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

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Vragen in de praktijk

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

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

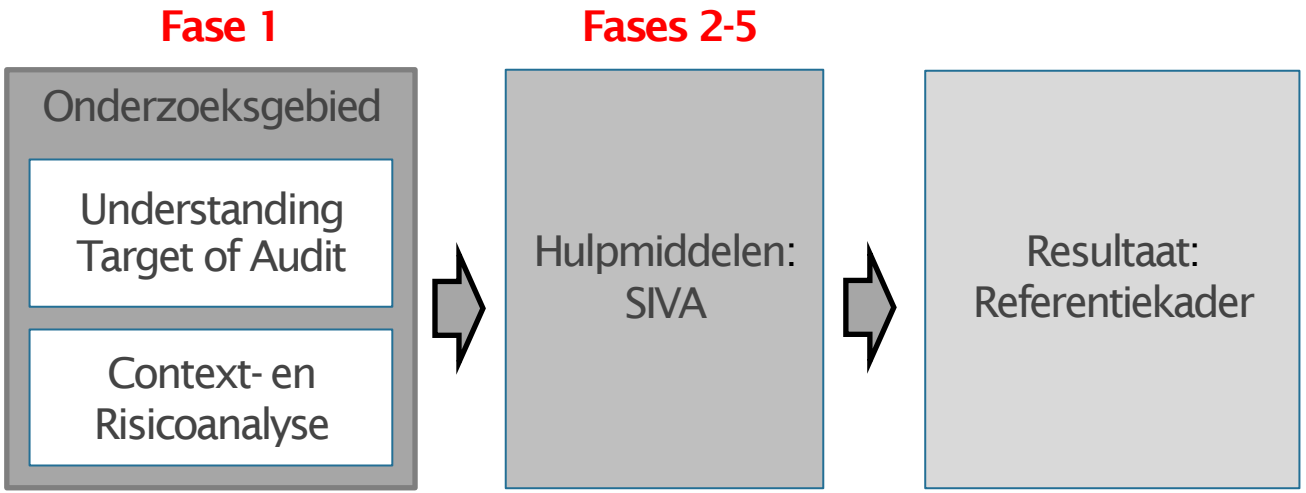
Ontwikkelfasen van een referentiekader

1. Analyseren en identificeren	Brainstorm-/ Creatieve fase
2. Clusteren 3. Ordenen 4. Bewerken	Zoeken naar ontbrekende elementen en samenhang
5. Formuleren	Definiëren van Hoofd- en Subnormen

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

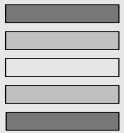
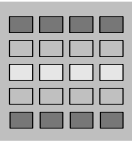
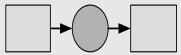
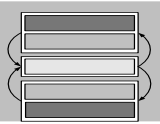
Hulpmiddelen: Raamwerk



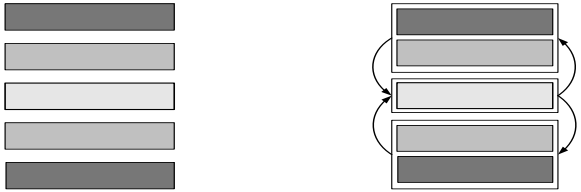
ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

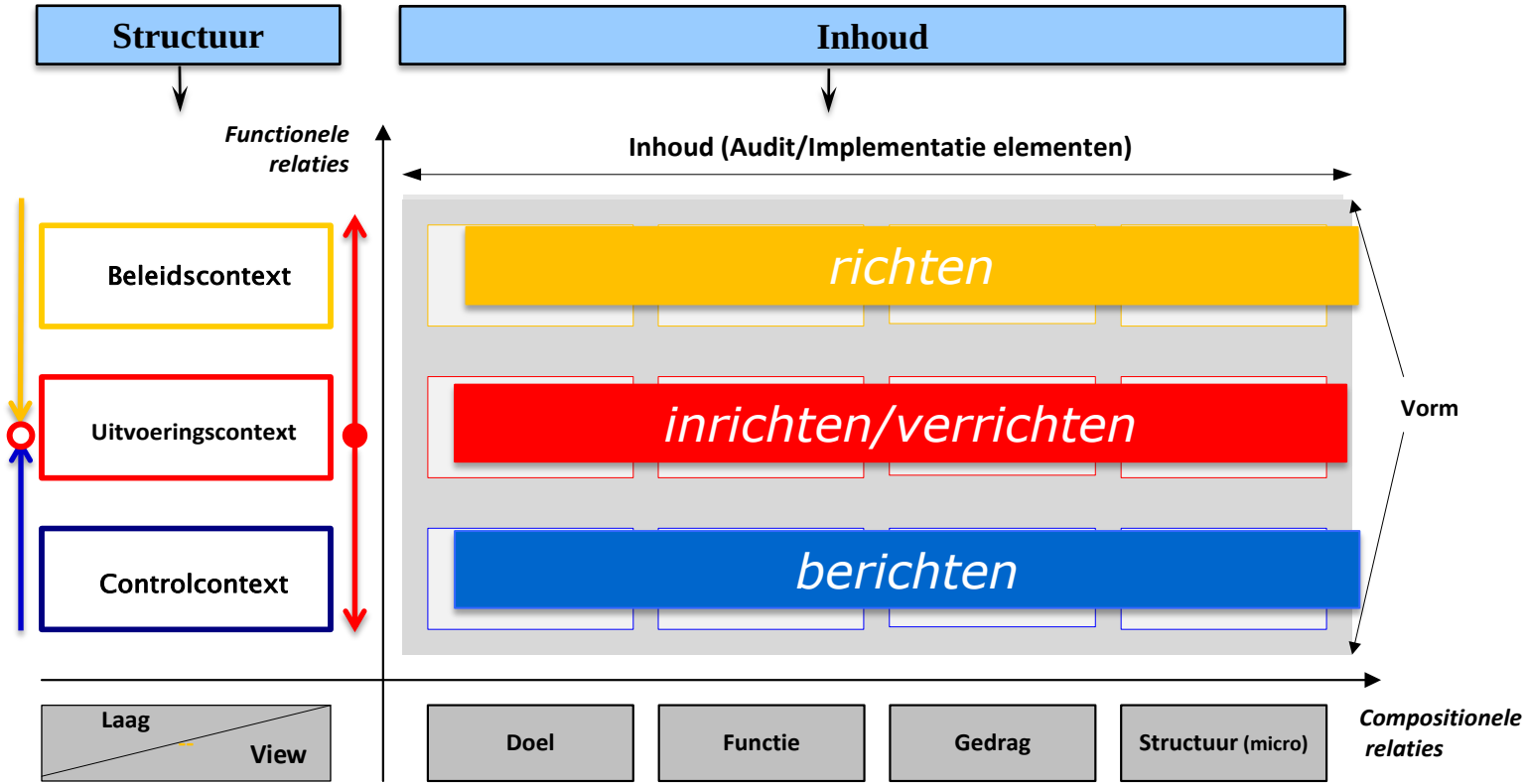
Hulpmiddelen: Raamwerk

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

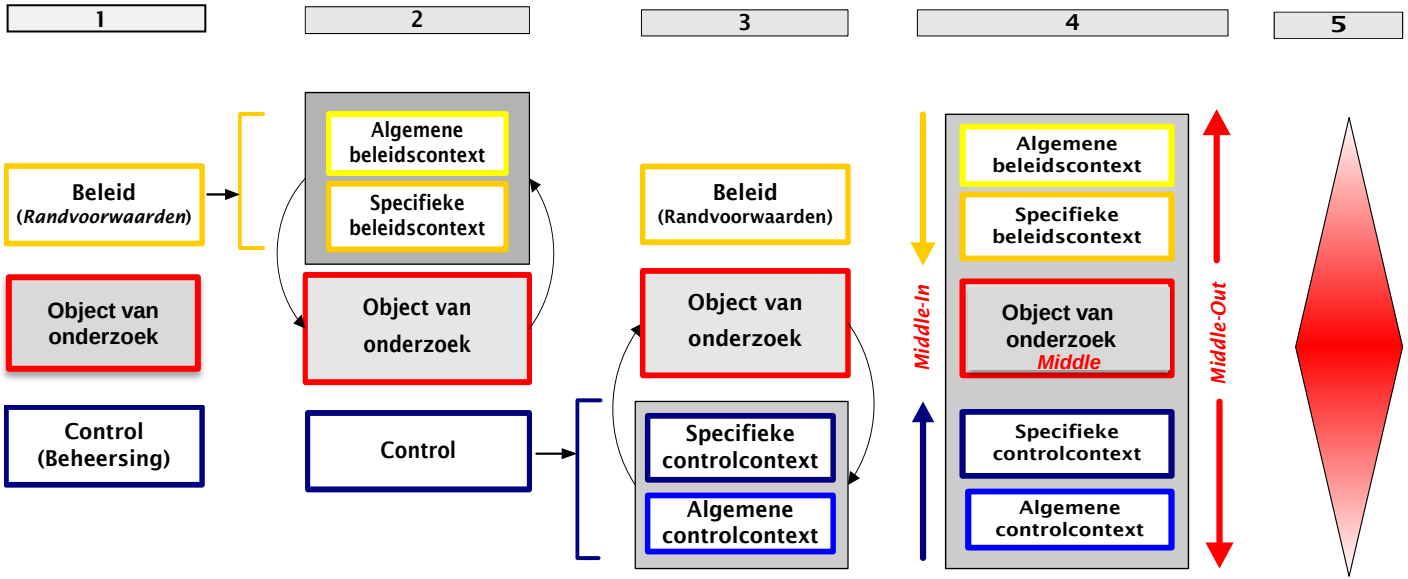
Structuur en Volgorde



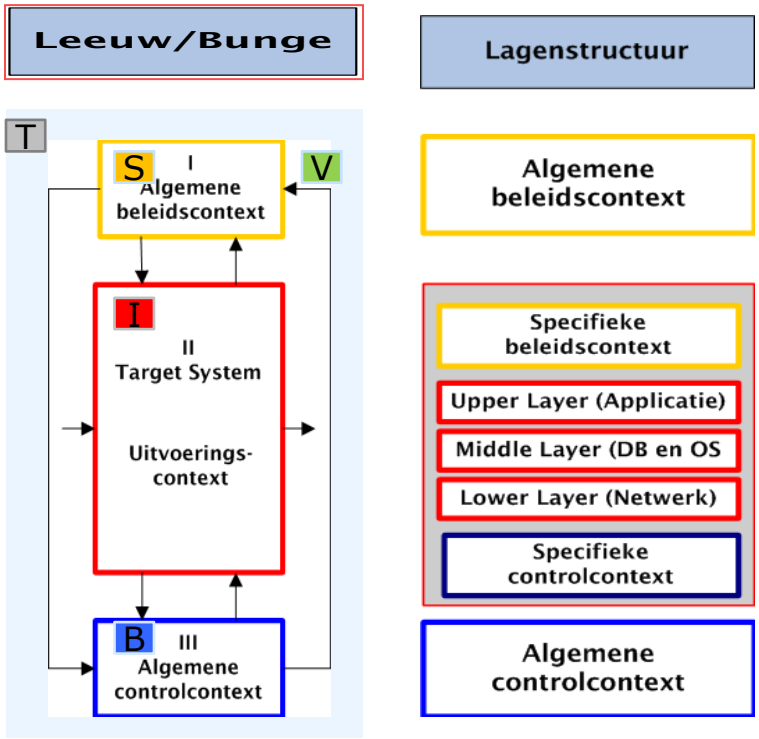
SIVA-raamwerk: Structuur, Inhoud, Vorm en Analysevolgorde



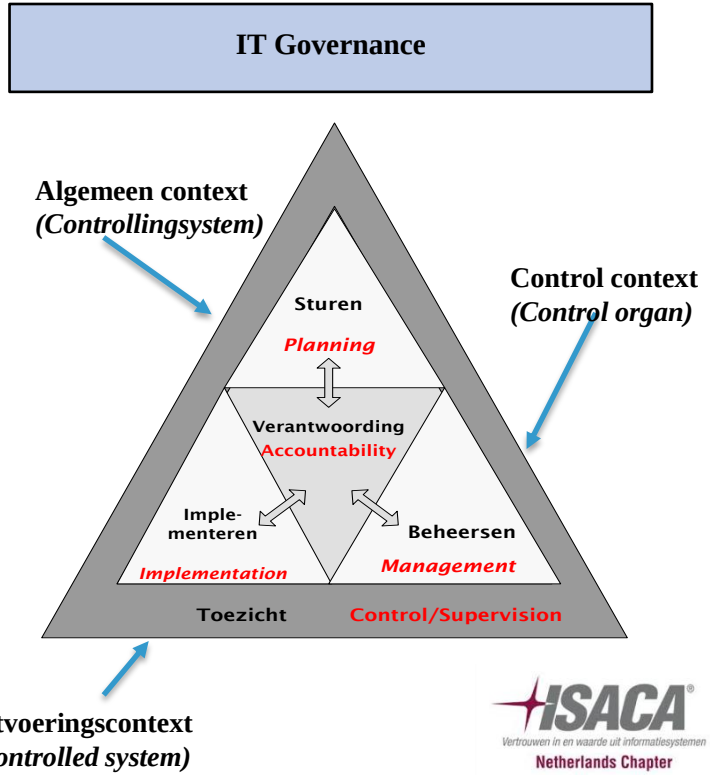
Structuur (Macro)



