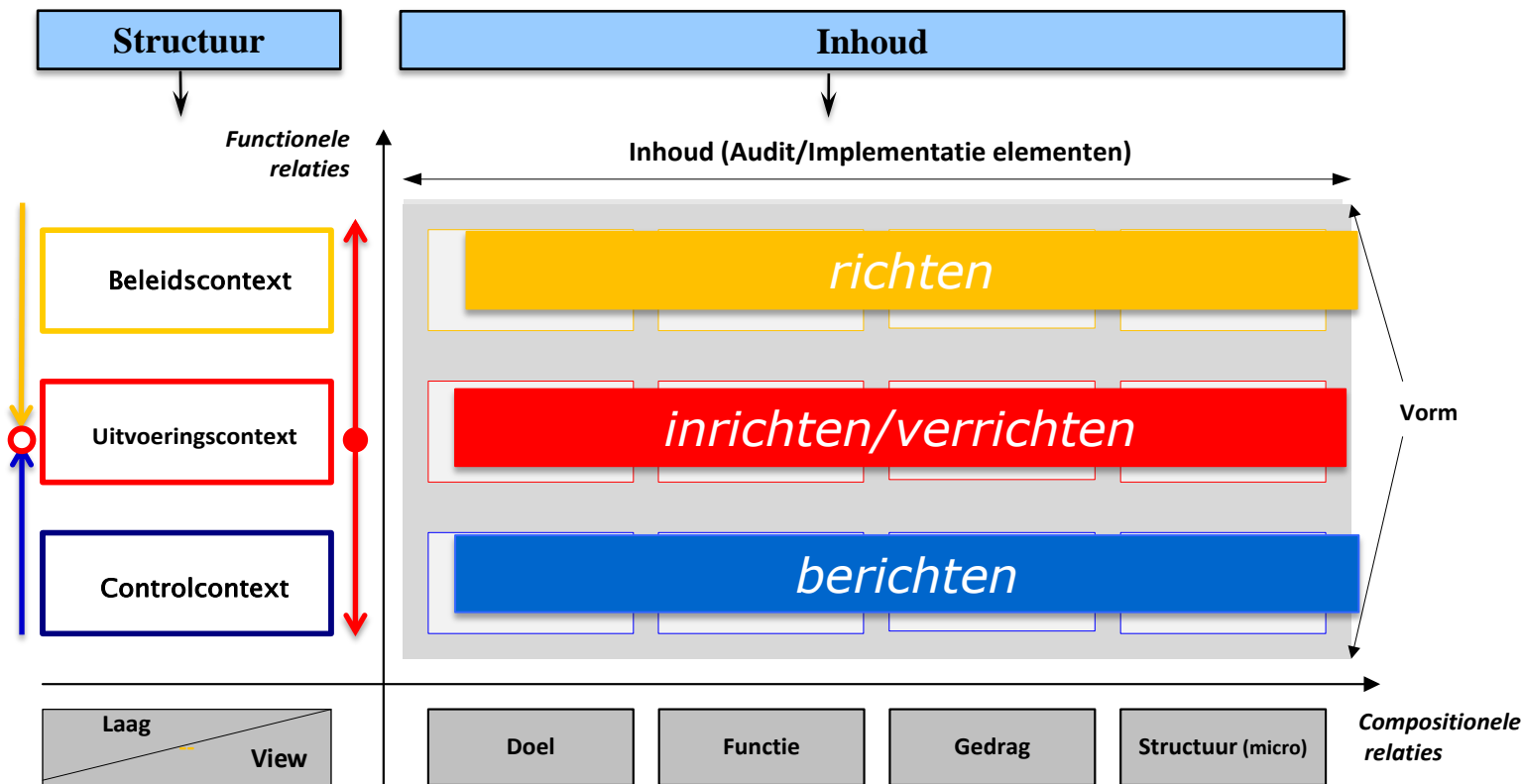
Hulpmiddelen: Raamwerk

Component	Symbol	Kenmerk
Structuur		Lagenstructuur <i>“patroon van domeinen”</i> om de auditomgeving in samenhang te kunnen analyseren
Inhoud		Inhoudanalyse: <i>“patroon van neutrale auditelementen”</i>
Vorm		Formuleringsvoorschrift Interpretatie (syntax/semantiek) <i>“patroon van formuleren”</i>
Analyse volgorde		Volgorde van de analyse van de lagenstructuur (M,Mo,Mi)

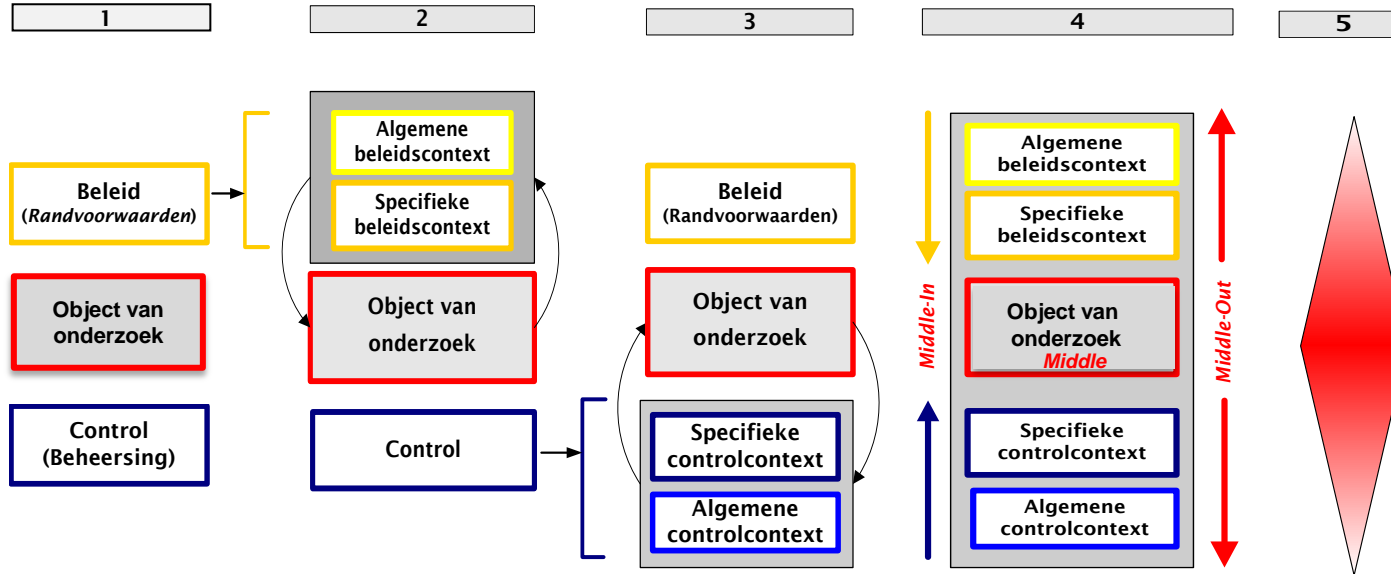
Structuur en Volgorde



SIVA-raamwerk: Structuur, Inhoud, Vorm en Analysevolgorde

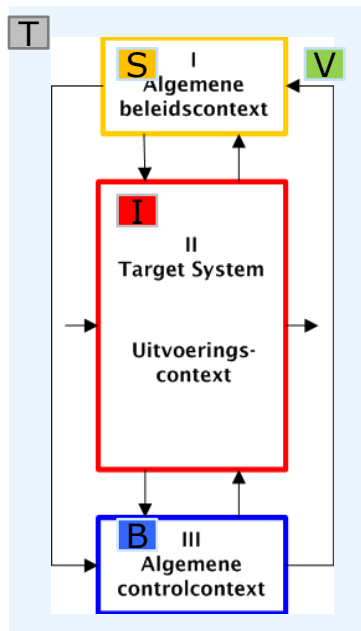


Structuur (Macro)