Structuur



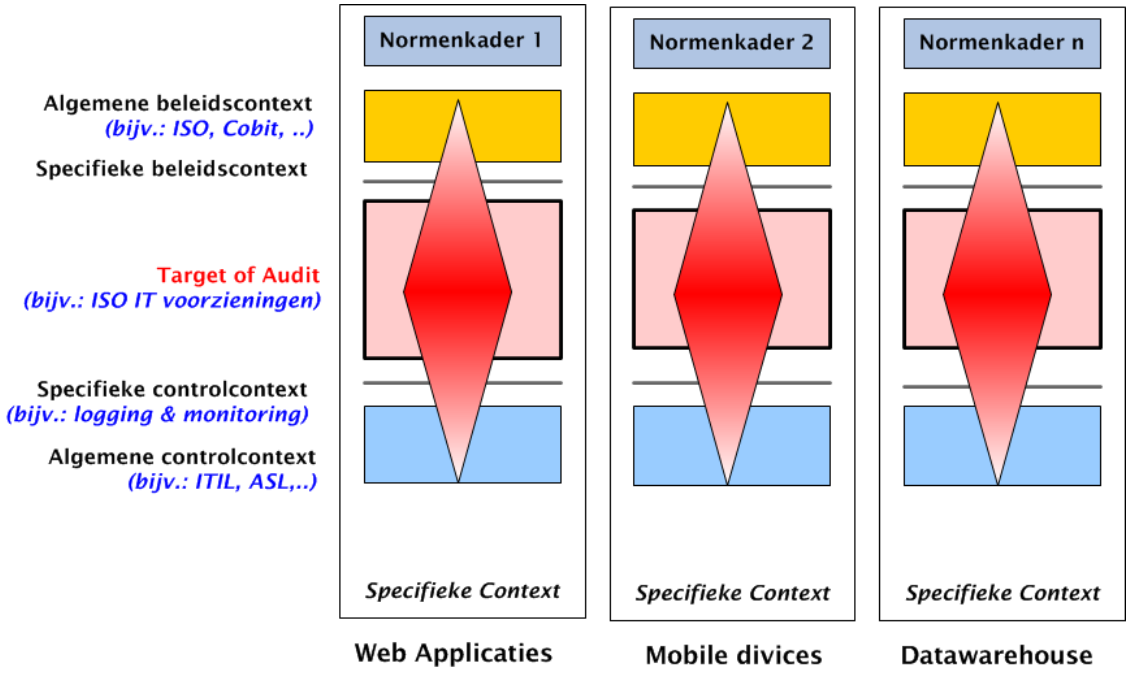
adresseert governance aspecten



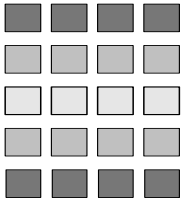
ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Gelijkvormige normenkaders



Inhoud



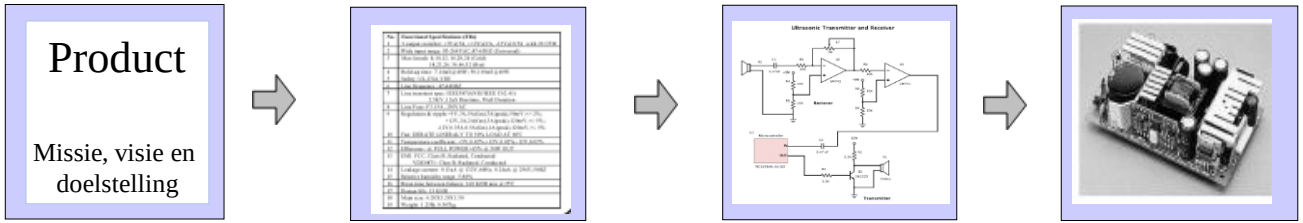
Inhoud (DFGS invalshoeken)

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

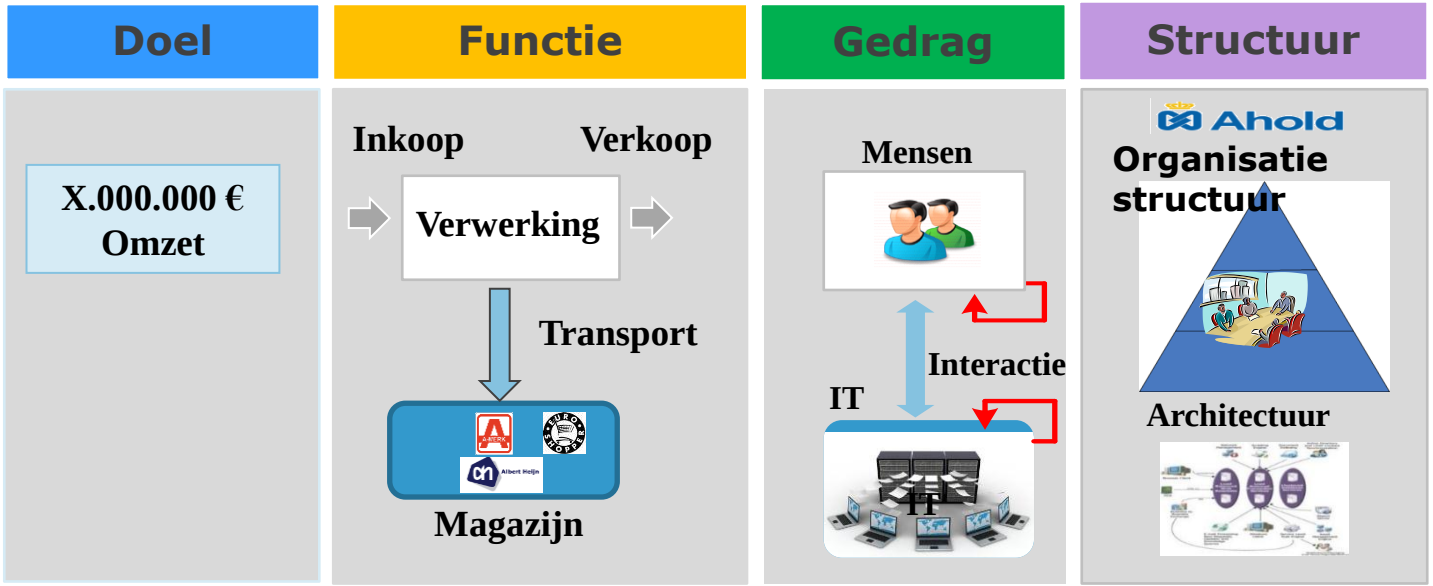
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

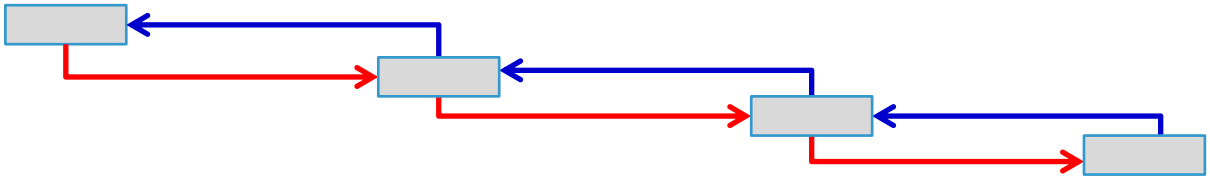
Toelichting (DFGS invalshoeken: Techniek)

Doel (Waarom)	**Functie** (Wat)	**Gedrag** (Hoe)	**Structuur** (Hoe)
Ontwikkelen van een apparaat	Wat gaat het apparaat doen, Welke functies	Hoe, in de vorm van technische specifcatie	Hoe, in de vorm van structuur

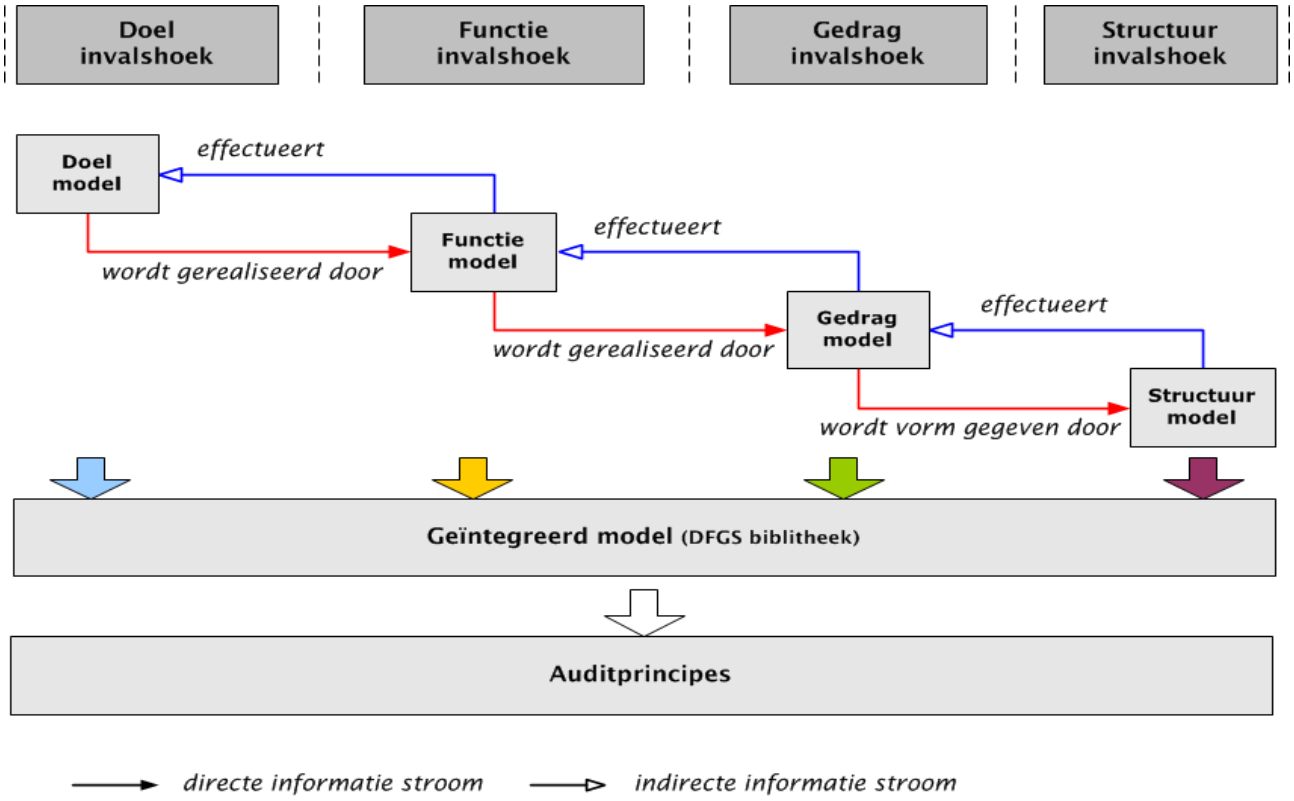


Toelichting (DFGS invalshoeken: organisatie)