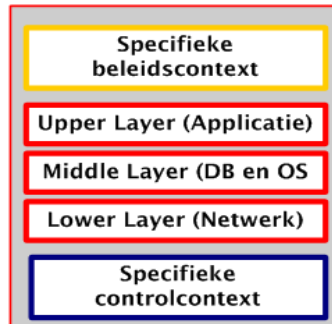
Structuur

Leeuw/Bunge



Lagenstructuur

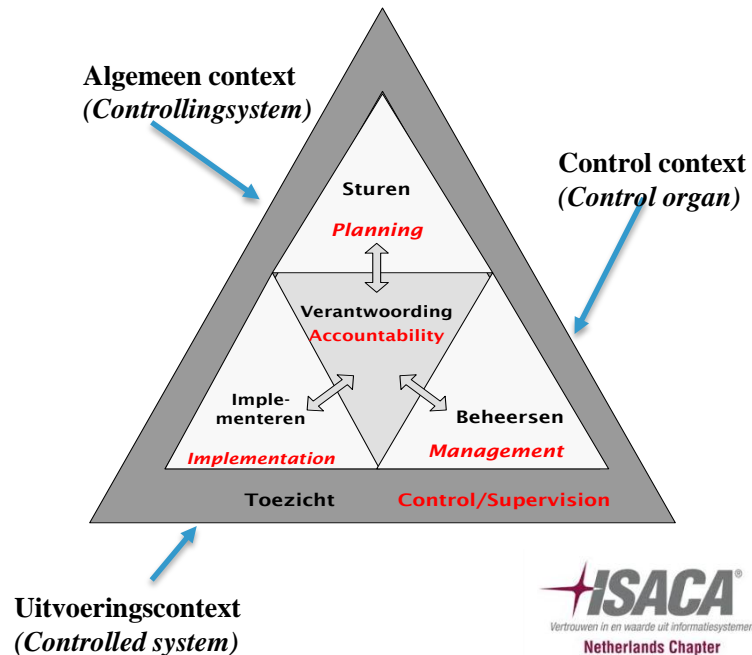
Algemene beleidscontext



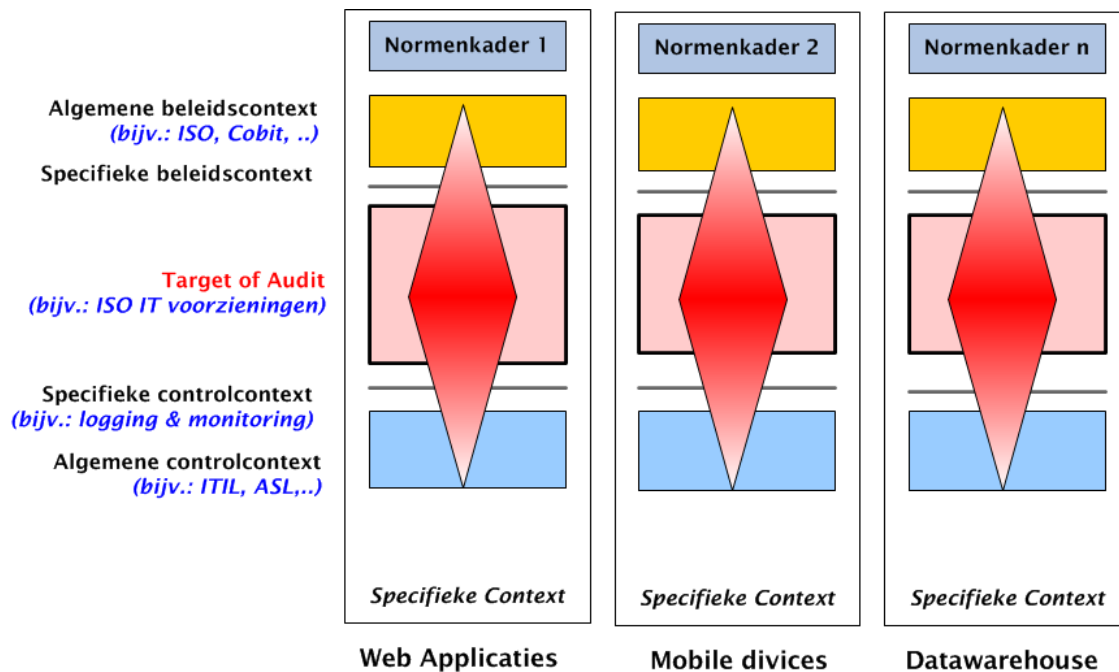
Algemene controlcontext

adresseert governance aspecten

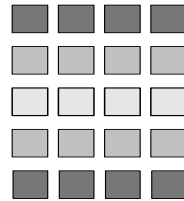
IT Governance



Gelijkvormige normenkaders



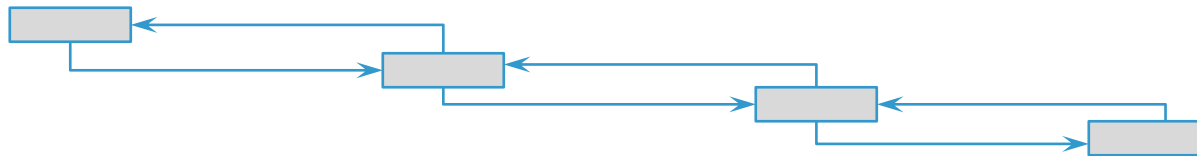
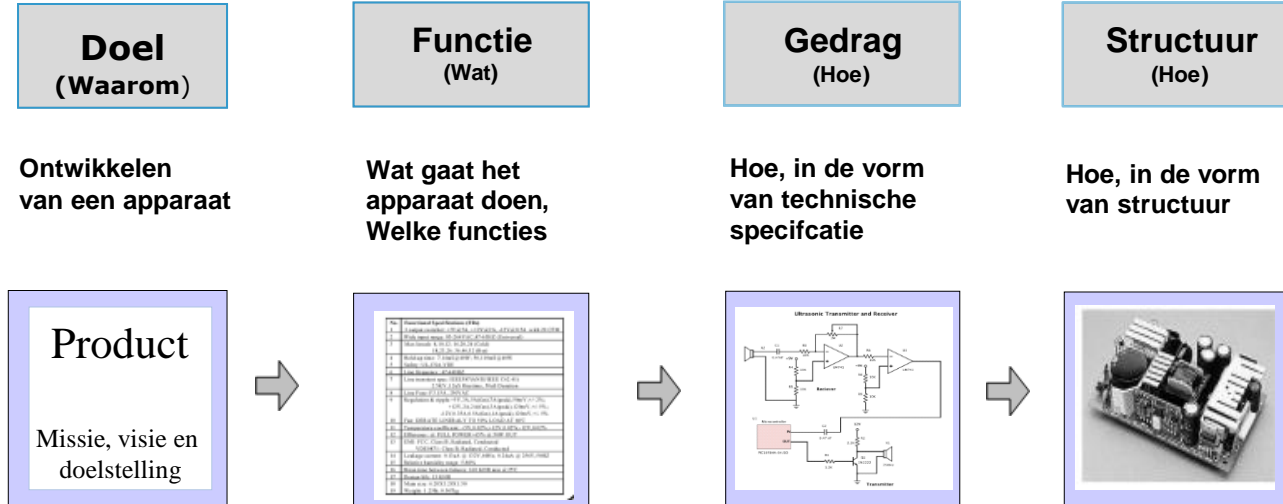
Inhoud



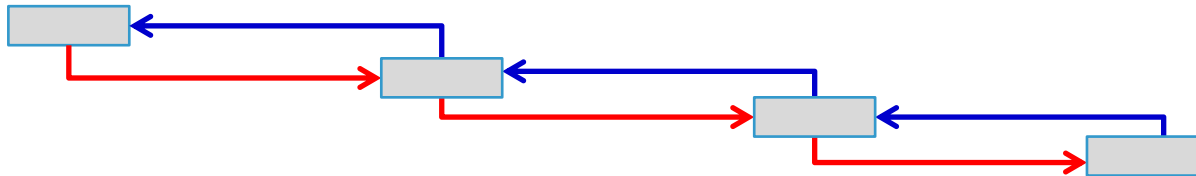
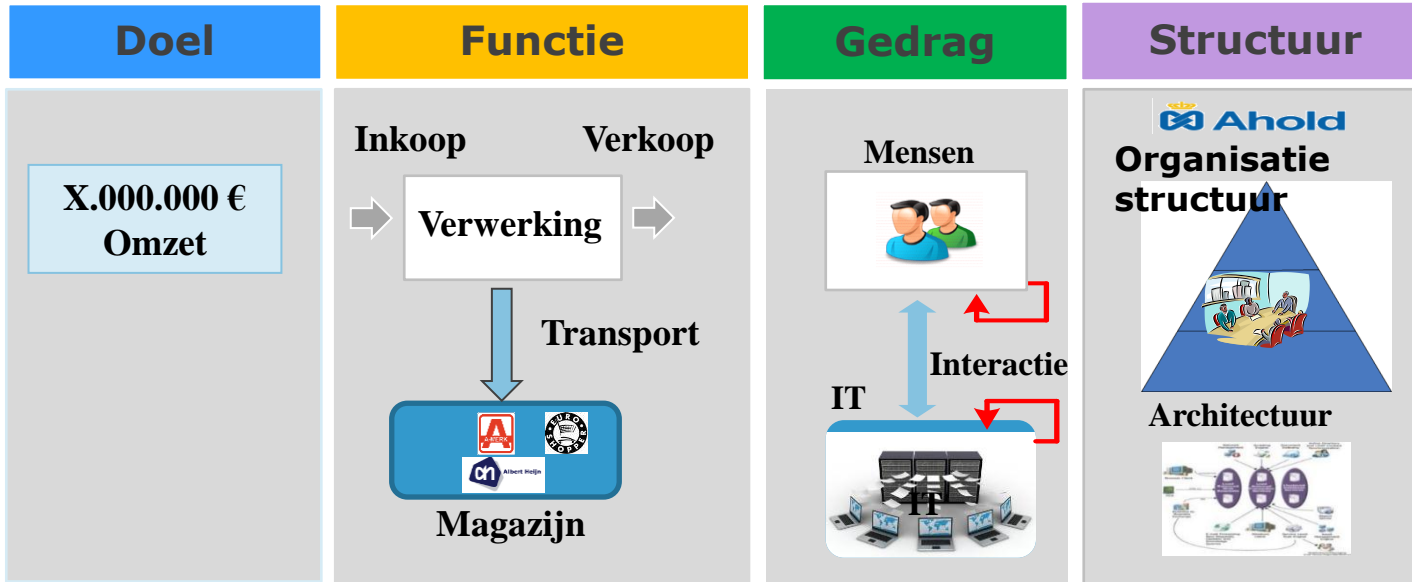
Inhoud (DFGS invalshoeken)



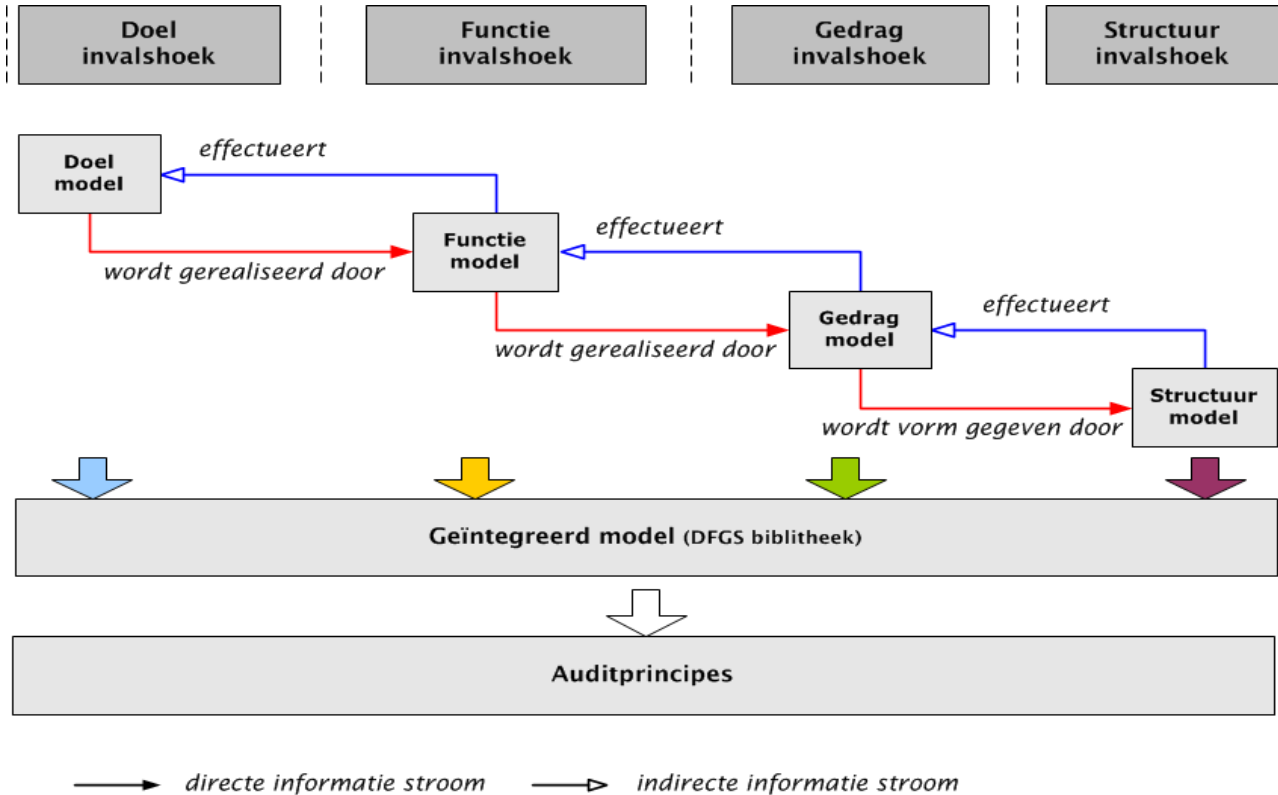
Toelichting (DFGS invalshoeken: Techniek)