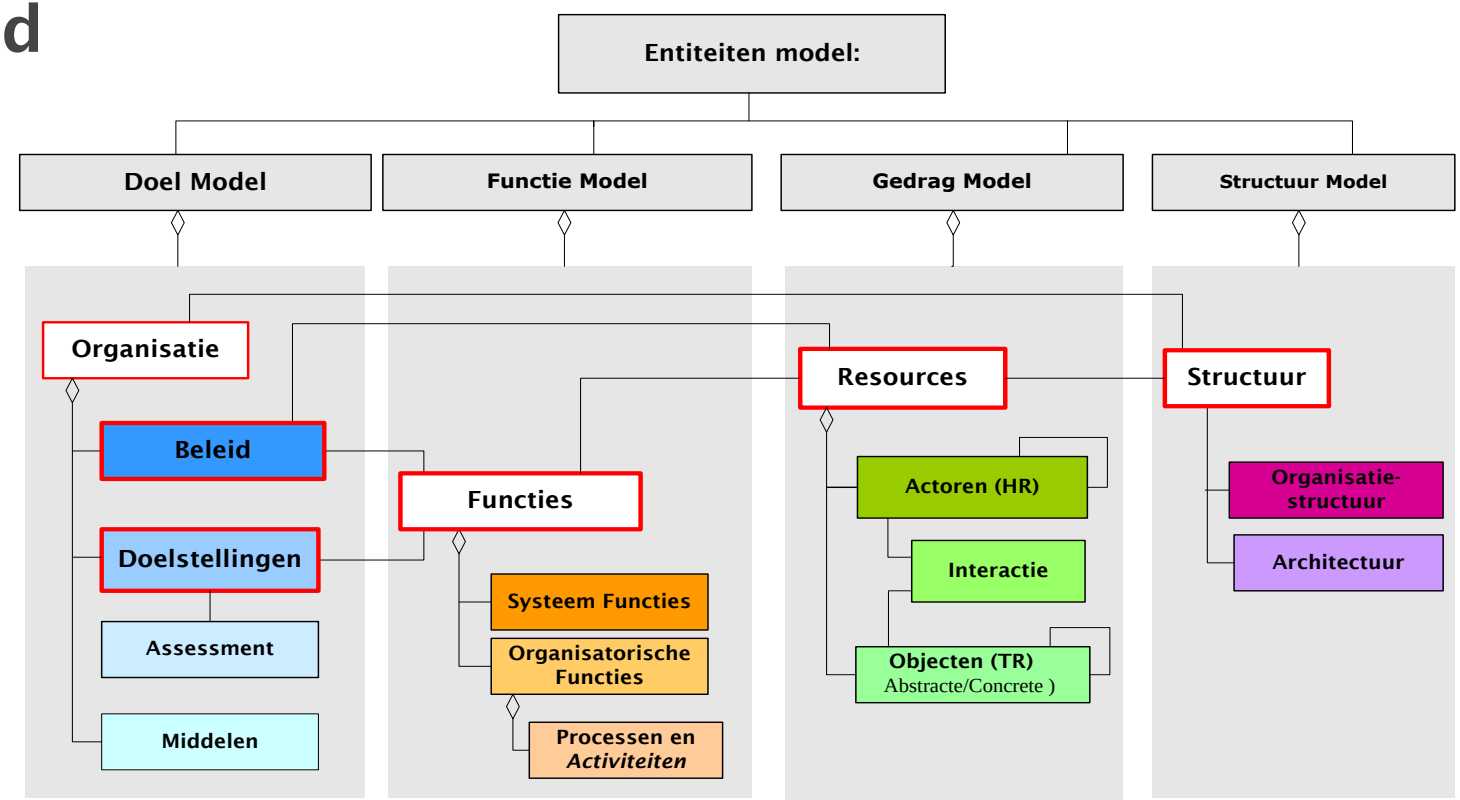
Inhoud



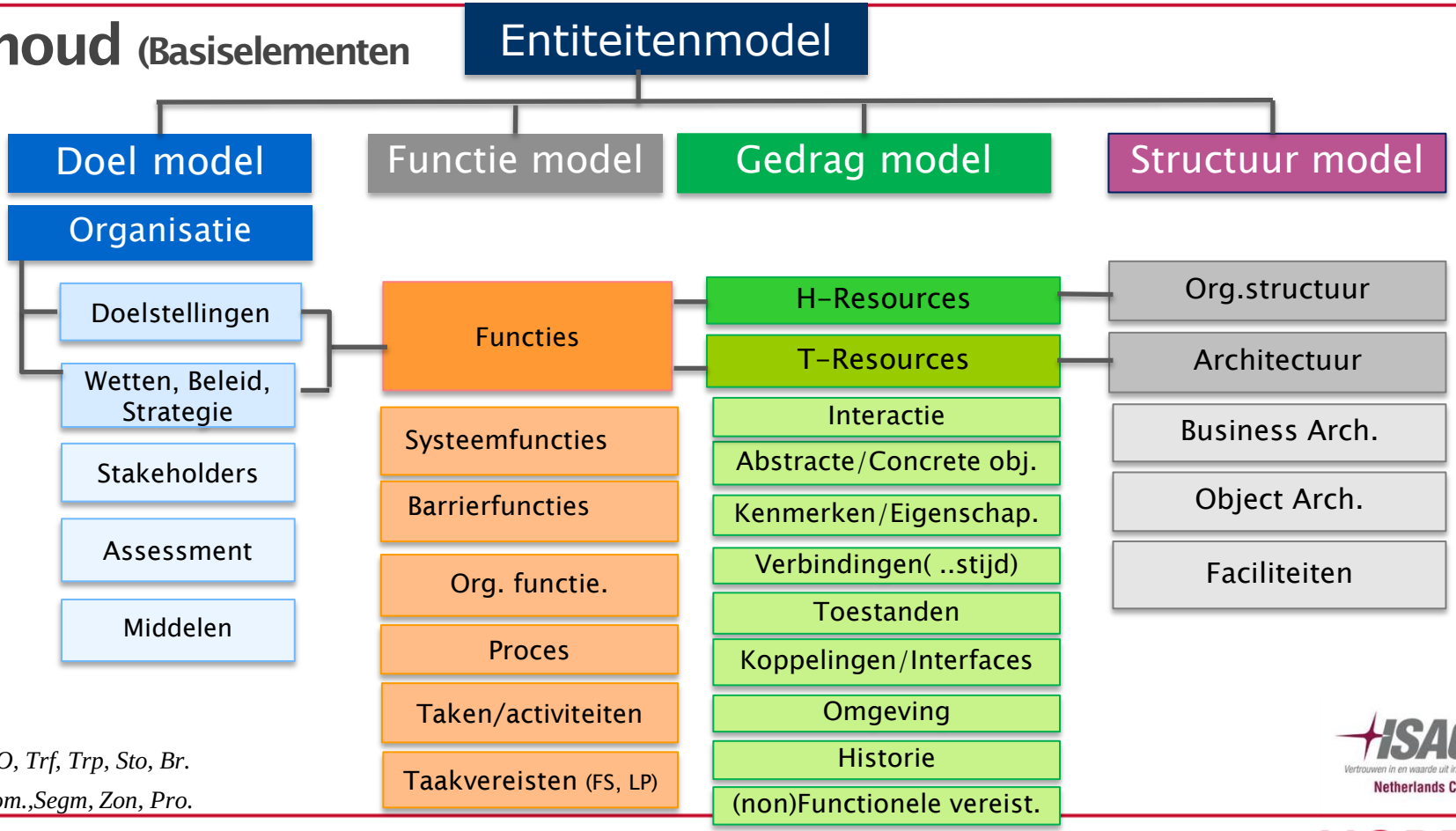
ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Inhoud


Entiteiten model:
Doel Model
Functie Model
Gedrag Model
Structuur Model
Organisatie
Beleid
Doelstellingen
Assessment
Middelen
Functies
Systeem Functies
Organisatorische Functies
Processen en Activiteiten
Resources
Actoren (HR)
Interactie
Objecten (TR)
Abstracte/Concrete)
Structuur
Organisatie-structuur
Architectuur

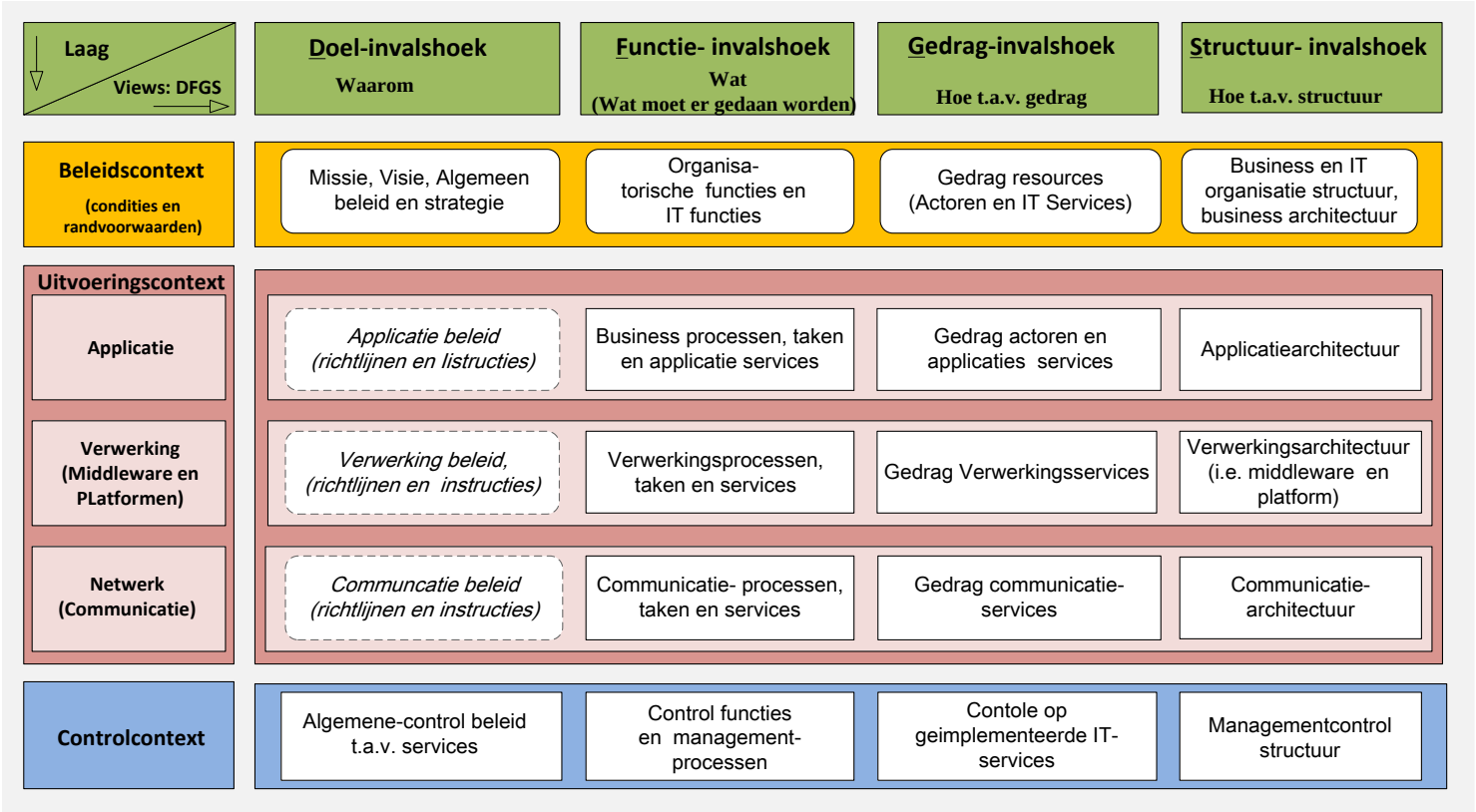
Inhoud (Basiselementen



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

Br = Com.,Segm, Zon, Pro.

Structuur-Inhoud matrix



ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Oordeelsvorming

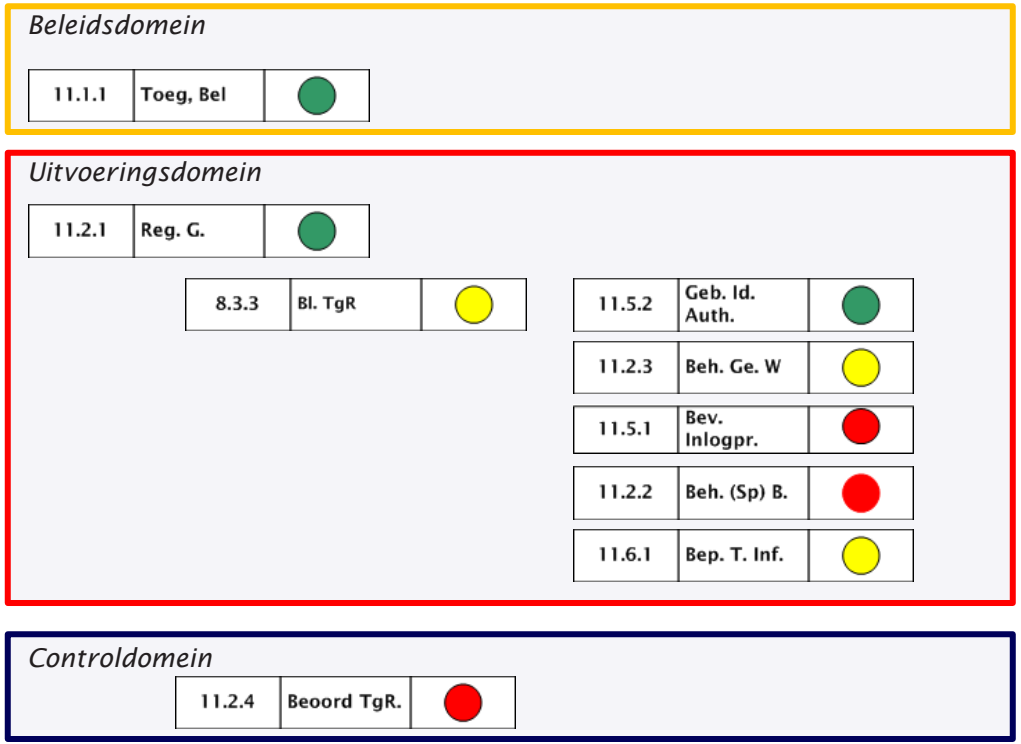
ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

Oordeelsvorming (Lijst)

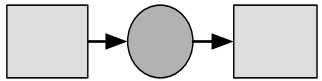
Nummer	Nummer BIR.	Onderwerpen BIR.	Oordeels -vorming
1	8.3.3	Blokkering van toegangsrechten	
2	11.1.1	Toegangsbeleid	
3	11.2.1	Registratie van gebruikers	
4	11.2.2	Beheer van (speciale) bevoegdheden	
5	11.2.3	Beheer van gebruikerswachtwoorden	
6	11.2.4	Beoordeling van toegangsrechten	
7	11.5.1	Beveiligde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

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

Oordeelsvorming (Lijst)



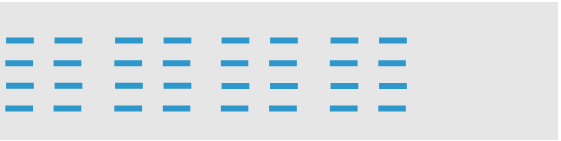
Vorm



Normen uit baselines/Best practices

Beheersmaatregel

Implementatierichtlijnen

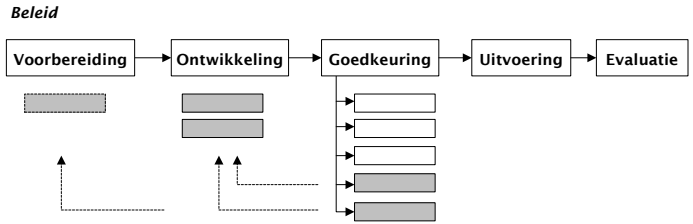


Verband ??

Voorbeeld ISO Norm

Beheersmaatregel

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



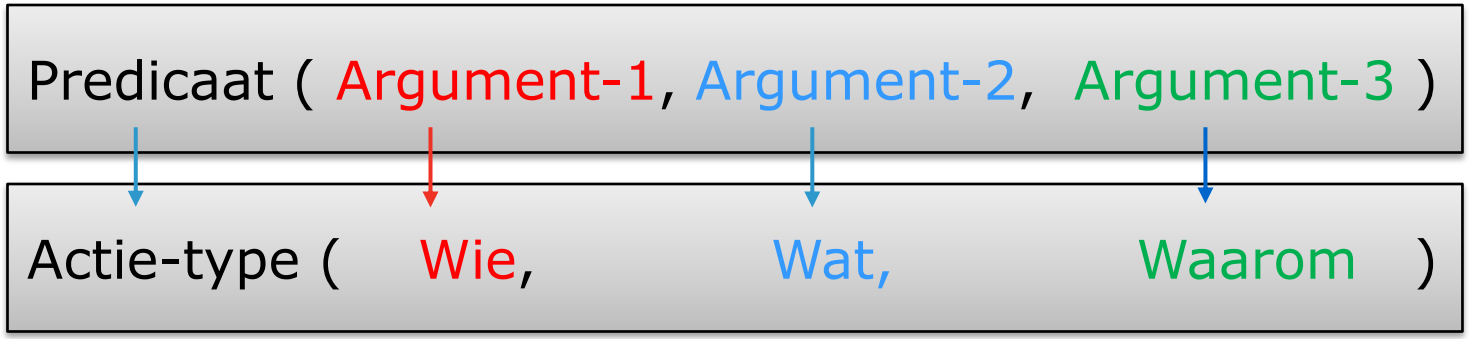
Implementatierichtlijnen

- 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

ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

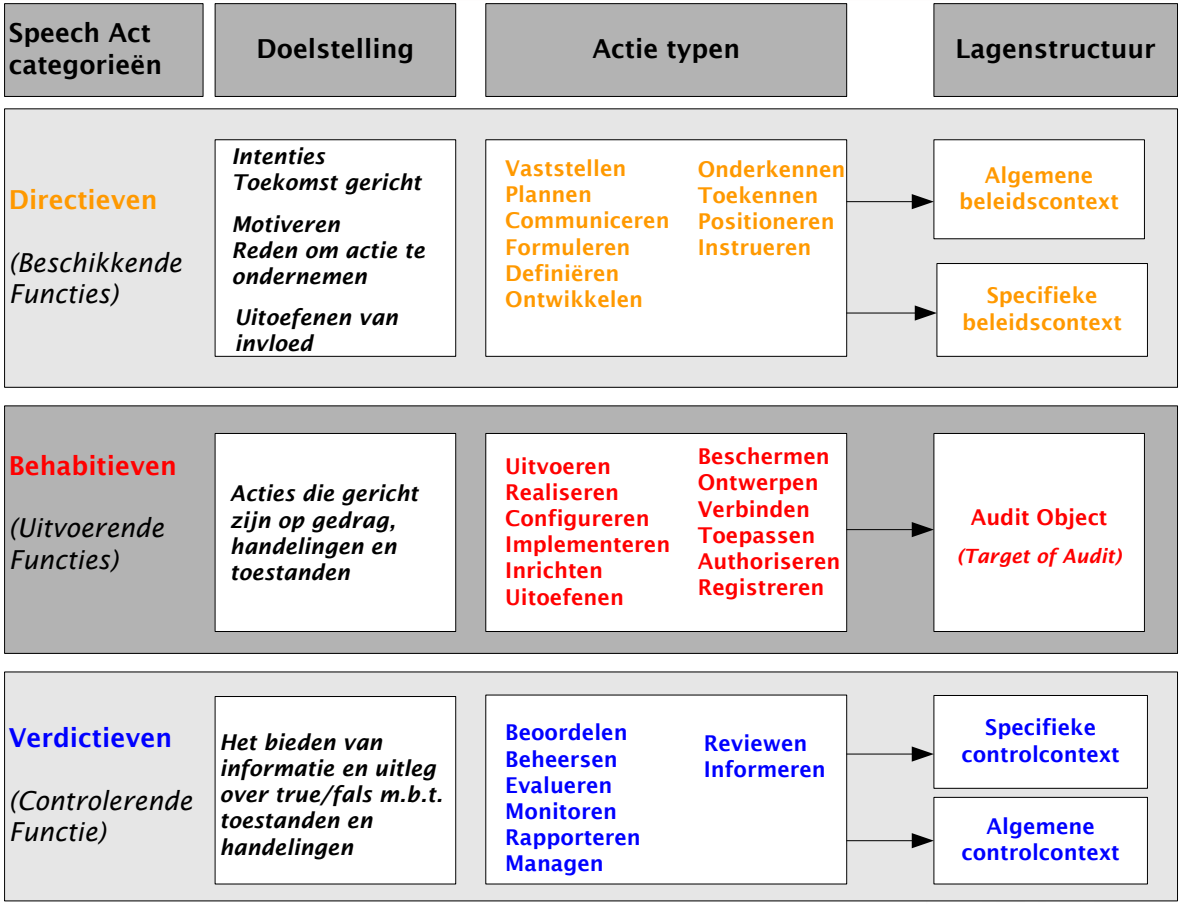
NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Vorm


Predicaat (Argument-1, Argument-2, Argument-3)
Actie-type (Wie, Wat, Waarom)

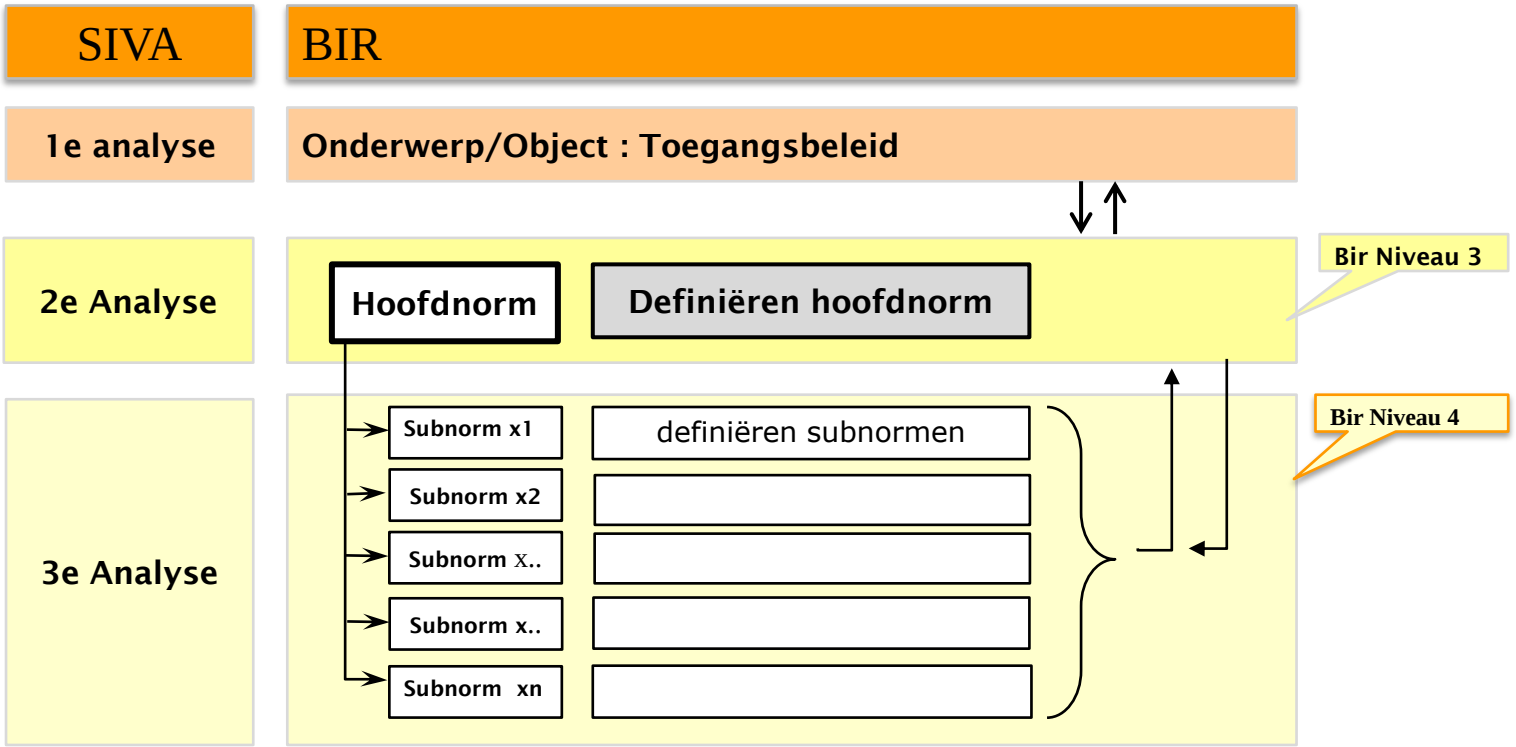
Vorm (Formuleringstemplate)

Vorm (Actie-typen)



Fase 5: Formuleren

Principes en gerelateerde maatregelen (Relatie : HN en SN)



ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

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.

ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

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

ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Voorbeeld objectenanalyse (Suwi-norm 5, Taskforce)

Wie/Wat
De Security Officer beheert en beheerst (formuleren)
beveiligingsprocedures en maatregelen in het kader van Suwinet

Waarom
zodanig dat de beveiliging van Suwi overeenkomstig wettelijke eisen is geïmplementeerd

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

ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

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

ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Voorbeeld: Formulering (SUWI-norm 5, Taskforce)

Informatiebeveiligingsfunctionaris – benoemen	
Criterium (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	*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*.
Conformiteitsindicatoren	

Voorbeeld: Formulering

Beveiligingsfunctionaris – benoemen	
Conformiteitsindicatoren	
Security Officer	
01	• De Security Officer is adequaat in de organisatie gepositioneerd en rapporteert aan het hoogste management
02	• De taken en verantwoordelijkheden van de Security Officer zijn vastgelegd en vastgesteld.
Formuleren	
03	• De Security Officer formuleert beveiligingsrichtlijnen, procedures en instructies voor de implementatie van beveiligingsmaatregelen inzake het gebruik van Suwi-diensten
Adviseren	
04	De Security Officer adviseert: • 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 thuissituatie)

Voorbeeld: Formulering

Beveiligingsfunctionaris – benoemen	
Conformiteitsindicatoren	
Controleren /Evalueren	
06	De Security Officer : • 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
Rapporteren	
07	De Security Officer rapporteert evaluaties: • 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.
Presenteren	
08	De Security Officer presenteert: • verbeteringsvoorstellen

Onderzoeksvraag pilot ADR

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

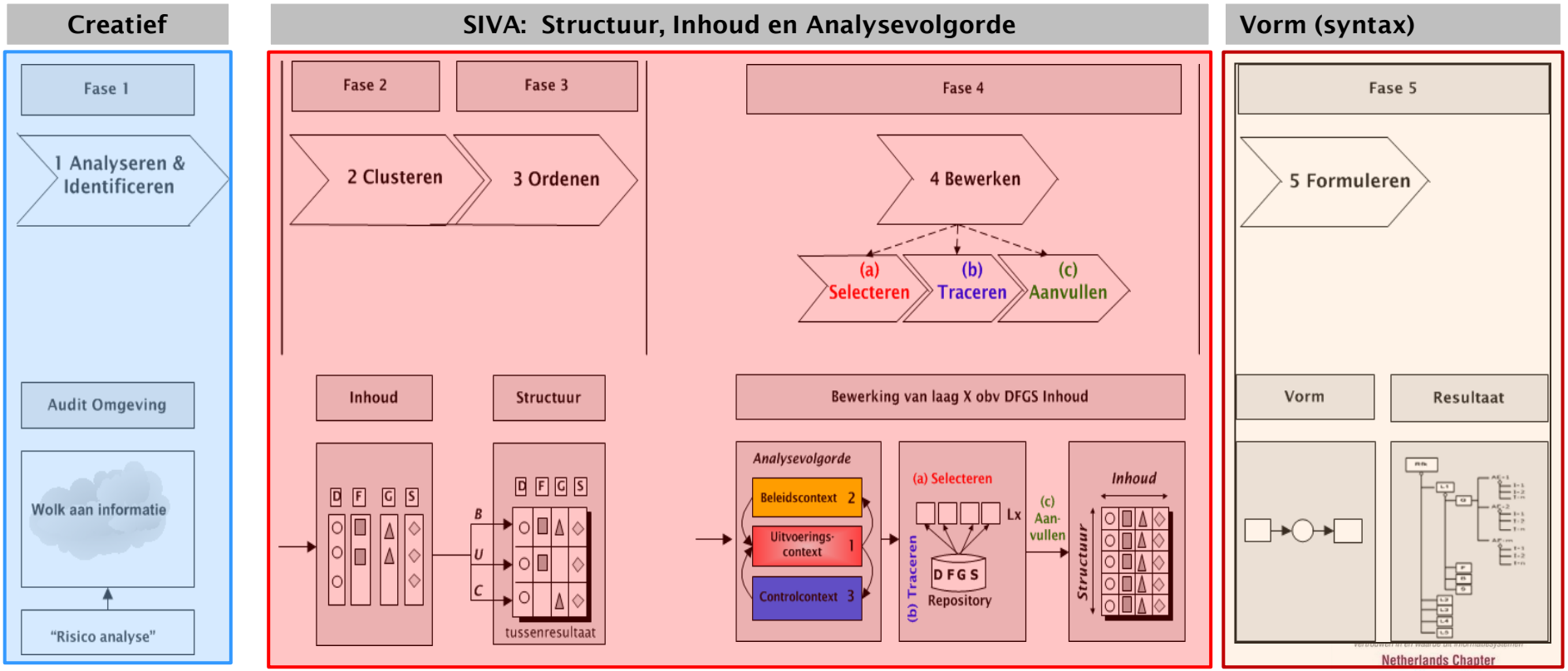
Ontwikkelfasen van een referentiekader

1. Analyseren en identificeren	Brainstorm–/ Creatieve fase	Normen DGOBR
2. Clusteren 3. Ordenen 4. Bewerken	Zoeken naar ontbrekende elementen en samenhang	Wat is de samenhang ?
5. Formuleren	Definiëren van Hoofd– en Subnormen	Kan het beter?

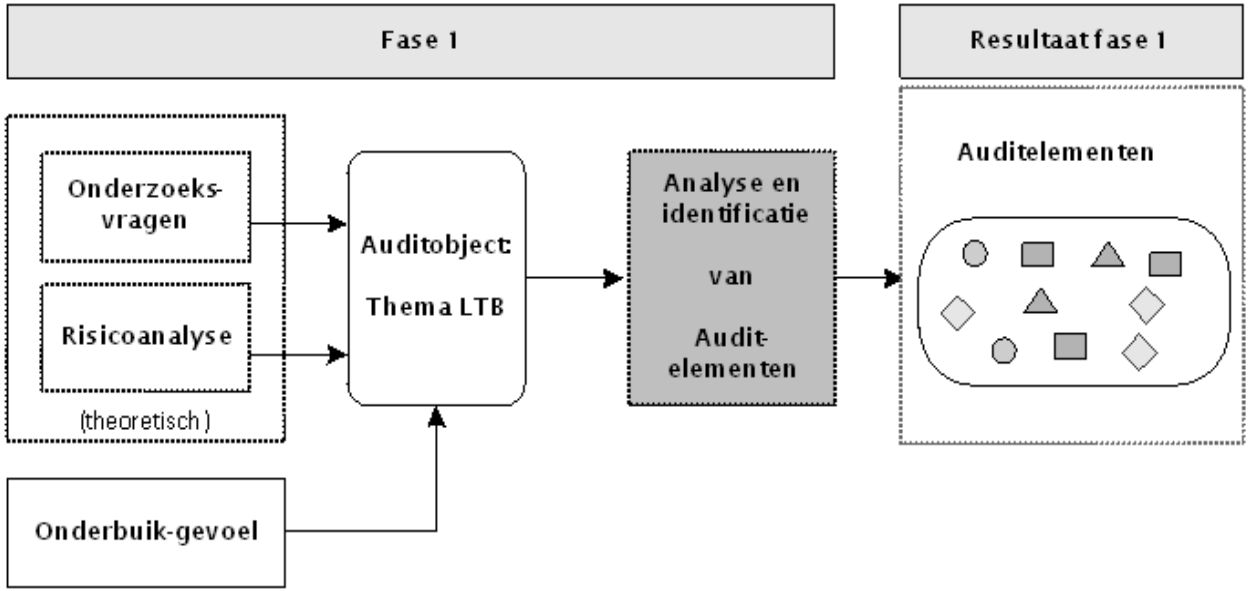
ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Toepassing SIVA raamwerk : Ontwikkelen van een RFK

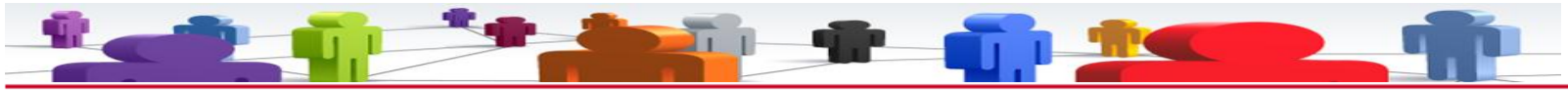


Fase 1: Analyseren en identificeren van auditelementen



Fase 1: Auditelementen & LTB - BIR

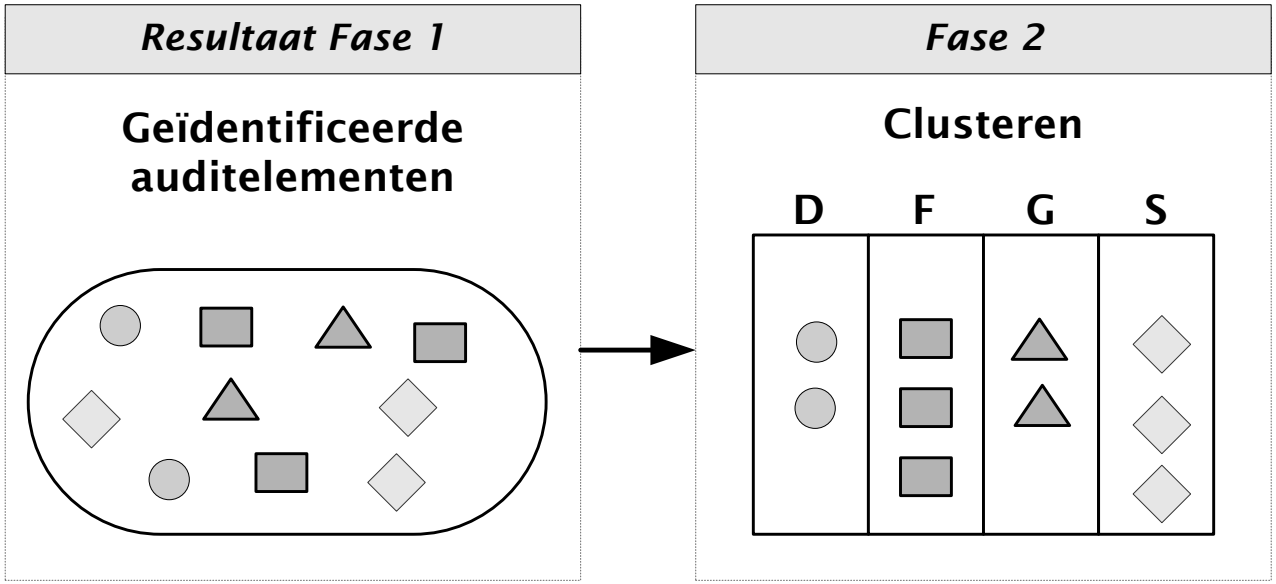
Nr.	Geïdentificeerde auditelementen		Basiselementen
1	8.3.3	Blokkering van toegangsrechten (Autorisatieproces)	Proces
2	11.1.1	Toegangsvoorzieningsbeleid	Beleid
3	11.2.1	Registratie van gebruikers (procedures)	Beleid (Operationeel-B)
4	11.2.2	Beheer van (speciale)bevoegdheden	Proces
5	11.2.3	Beheer van gebruikerswachtwoorden	Proces
6	11.2.4	Beoordeling van toegangsrechten	Proces (Controle-Proces)
7	11.5.1	Beveiligde inlogprocedures	Beleid (Operationeel-B)
8	11.5.2	Gebruikersindentificatie en -authenticatie	Interactie (I & A)
9	11.6.1	Beperken van toegang tot informatie	Interactie (Aut.)



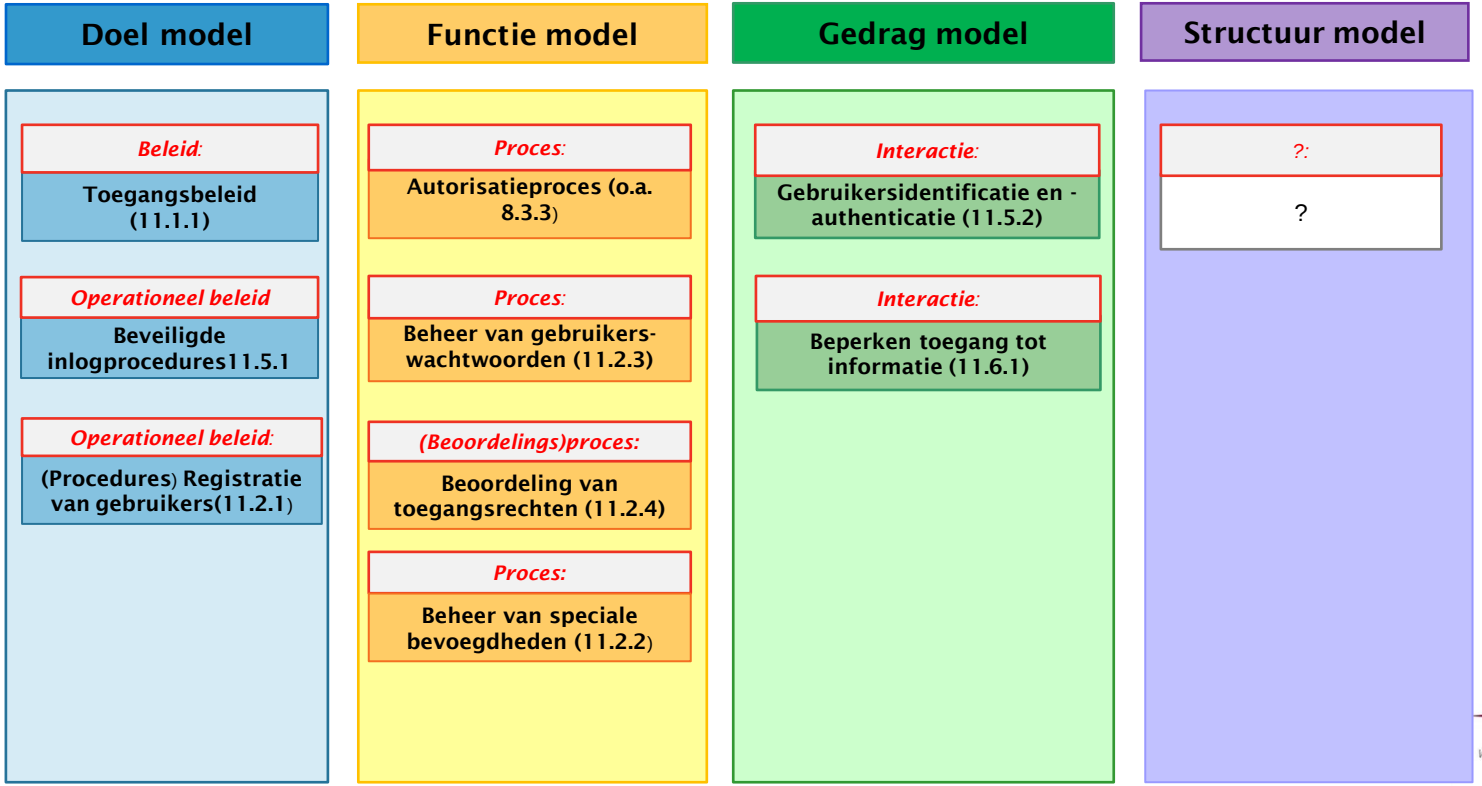
ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Fase 2: Clusteren van auditelementen