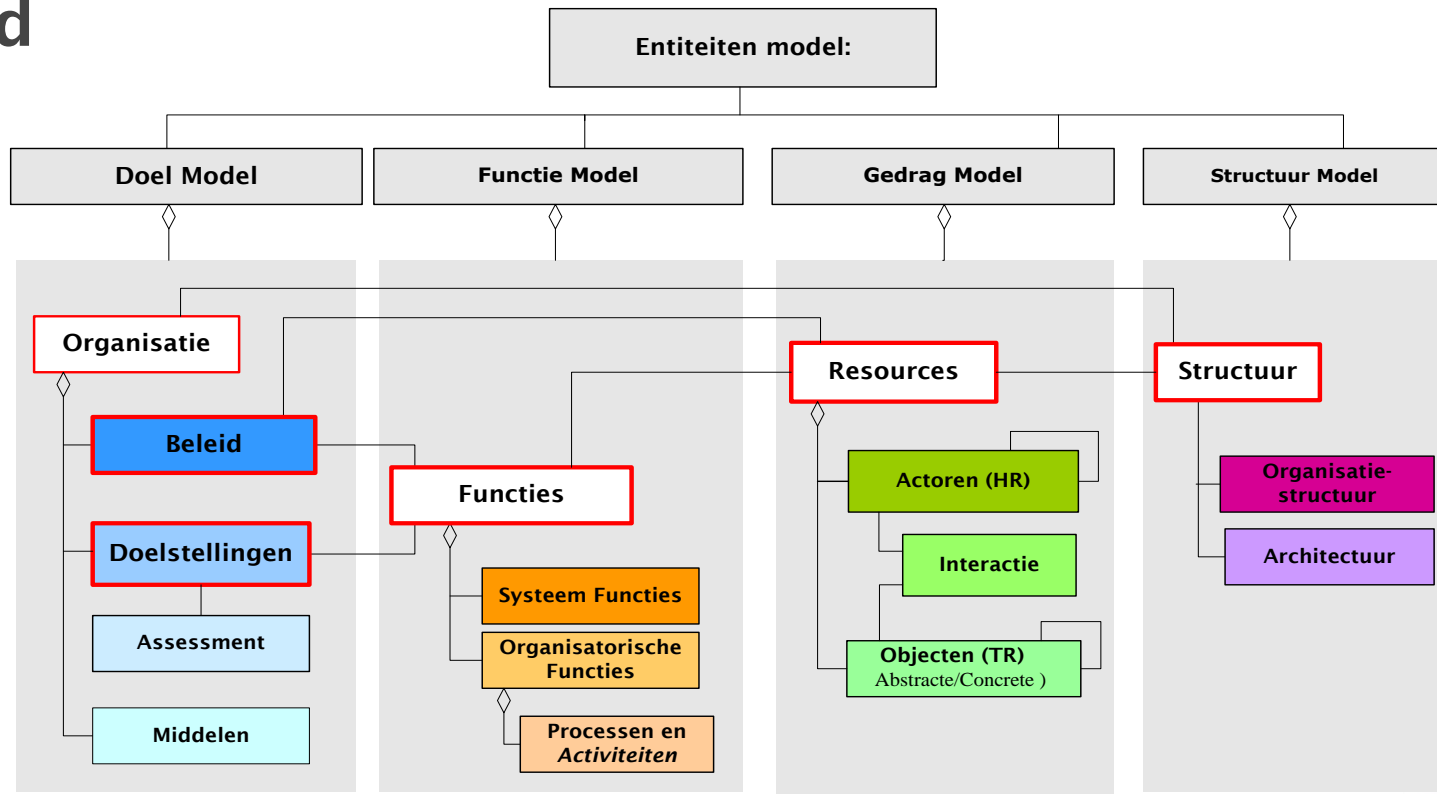
Toelichting (DFGS invalshoeken: organisatie)



Inhoud

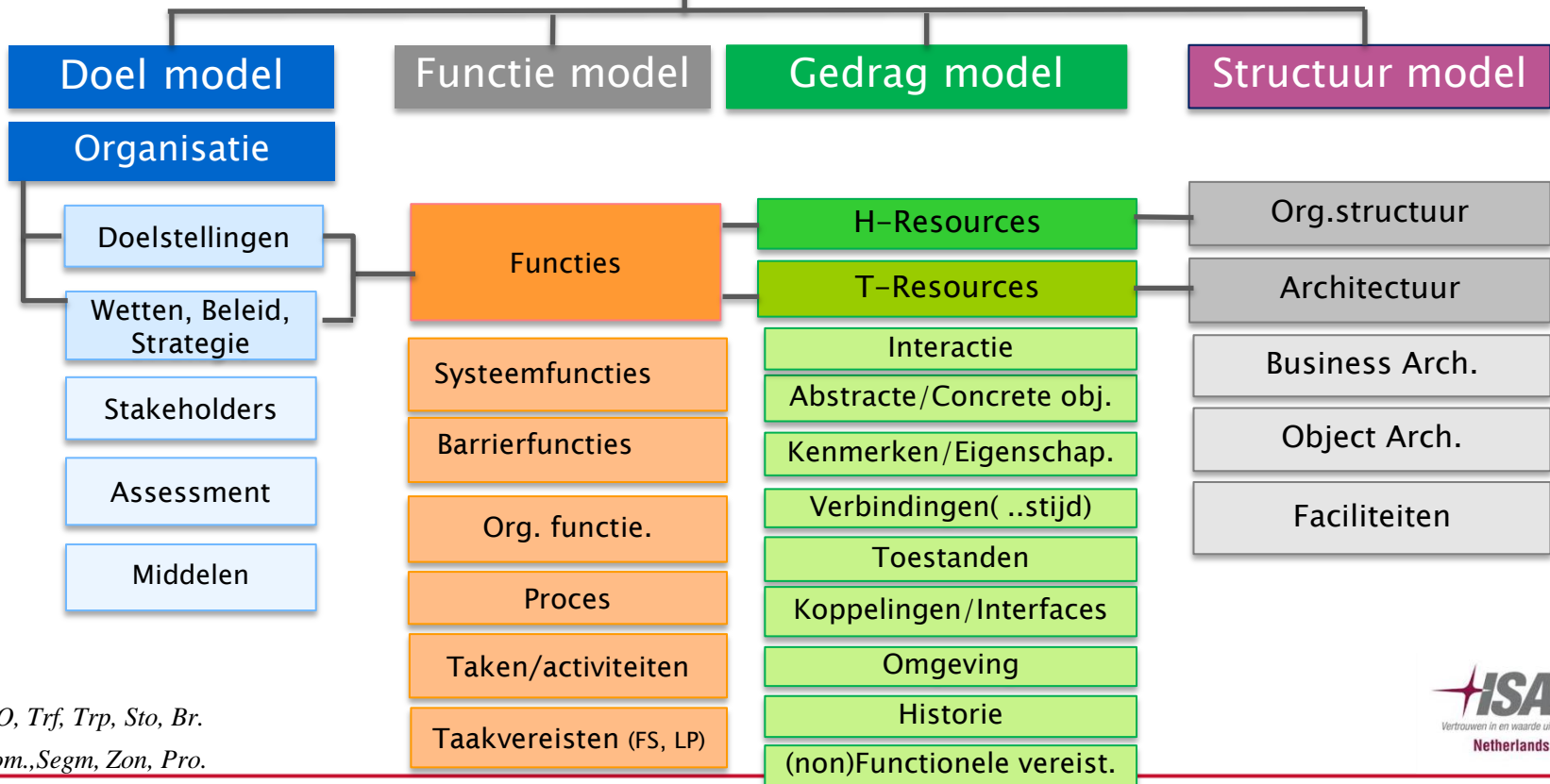


Inhoud



Inhoud (Basiselementen)

Entiteitenmodel



SF = I/O, Trf, Trp, Sto, Br.

Br = Com., Segm, Zon, Pro.

Structuur-Inhoud matrix

<p>Laag</p> <p>Views: DFGS</p>	<p>Doel-invalshoek</p> <p>Waarom</p>	<p>Functie- invalshoek</p> <p>Wat (Wat moet er gedaan worden)</p>	<p>Gedrag-invalshoek</p> <p>Hoe t.a.v. gedrag</p>	<p>Structuur- invalshoek</p> <p>Hoe t.a.v. structuur</p>
<p>Beleidscontext</p> <p>(condities en randvoorwaarden)</p>	<p>Missie, Visie, Algemeen beleid en strategie</p>	<p>Organisatorische functies en IT functies</p>	<p>Gedrag resources (Actoren en IT Services)</p>	<p>Business en IT organisatie structuur, business architectuur</p>
<p>Uitvoeringscontext</p> <p>Applicatie</p> <p>Verwerking (Middleware en PLatformen)</p> <p>Netwerk (Communicatie)</p>	<p><i>Applicatie beleid (richtlijnen en instructies)</i></p> <p><i>Verwerking beleid, (richtlijnen en instructies)</i></p> <p><i>Communicatie beleid (richtlijnen en instructies)</i></p>	<p>Business processen, taken en applicatie services</p> <p>Verwerkingsprocessen, taken en services</p> <p>Communicatie- processen, taken en services</p>	<p>Gedrag actoren en applicaties services</p> <p>Gedrag Verwerkingservices</p> <p>Gedrag communicatie-services</p>	<p>Applicatiearchitectuur</p> <p>Verwerkingsarchitectuur (i.e. middleware en platform)</p> <p>Communicatie-architectuur</p>
<p>Controlcontext</p>	<p>Algemene-control beleid t.a.v. services</p>	<p>Control functies en management-processen</p>	<p>Controle op geïmplementeerde IT-services</p>	<p>Managementcontrol structuur</p>

Oordeelsvorming

Oordeelsvorming (Lijst)

Nummer	Nummer BIR.	Onderwerpen BIR.	Oordeels-vorming
1	8.3.3	Blokkering van toegangsrechten	
2	11.1.1	Toegangsbeleid	
3	11.2.1	Registratie van gebruikers	
4	11.2.2	Beheer van (speciale) bevoegdheden	
5	11.2.3	Beheer van gebruikerswachtwoorden	
6	11.2.4	Beoordeling van toegangsrechten	
7	11.5.1	Beveiligde Inlogprocedure	
8	11.5.2	Gebruikers identificatie en -authenticatie	
9	11.6.1	Beperken toegang tot informatie	

Oordeelsvorming (Lijst)

Beleidsdomein

11.1.1	Toeg, Bel	●
--------	-----------	---

Uitvoeringsdomein

11.2.1	Reg. G.	●
--------	---------	---

8.3.3	Bl. TgR	●
-------	---------	---

11.5.2	Geb. Id. Auth.	●
--------	----------------	---

11.2.3	Beh. Ge. W	●
--------	------------	---

11.5.1	Bev. Inlogpr.	●
--------	---------------	---

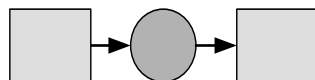
11.2.2	Beh. (Sp) B.	●
--------	--------------	---