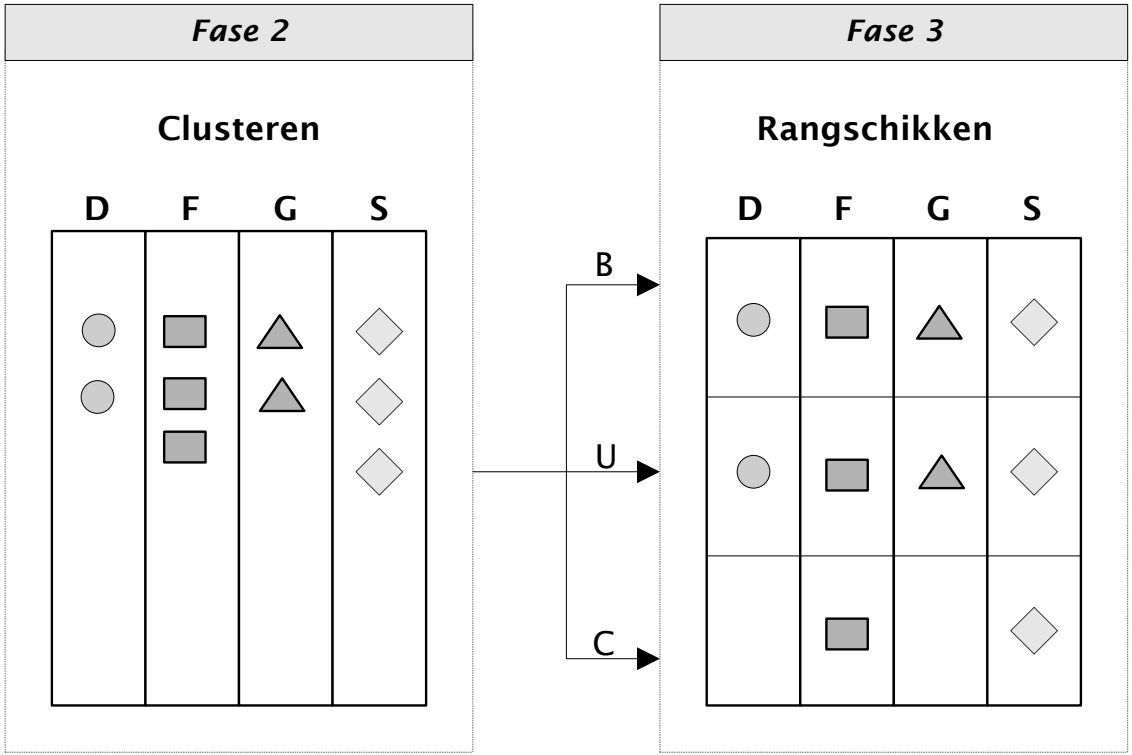
Fase 2: Clusteren van auditelementen van DGOBR



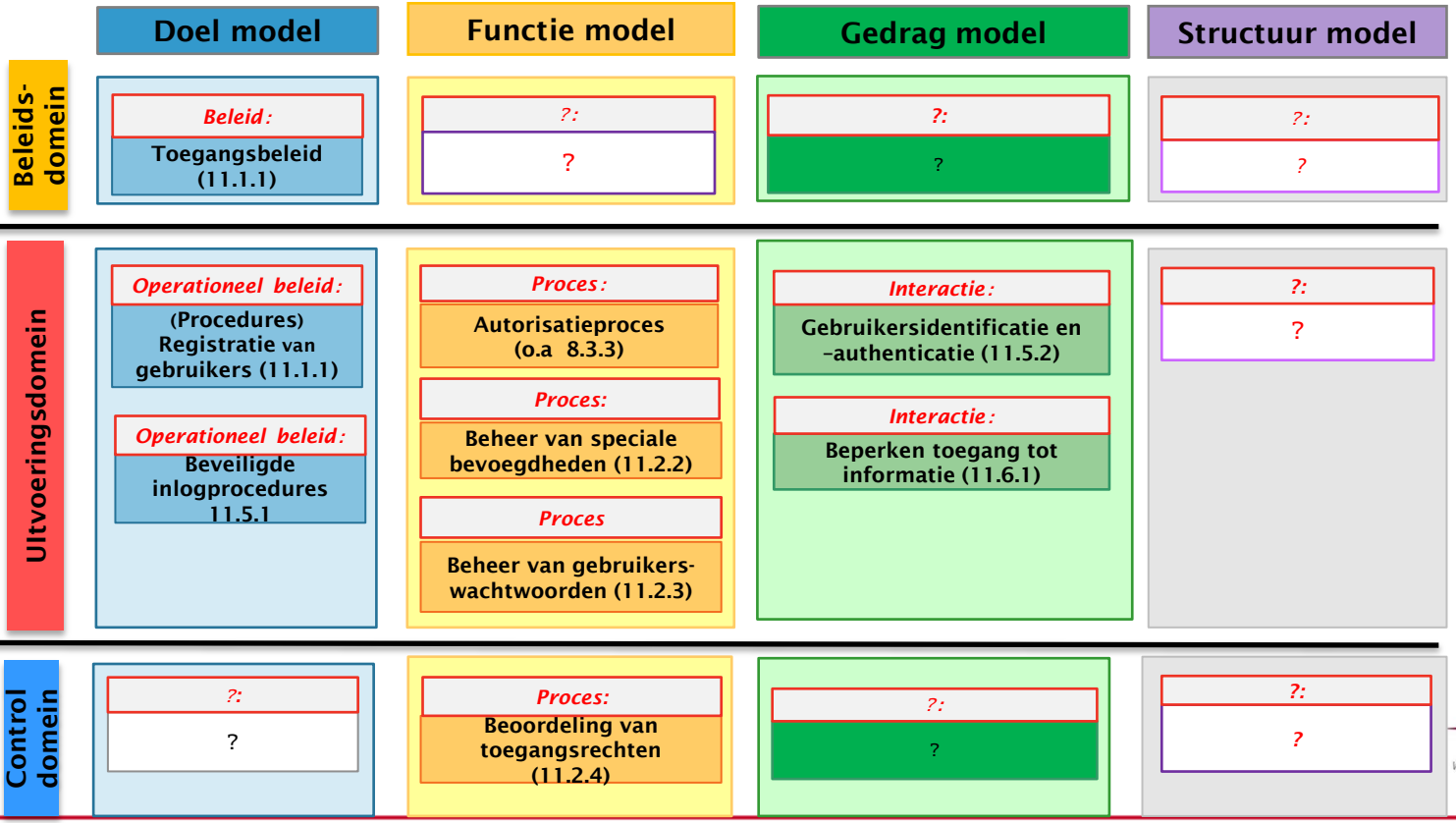
ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Fase 3: Ordenen van auditelementen



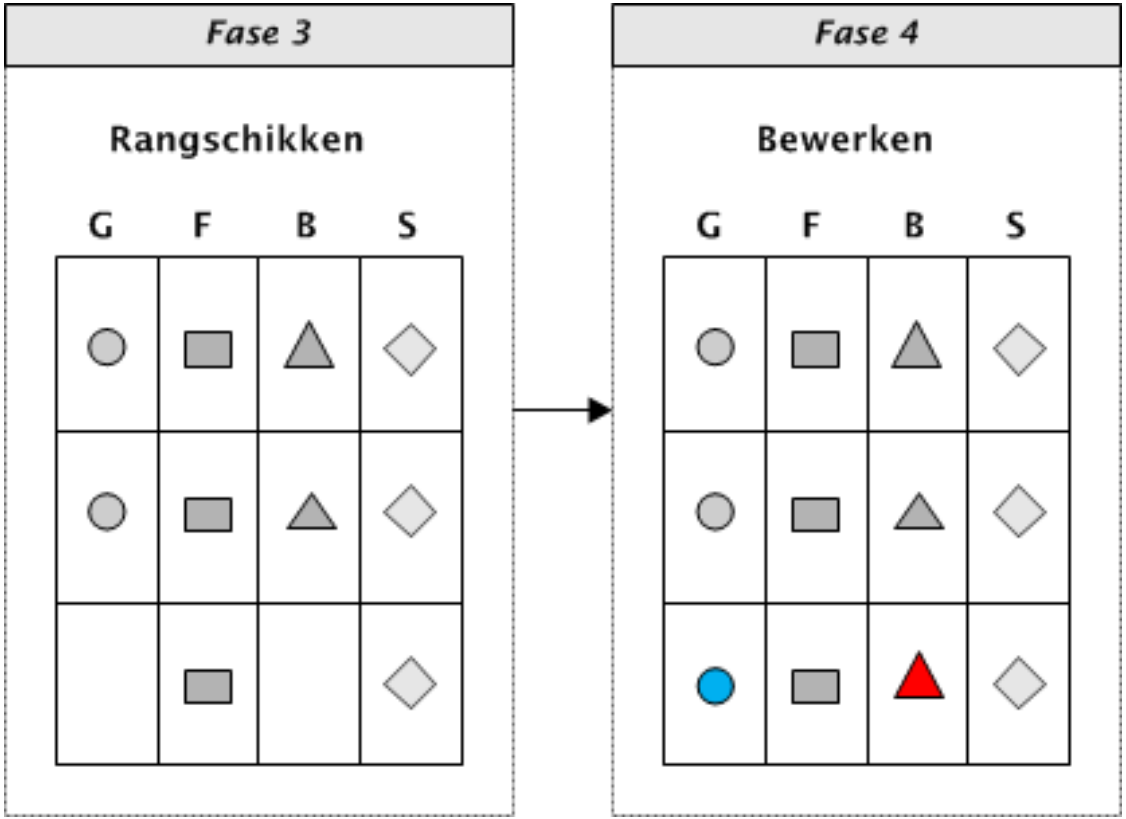
Fase 3: Ordenen van auditelementen van DGOBR



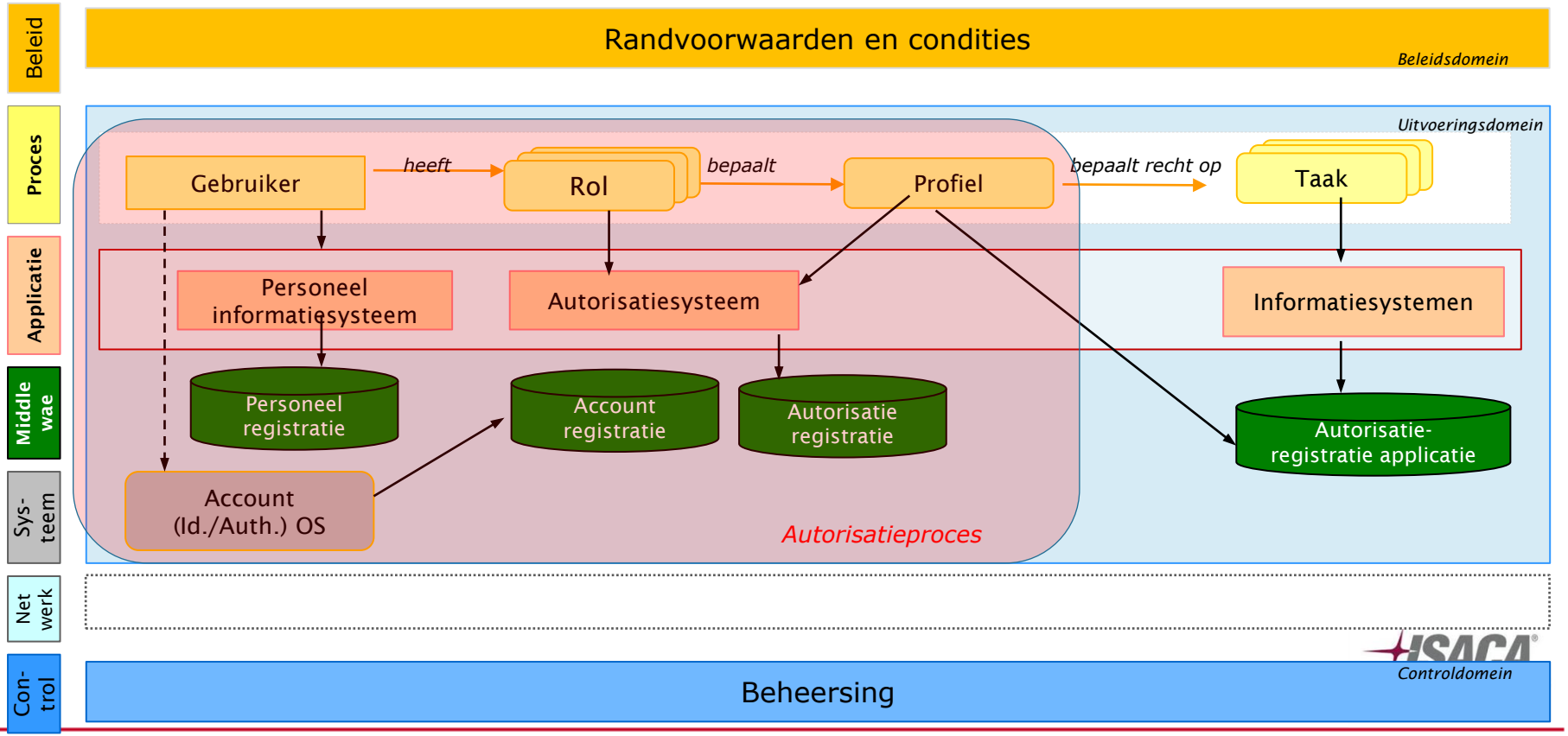
ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

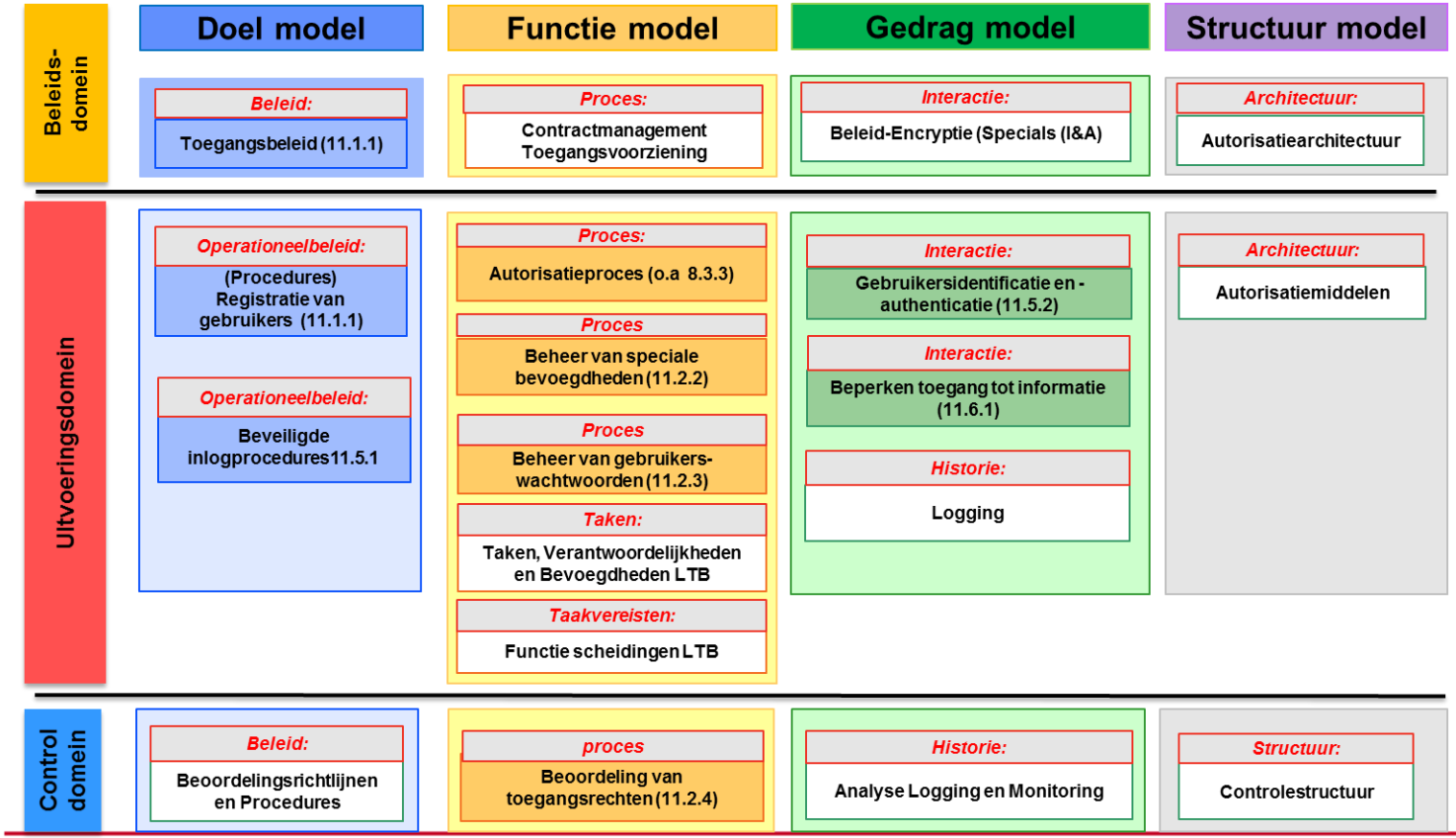
Fase 4: Bewerken



Overzicht Logische Toegangsvoorziening: Objecten



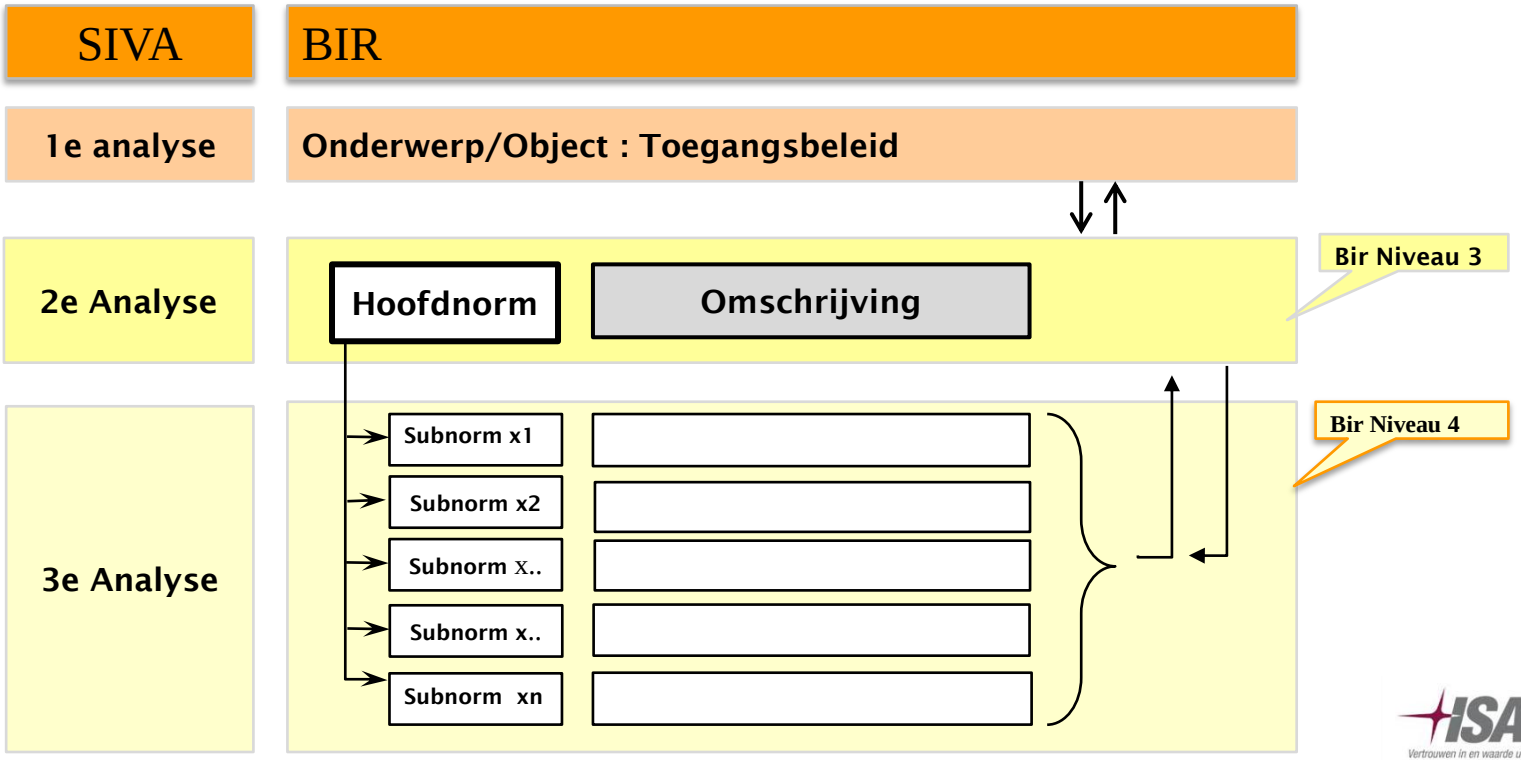
Fase 4: Bewerkenvan auditelementen van DGOBR



ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

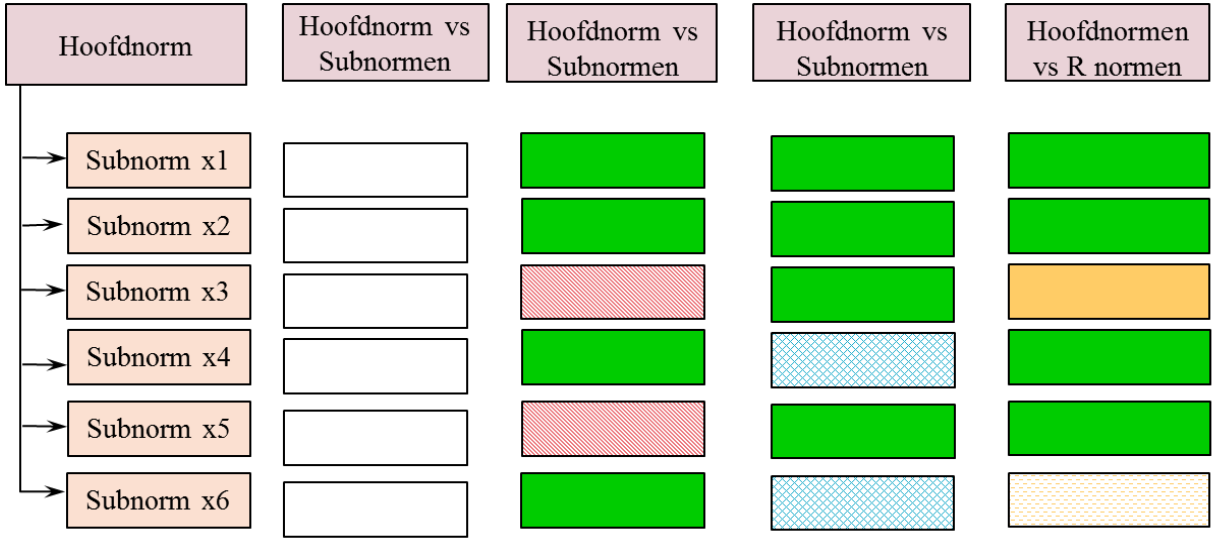
Fase 5: Formuleren



ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Bevindingen



ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

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.

ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

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

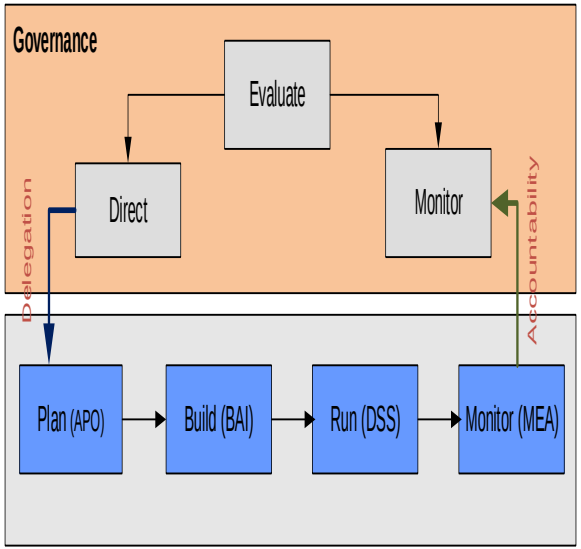
- Kunnen meer organisaties toepassen?
  - Ja,..
  - Verminder de complexiteit
  - Maak gebruik van de sterke punten
- Wat zijn de sterke punten
  - Governance benadering (onderscheid governance- en management body)
  - Gelaagde structuur (systeem benadering)
  - Vaak gebruikt als legitimering van de gekozen processen/objecten
  -
- Vraag

  Wil je cobit gebruiken als leidraad of reglement /richtlijn ?