11.6.1	Bep. T. Inf.	●
--------	--------------	---

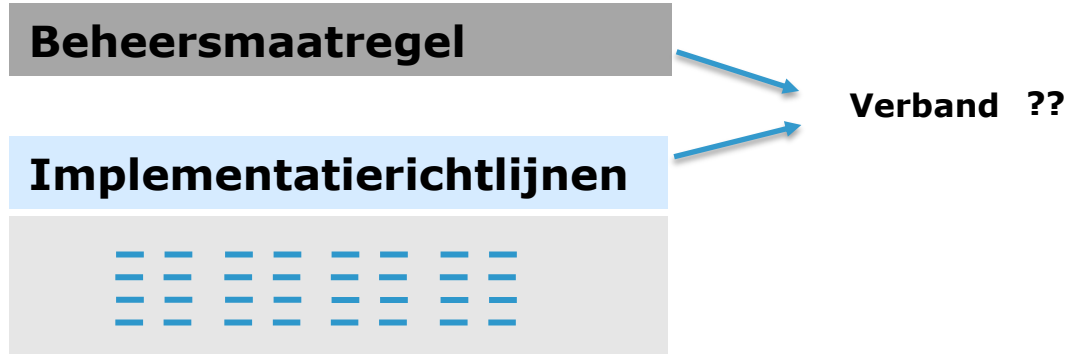
Controldomein

11.2.4	Beoord TgR.	●
--------	-------------	---

Vorm



Normen uit baselines/Best practices



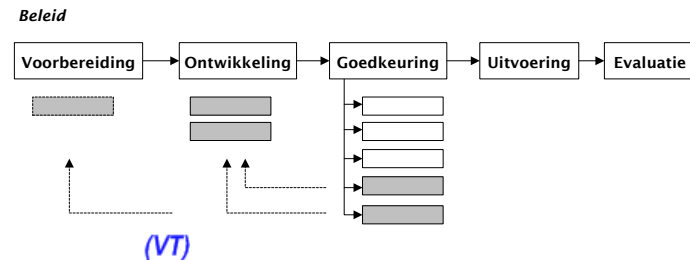
Voorbeeld ISO Norm

Beheersmaatregel

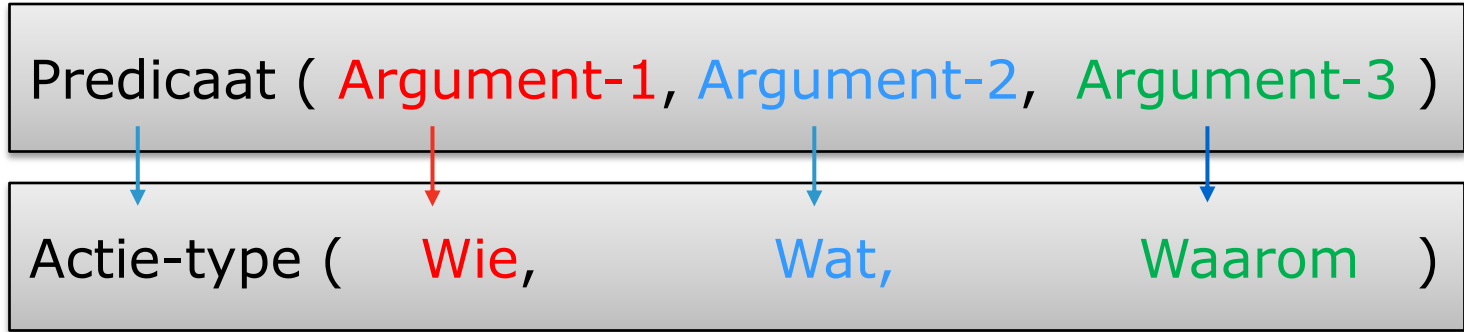
Directie moet informatiebeveiligingsbeleid goedkeuren en communiceren met werknemers en externe partijen)

Implementatierichtlijnen

- Beleidsdocument voor informatiebeveiliging **verwoordt:**
 - De betrokkenheid van de directie en beheer van informatiebeveiliging
 - *De benadering van de organisatie ten aanzien van het beheer van informatiebeveiliging* (VT)
- Beleidsdocument bevat ten minste de volgende informatie:
 - Definitie, algemene doelstellingen, reikwijdte, intentieverklaring, ...
 - *Kader voor beheersdoelstellingen en beheersmaatregelen* (VT)
 - *Uiteenzetting van beleid, uitgangspunten, normen en nalevingseisen ten aanzien van de beveiliging* (VT)
 - Verwijzingen naar documentatie die het beleid kan ondersteunen
 - *Algemene en specifieke verantwoordelijkheden voor het beheer van informatiebeveiliging* (VT)
- **Beveiligingsrichtlijnen en procedures** voor specifieke informatiesystemen of beveiligingsvoorschriften die door gebruikers behoren te worden nageleefd
- **Dit informatiebeveiligingsbeleid behoort kenbaar te worden gemaakt aan gebruikers**



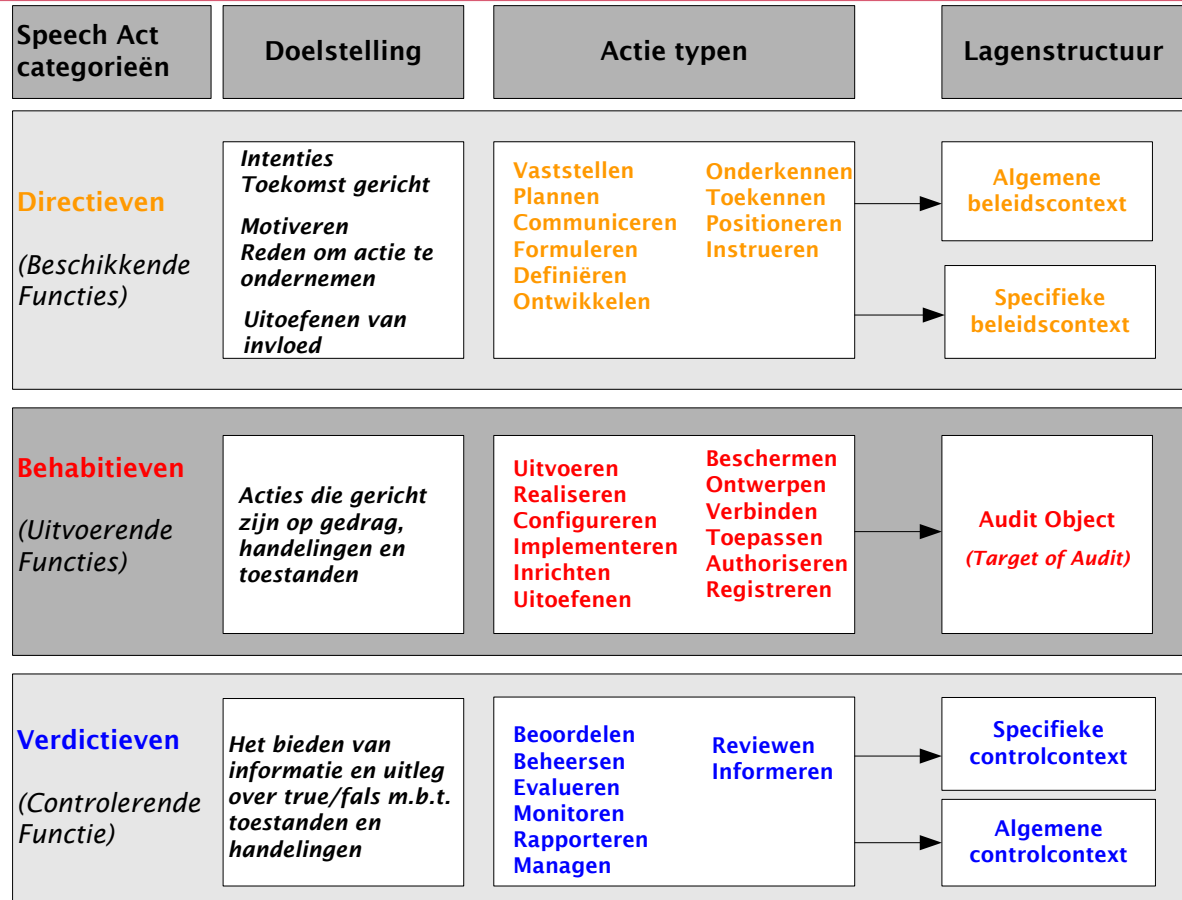
Vorm

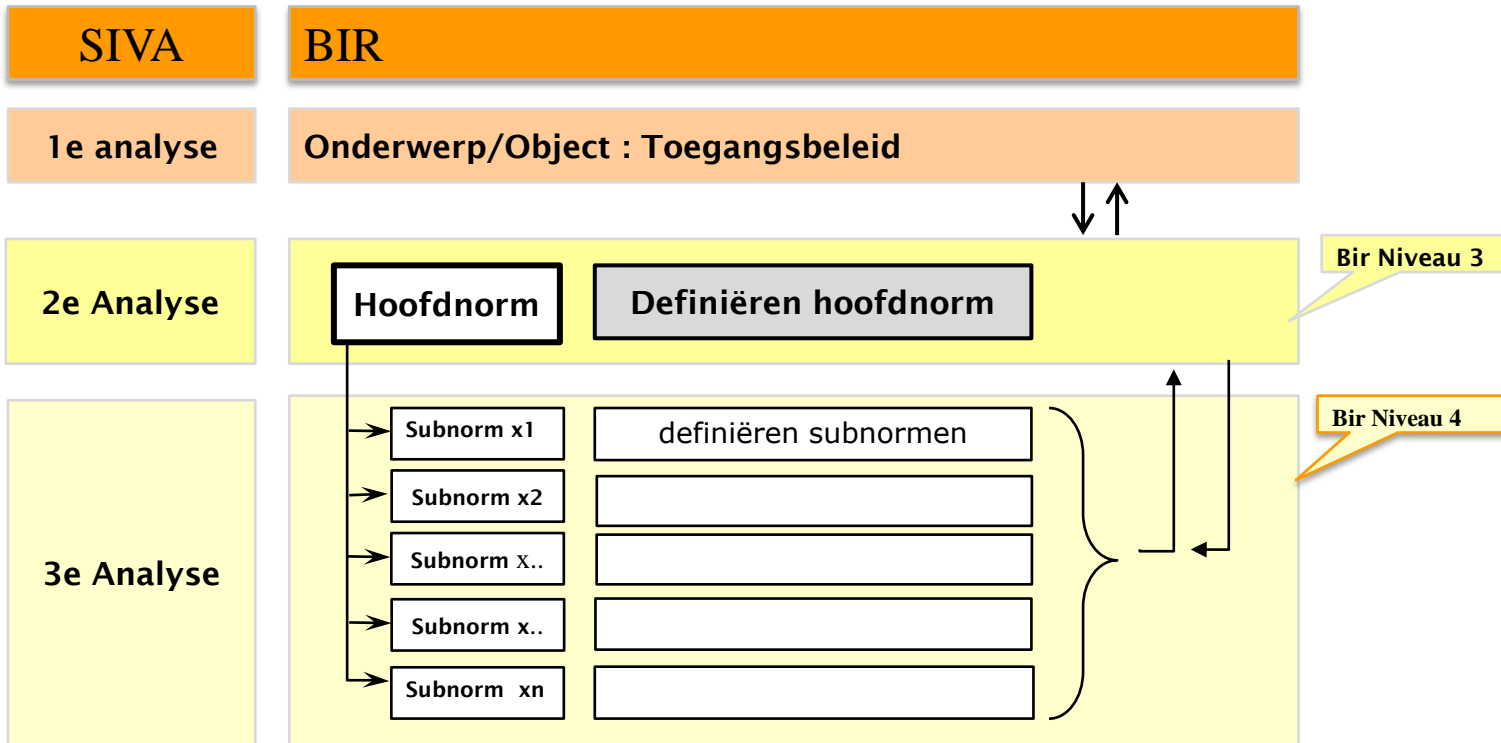


Vorm (Formuleringstemplate)



Vorm (Actie-typen)





Het belang van het consequent formuleringspatroon

□ Aanpak

- ❖ Hergebruik van BIR/BIG-normen (ISO 27000, 2013), Cobit , SoGP
- ❖ Identificeren van objecten per norm (niveau 3)
- ❖ Vaststellen van indicatoren/trefwoorden
- ❖ Per indicator
 - vaststellen van (ontbrekende) maatregelen (niveau 4)
 - elimineren van niet relevante maatregelen

□ Resultaat

- ❖ Door consequent formuleringspatroon worden omissies en/of dubbelingen binnen en tussen normen blootgelegd.

Voorbeeld Formulering

Voorbeeld objectenanalyse (Suwi-norm 5, Taskforce)

De Security Officer beheert en beheerst beveiligingsprocedures en maatregelen in het kader van Suwinet, *zodanig dat de beveiliging van Suwi overeenkomstig wettelijke eisen is geïmplementeerd.*

- De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert dat m.b.t. de beveiliging van Suwinet de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet
- De Security Officer rapporteert rechtstreeks aan het hoogste management

Voorbeeld objectenanalyse (Suwi-norm 5, Taskforce)

Wie/Wat

De Security Officer beheert en beheerst (formulieren) beveiligingsprocedures en maatregelen in het kader van Suwinet

Waarom

zodanig dat de beveiliging van Suwi overeenkomstig wettelijke eisen is geïmplementeerd

Formulieren (Security Officer, beveiligingsprocedures en maatregelen in het kader van Suwinet)

Voorbeeld objectenanalyse (Suwi-norm 5, Taskforce)

▪ De Security Officer :

- bevordert (?) en adviseert over de beveiliging van Suwinet,

adviseren (Security Officer, beveiliging van Suwinet)

1

5

- verzorgt rapportages over de status,

rapporteren (Security Officer, over de status beveiliging van Suwinet)

2

3

- controleert dat m.b.t. de beveiliging van Suwinet de maatregelen worden nageleefd,

controleren (Security Officer, naleving Suwinet maatregelen)

3

1

- evalueert de uitkomsten en

evalueren (Security Officer, uitkomsten)

4

2

- doet voorstellen tot implementatie

presenteren (Security Officer, verbetervoorstellen)

5

4

Voorbeeld: Formulering (SUWI-norm 5, Taskforce)

Informatiebeveiligingsfunctionaris – benoemen	
Criterion (wie en wat)	Er is een Security Officer benoemd met specifieke verantwoordelijkheid voor het formuleren van beleid, het adviseren over de beveiliging van de Suwinet, het controleren/evalueren van en rapporteren over de getroffen beveiligingsmaatregelen en presenteren van verbetervoorstellen.
Doelstelling (waarom)	Het zeker stellen dat effectieve en consistente informatiebeveiliging binnen de organisatie wordt geïmplementeerd.
Risico	<i>Het ontbreken van een Informatiebeveiligingsfunctionaris zal ertoe leiden dat informatiebeveiliging niet gecoördineerd plaatsvindt waardoor een variëteit aan beveiligingsmaatregelen worden getroffen. Dit zal leiden tot inconsistenties en kwetsbaarheden in de infrastructuur van de organisatie.</i>
Conformiteitsindicatoren	

Voorbeeld: Formulering

Beveiligingsfunctionaris – benoemen	
<i>Conformiteitsindicatoren</i>	
<u>Security Officer</u>	
01	<ul style="list-style-type: none">De Security Officer is adequaat in de organisatie gepositioneerd en rapporteert aan het hoogste management
02	<ul style="list-style-type: none">De taken en verantwoordelijkheden van de Security Officer zijn vastgelegd en vastgesteld.
<u>Formuleren</u>	
03	<ul style="list-style-type: none">De Security Officer formuleert beveiligingsrichtlijnen, procedures en instructies voor de implementatie van beveiligingsmaatregelen inzake het gebruik van Suwi-diensten
<u>Adviseren</u>	
04	<p>De Security Officer adviseert:</p> <ul style="list-style-type: none">de organisatie over de beveiliging van de koppeling tussen het netwerk van de organisatie en het Suwinet,het gebruik van gegevens van Suwinet vanuit IT omgeving van de organisatie,het gebruik van gegevens van Suwinet vanuit een “vreemde omgeving” (bijv. het gebruik van gegevens vanuit thuisituatie)

Voorbeeld: Formulering

Beveiligingsfunctionaris – benoemen	
<i>Conformiteitsindicatoren</i>	
<u>Controleren / Evalueren</u>	
06	De Security Officer : <ul style="list-style-type: none">• Controleert en evalueert de beveiliging van Suwinet of de getroffen maatregelen worden nageleefd,• Voert periodiek compliancy checks uit waarbij de getroffen maatregelen afgezet worden tegen de wet- en regelgeving
<u>Rapporteren</u>	
07	De Security Officer rapporteert evaluaties: <ul style="list-style-type: none">• over de getroffen beveiligingsmaatregelen .• over opgetreden security incidenten,• over de stand van zaken rond beveiligingsbewust zijn van gebruikers (eindgebruikers en beheerders) binnen de organisatie m.b.t. het gebruik van gegevens vanuit Suwinet.
<u>Presenteren</u>	
08	De Security Officer presenteert: <ul style="list-style-type: none">• verbeteringsvoorstellen

Onderzoeksvraag pilot ADR

*Verhoogt het toepassen van het SIVA-
raamwerk de kwaliteit van de normen?*



Ontwikkelfasen van een referentiekader

1. Analyseren en identificeren

2. Clusteren

3. Ordenen

4. Bewerken

5. Formuleren

Brainstorm- / Creatieve fase

Zoeken
naar
ontbrekende elementen
en
samenhang

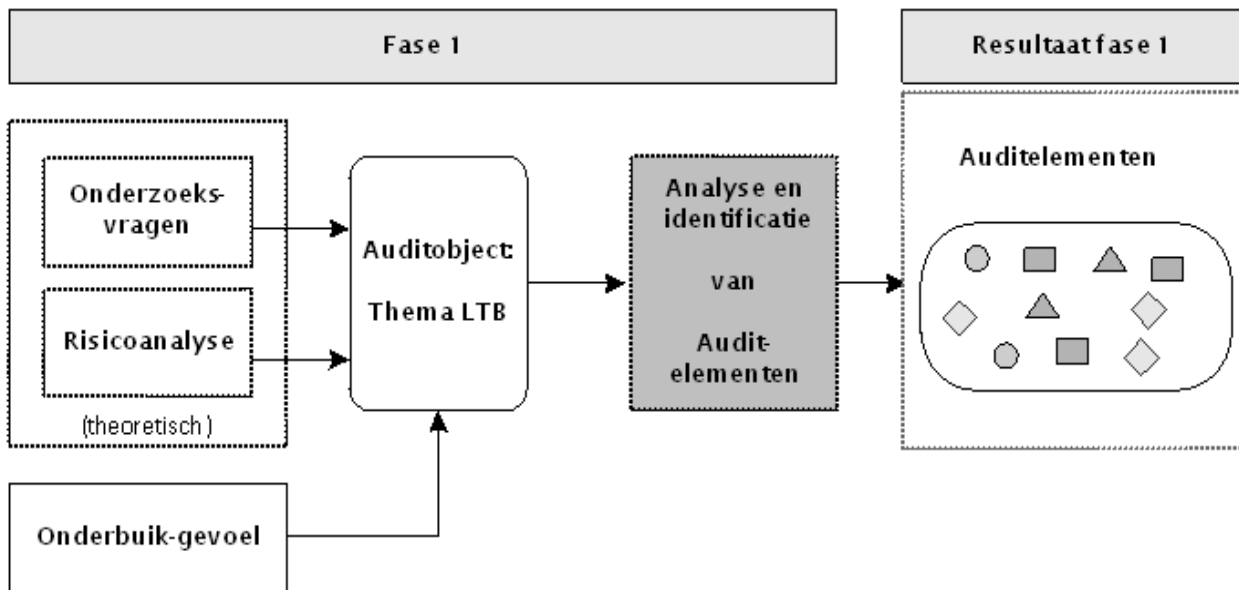
Definiëren van
Hoofd- en Subnormen

Normen DGOBR

Wat is de
samenhang?

Kan het beter?

Fase 1: Analyseren en identificeren van auditelementen



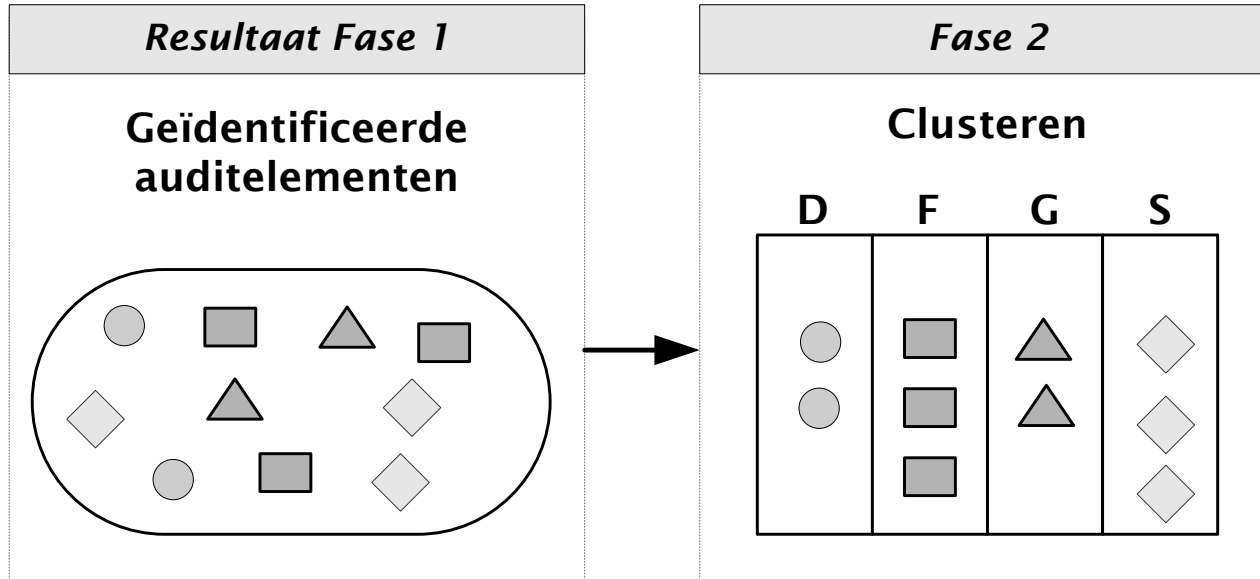
Fase 1: Auditelementen & LTB - BIR

Nr.	Geïdentificeerde auditelementen	
1	8.3.3	Blokkering van toegangsrechten (Autorisatieproces)
2	11.1.1	Toegangsvoorzieningsbeleid
3	11.2.1	Registratie van gebruikers (procedures)
4	11.2.2	Beheer van (speciale)bevoegdheden
5	11.2.3	Beheer van gebruikerswachtwoorden
6	11.2.4	Beoordeling van toegangsrechten
7	11.5.1	Beveiligde inlogprocedures
8	11.5.2	Gebruikersidentificatie en -authenticatie
9	11.6.1	Beperken van toegang tot informatie

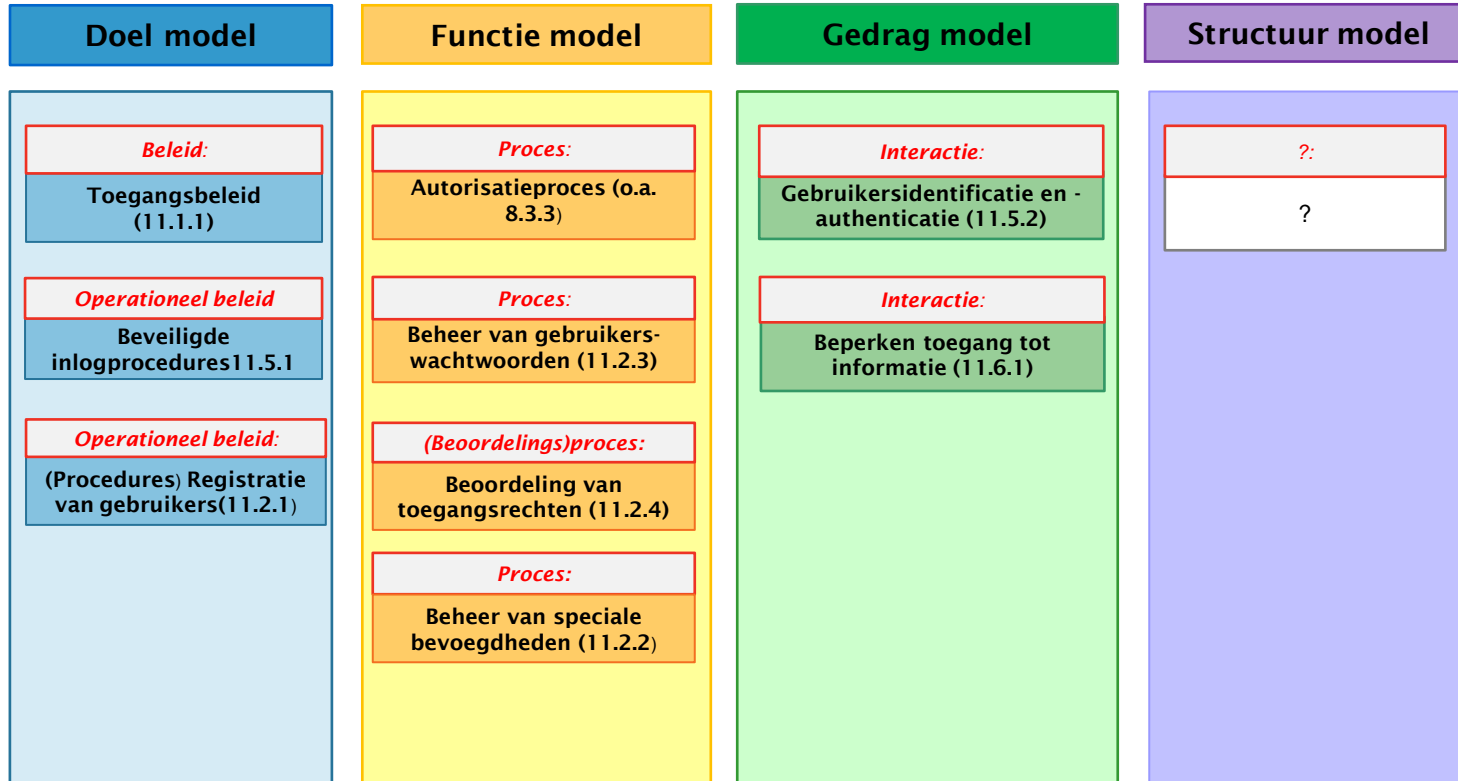
Basiselementen
Proces
Beleid
Beleid (Operationeel-B)
Proces
Proces
Proces (Controle-Proces)
Beleid (Operationeel-B)
Interactie (I & A)
Interactie (Aut.)



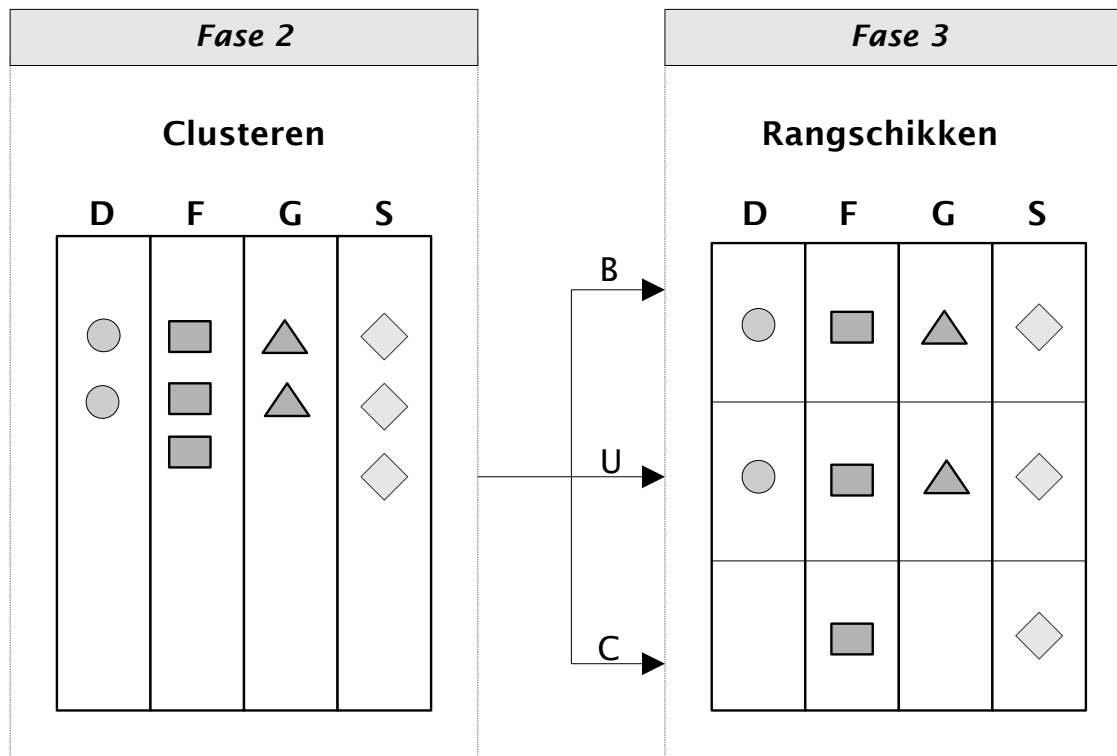
Fase 2: Clusteren van auditelementen



Fase 2: Clusteren van auditelementen van DGOBR



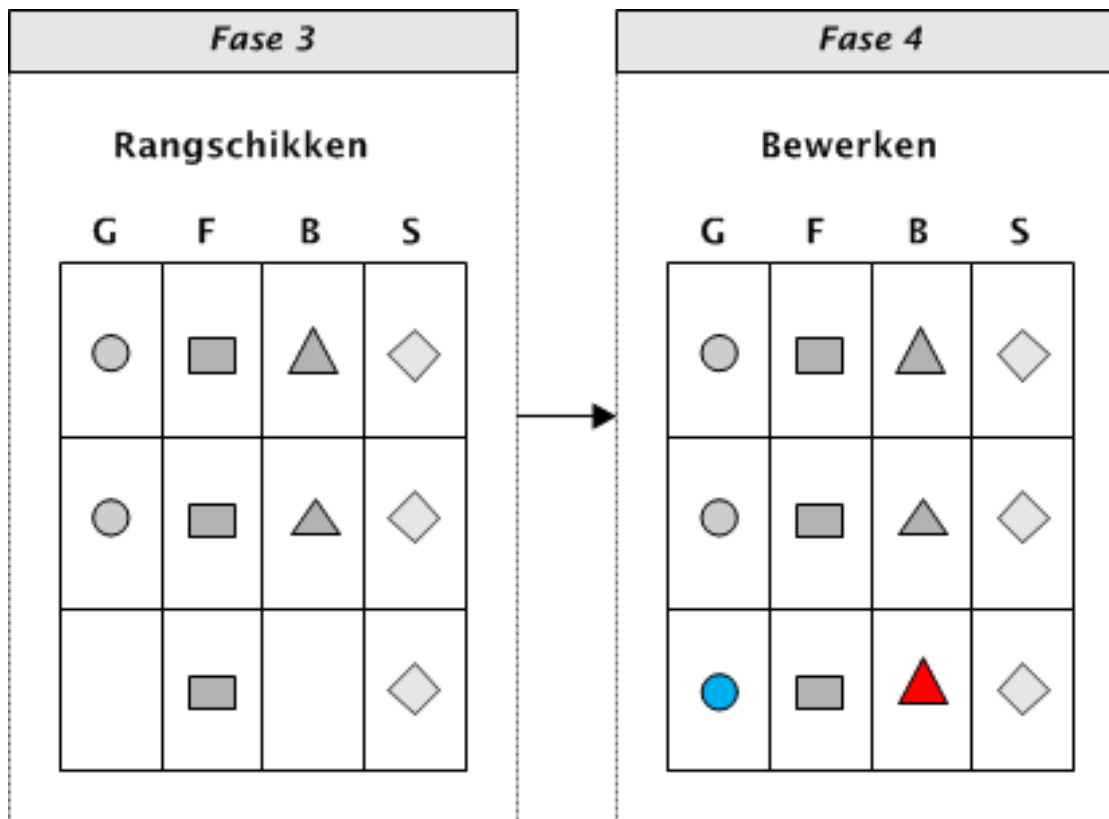
Fase 3: Ordenen van auditelementen



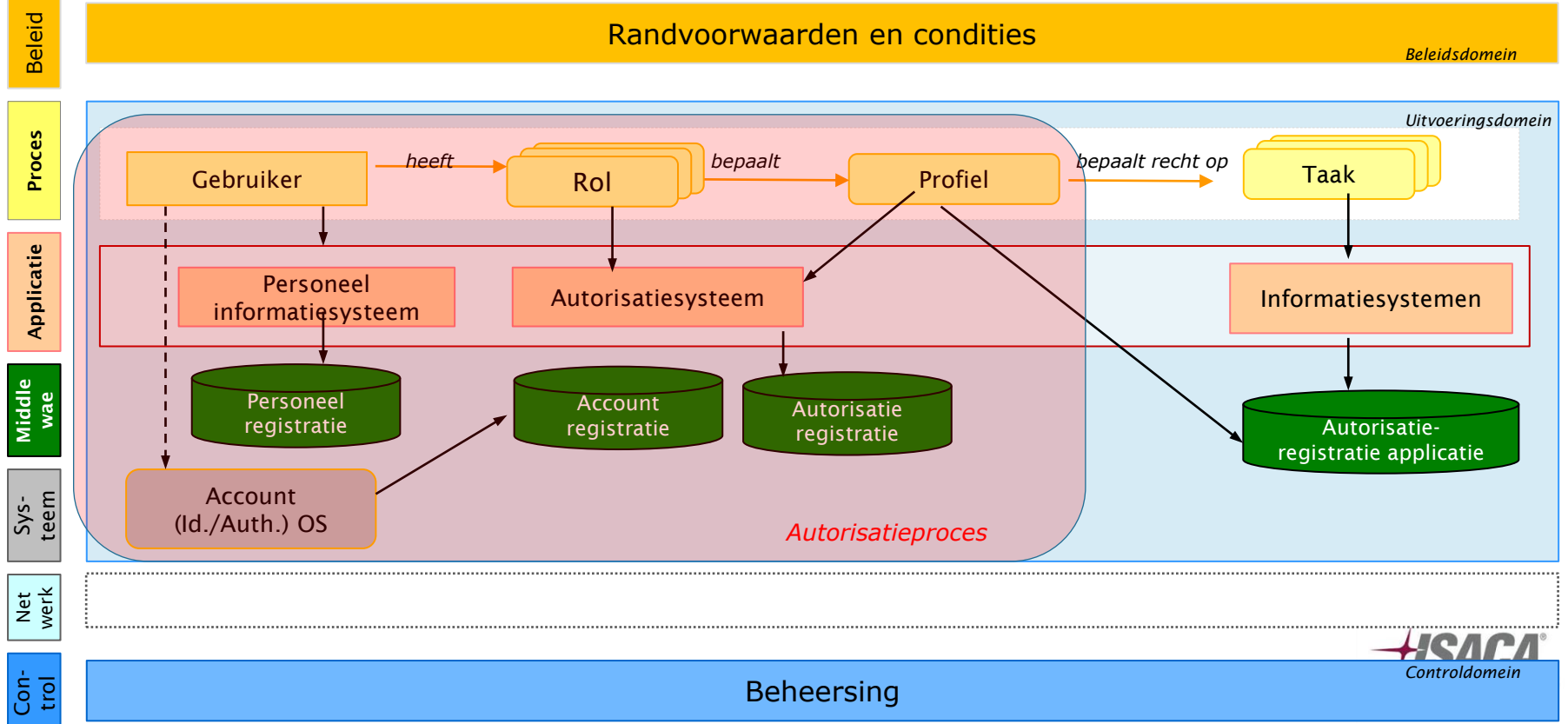
Fase 3: Ordenen van auditelementen van DGOBR

	Doel model	Functie model	Gedrag model	Structuur model
Beleids- domein	<p><i>Beleid:</i></p> <p>Toegangsbeleid (11.1.1)</p>	<p>?:</p> <p>?</p>	<p>?:</p> <p>?</p>	<p>?:</p> <p>?</p>
Uitvoeringsdomein	<p><i>Operationeel beleid:</i></p> <p>(Procedures) Registratie van gebruikers (11.1.1)</p> <p><i>Operationeel beleid:</i></p> <p>Beveiligde inlogprocedures 11.5.1</p>	<p><i>Proces:</i></p> <p>Autorisatieproces (o.a 8.3.3)</p> <p><i>Proces:</i></p> <p>Beheer van speciale bevoegdheden (11.2.2)</p> <p><i>Proces:</i></p> <p>Beheer van gebruikerswachtwoorden (11.2.3)</p>	<p><i>Interactie:</i></p> <p>Gebruikersidentificatie en -authenticatie (11.5.2)</p> <p><i>Interactie:</i></p> <p>Beperken toegang tot informatie (11.6.1)</p>	<p>?:</p> <p>?</p>
	Control domein	<p>?:</p> <p>?</p>	<p><i>Proces:</i></p> <p>Beoordeling van toegangsrechten (11.2.4)</p>	<p>?:</p> <p>?</p>

Fase 4: Bewerken



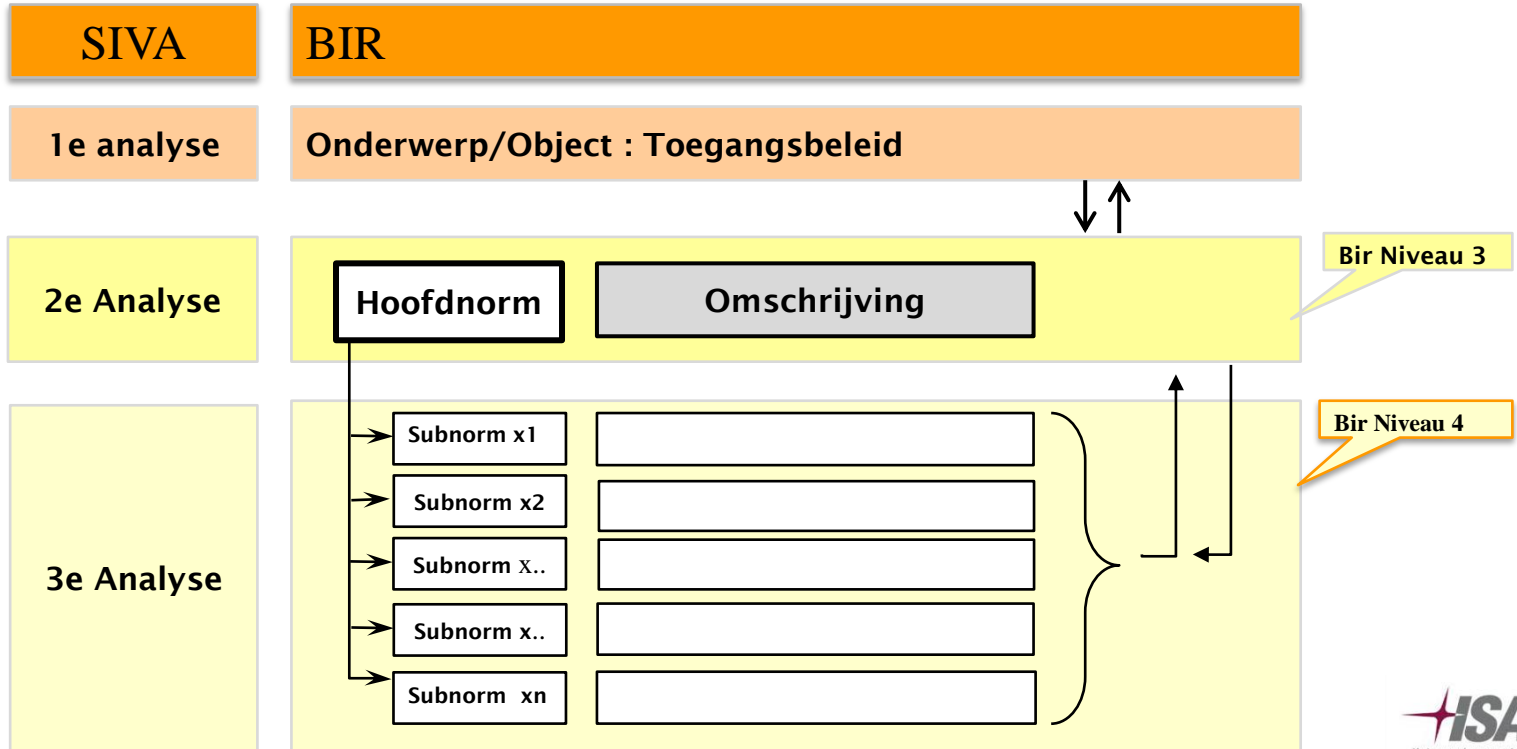
Overzicht Logische Toegangsvoorziening: Objecten



Fase 4: Bewerken van auditelementen van DGOBR

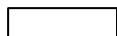





	Doel model	Functie model	Gedrag model	Structuur model
Beleids- domein	<p>Beleid:</p> <p>Toegangsbeleid (11.1.1)</p>	<p>Proces:</p> <p>Contractmanagement Toegangsvoorziening</p>	<p>Interactie:</p> <p>Beleid-Encryptie (Specials (I&A))</p>	<p>Architectuur:</p> <p>Autorisatiearchitectuur</p>
Uitvoeringsdomein	<p>Operationeelbeleid: (Procedures) Registratie van gebruikers (11.1.1)</p> <p>Operationeelbeleid: Beveiligde inlogprocedures 11.5.1</p>	<p>Proces: Autorisatieproces (o.a 8.3.3)</p> <p>Proces: Beheer van speciale bevoegdheden (11.2.2)</p> <p>Proces: Beheer van gebruikers-wachtwoorden (11.2.3)</p> <p>Taken: Taken, Verantwoordelijkheden en Bevoegdheden LTB</p> <p>Taakvereisten: Functie scheidingen LTB</p>	<p>Interactie: Gebruikersidentificatie en - authenticatie (11.5.2)</p> <p>Interactie: Beperken toegang tot informatie (11.6.1)</p> <p>Historie: Logging</p>	<p>Architectuur: Autorisatiemiddelen</p>
	Control domein	<p>Beleid:</p> <p>Beoordelingsrichtlijnen en Procedures</p>	<p>proces</p> <p>Beoordeling van toegangsrechten (11.2.4)</p>	<p>Historie:</p> <p>Analyse Logging en Monitoring</p>

Fase 5: Formuleren



Bevindingen

	Hoofdnorm	Hoofdnorm vs Subnormen	Hoofdnorm vs Subnormen	Hoofdnorm vs Subnormen	Hoofdnormen vs R normen
→	Subnorm x1				
→	Subnorm x2				
→	Subnorm x3				
→	Subnorm x4				
→	Subnorm x5				
→	Subnorm x6				

-  Geen subnormen vermeld
-  Juiste subnormen vermeld
-  Ontbrekende subnormen, hoofdnorm niet geheel afgedekt door subnormen
-  Subnormen die niet gerelateerd zijn aan de hoofdnorm
-  Juist toegevoegde R-normen als aanvulling bij de hoofdnorm
-  Toegevoegde R-normen niet gerelateerd aan de hoofdnorm

Bevindingen bij de pilot

- Identificeren van tekortkomingen
 - helpt tekortkomingen in de formuleringen duidelijk te maken
- Link hoofdnorm en subnormen
 - legt een directe link naar onderliggende normen en maatregelen.
- Matching van normenkaders en verhoudingen normenkaders
 - maakt matching van normenkaders mogelijk .
 - kan de duidelijkheid in de verhouding tussen normenkaders vergroten
- Acceptatie resultaten
 - kan de acceptatie van resultaten uit audit door gebruikers vergroten
- Structuur en schrijfwijze
 - bevordert efficiëntie door indeling en schrijfwijze en brengt de single audit gedachte dichterbij.
- Volwassenheid
 - bevordert de volwassenheid in het bereiken van implementatie van maatregelen.

Aanbeveling t.a.v. BIR

- Verbreed thema gewijze benadering naar gehele BIR
 - Makkelijker koppelen aan een eigenaar
 - Geeft herkenbare structuur (opdrachtgever, gebruiker, auditor)
 - Makkelijker afstemmen normenkaders door beleidsmakers en eigenaren
 - Effectiever
 - Efficiënter
 - Creëert een groeimodel naar een BIO en daarmee naar single audit filosofie
- Houd vast aan ISO want herkenbare wereldstandaard,
- Repareer tekortkomingen ISO-standaard d.m.v. thema's

Cobit IT Governance

Toepassing van het Cobit

□ Vragen

- Waar in Nederland wordt het toegepast?, Welke organisaties?
- Wordt het toegepast in overheidsland ?

□ Waarom niet?

- Wat zijn de nadelen.
- Zijn er organisaties die daar bepaalde redenen voor opgeven?

Toepassing van Cobit

❑ Kunnen meer organisaties toepassen?

- Ja,..
- Verminder de complexiteit
- Maak gebruik van de sterke punten

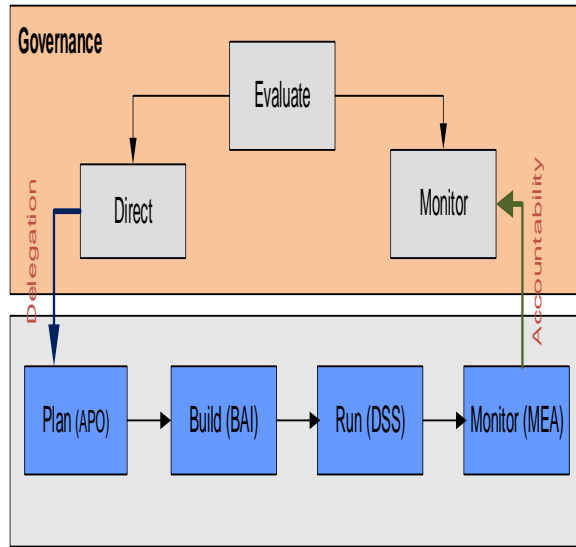
❑ Wat zijn de sterke punten

- Governance benadering (onderscheid governance- en management body)
- Gelaagde structuur (systeem benadering)
- Vaak gebruikt als legitimering van de gekozen processen/objecten
-

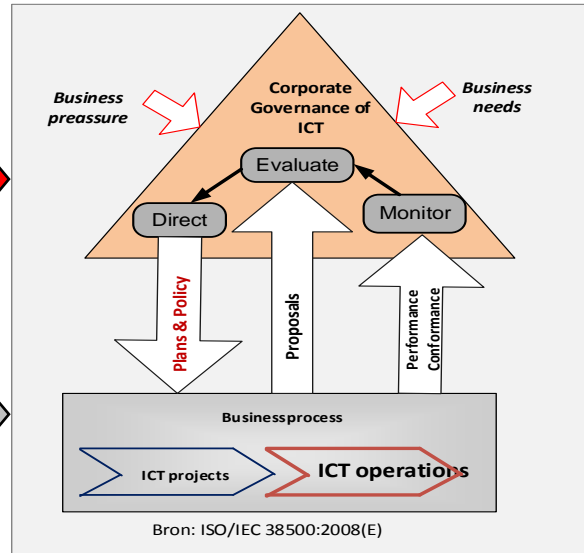
❑ Vraag

Wil je cobit gebruiken als leidraad of reglement /richtlijn ?

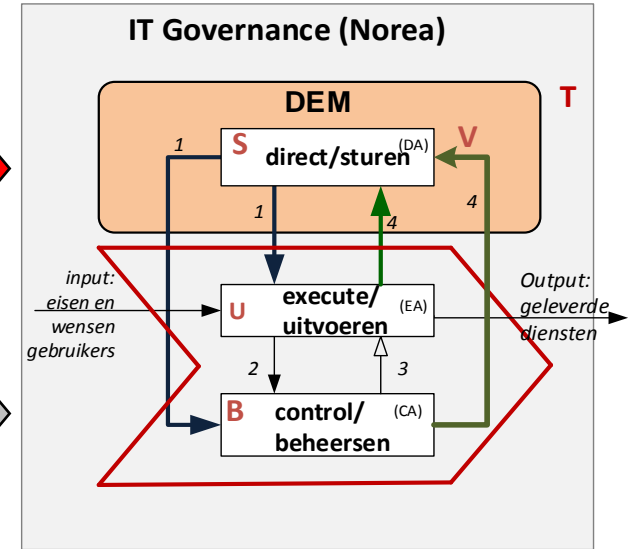
Governance modellen



Bron: ISACA/COBIT



Bron: ISO/IEC 38500:2008(E)



Cobit processen

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI10 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

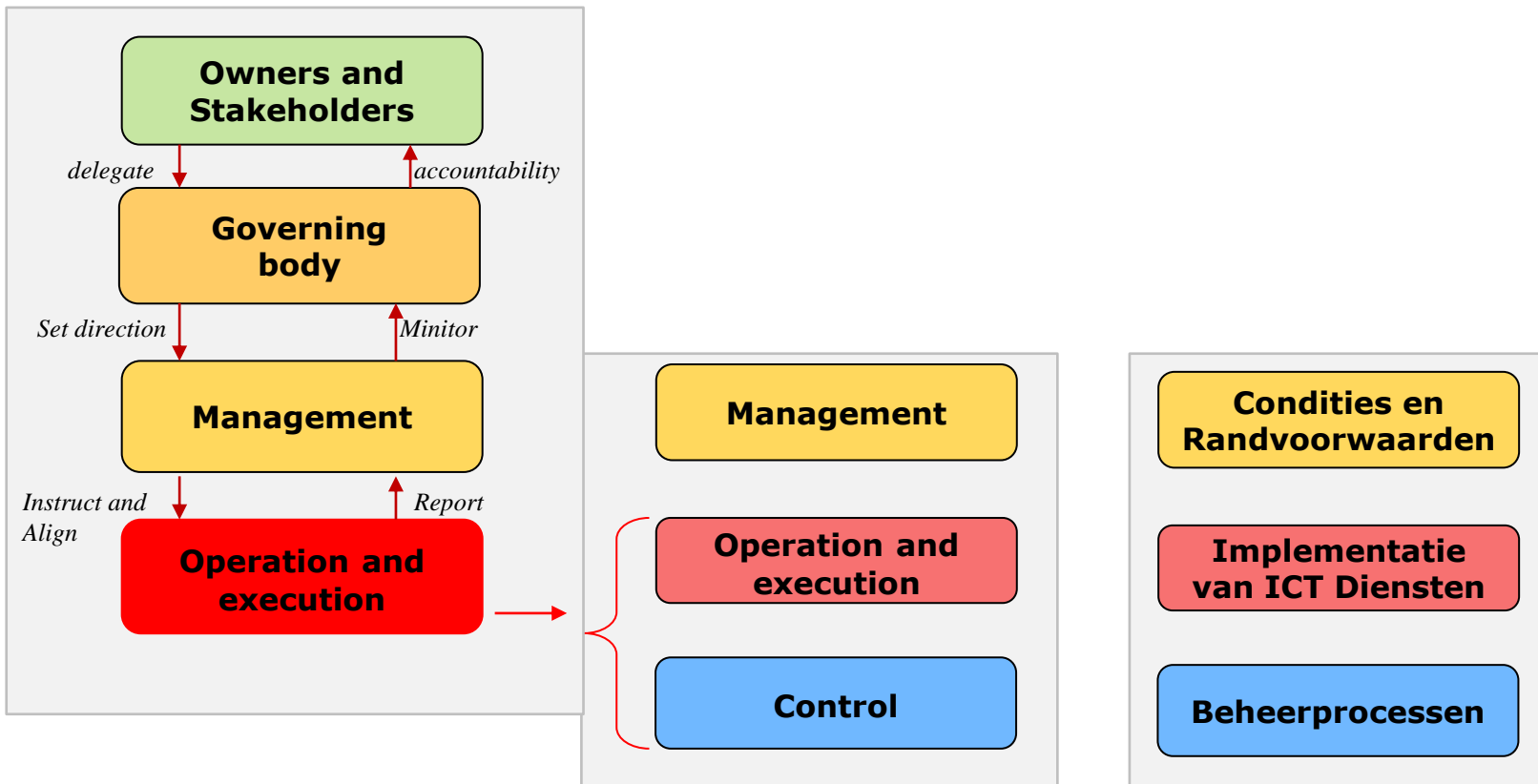
MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Rollen en activiteiten/ uitwerken per thema



Rollen en activiteiten/ uitwerken per thema

APO02 Manage Strategy

....

Implementaties ICT diensten

DSS05 Manage Service security

Identity en Logical Access

Infrastructure

Beheerprocessen

BAI04 Manage Availability and Capacity

BAI06 Manage Changes

BAI10 Manage Configuration

DSS03 Manage Problem

....

Vragen



Bedankt

Voor meer informatie kun je contact opnemen met:

Wiekram Tewarie – wiekram.tewarie@uwv.nl

Michiel Oosterwijk – michiel.oosterwijk@ncsc.nl

Kees van der Maarel – c.p.j.maarel@minfin.nl

© NOREA / ISACA

24 september 2015


Vertrouwen in en waarde uit Informatiesystemen
Netherlands Chapter


DE BEROEPSORGANISATIE VAN IT-AUDITORS