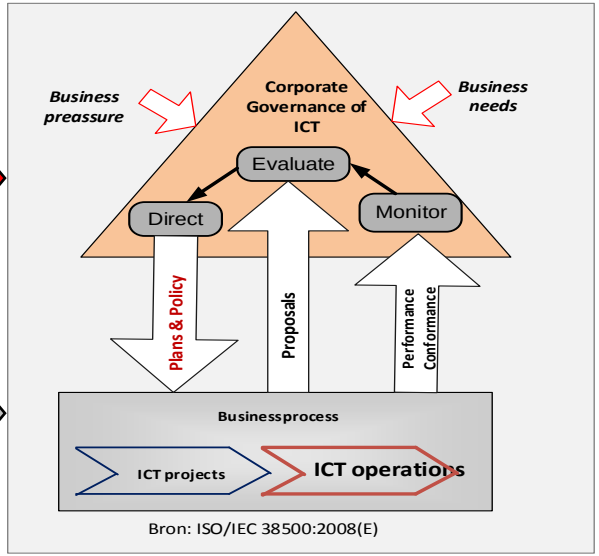
ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

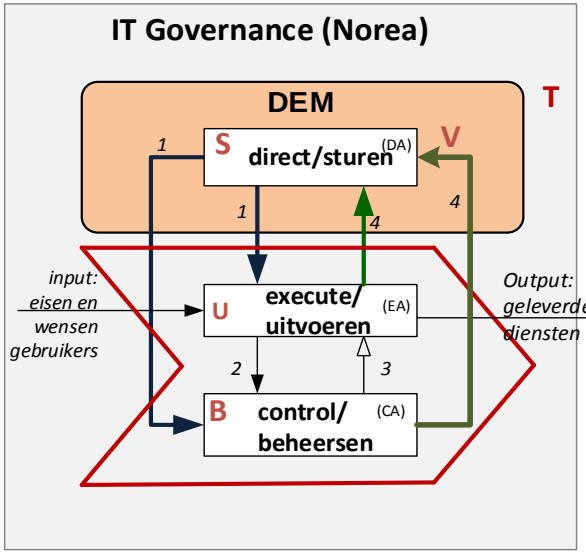
Governance modellen



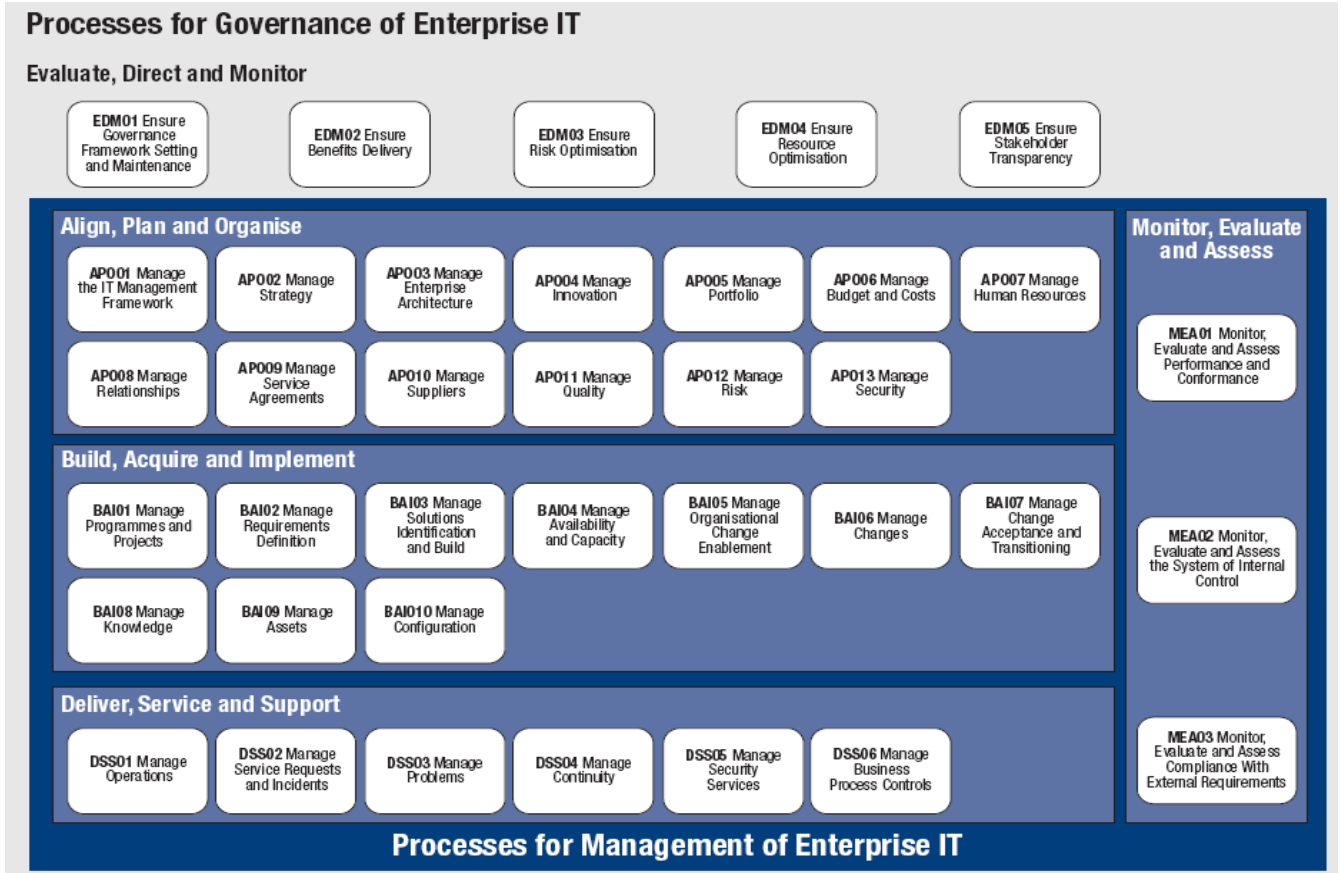
Bron: ISACA/COBIT



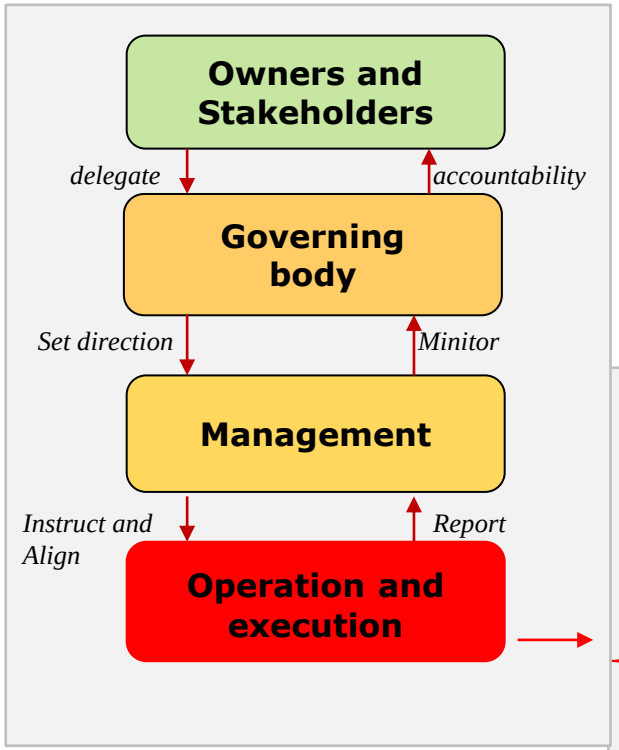
Bron: ISO/IEC 38500:2008(E)

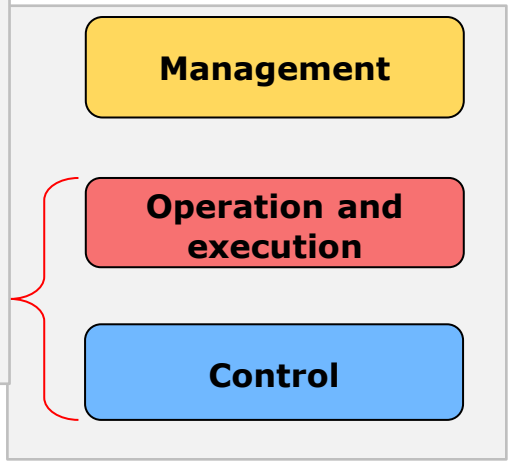


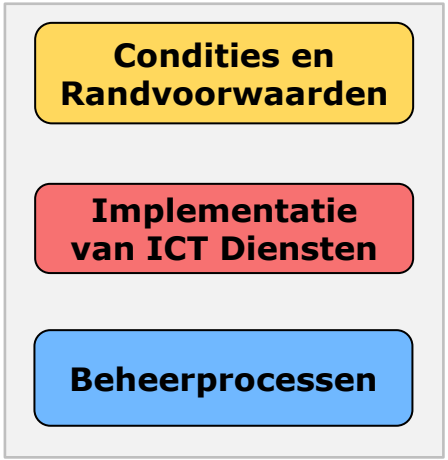
Cobit processen



Rollen en activiteiten/ uitwerken per thema



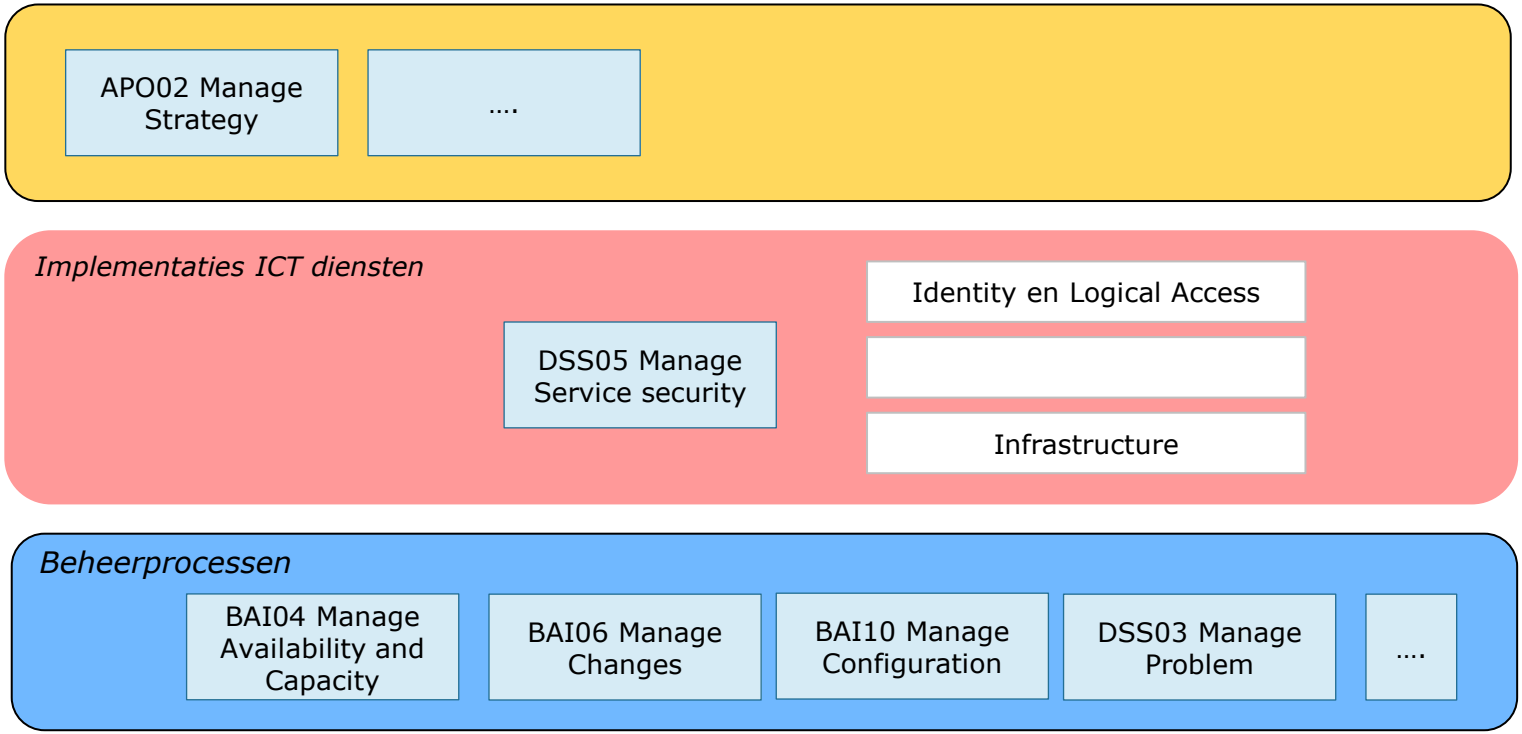




ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Rollen en activiteiten/ uitwerken per thema



ISACA Vertrouwen in en waarde uit informatiesystemen Netherlands Chapter

NOREA DE BEROEPSORGANISATIE VAN IT-AUDITORS

Vragen

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

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

24 september 2015

ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS