NORA werkdocument

Sessie 4

In stappen naar een BBO

Baseline Beveiliging Overheid

Bijgewerkte versie 10 april. 2013

Expertgroep NORA katern Beveiliging

Jaap van der Veen

Agenda Sessie 4

1. Terugkoppeling afstemming met Provincie & Gemeenten / KING
   - Memo Cor Franke
2. Ervaring activiteiten (NORA-CIP-NCSC)
   - Herziening normen voor DigID assessment: CIP; Wiekram T. & Jaap
3. Vervolgstappen

Opdracht + aanpak katern

1. Samenhang van normenkaders- Beveiliging voor de overheid
2. Actualisering NORA dossier “Normen voor IT-voorzieningen” tot ISO-toepassingskader voor ontwerp: “Normen voor informatievoorzieningen”, met met integratie van relevante normen uit kaders als NCSC en BIR.

Actie:

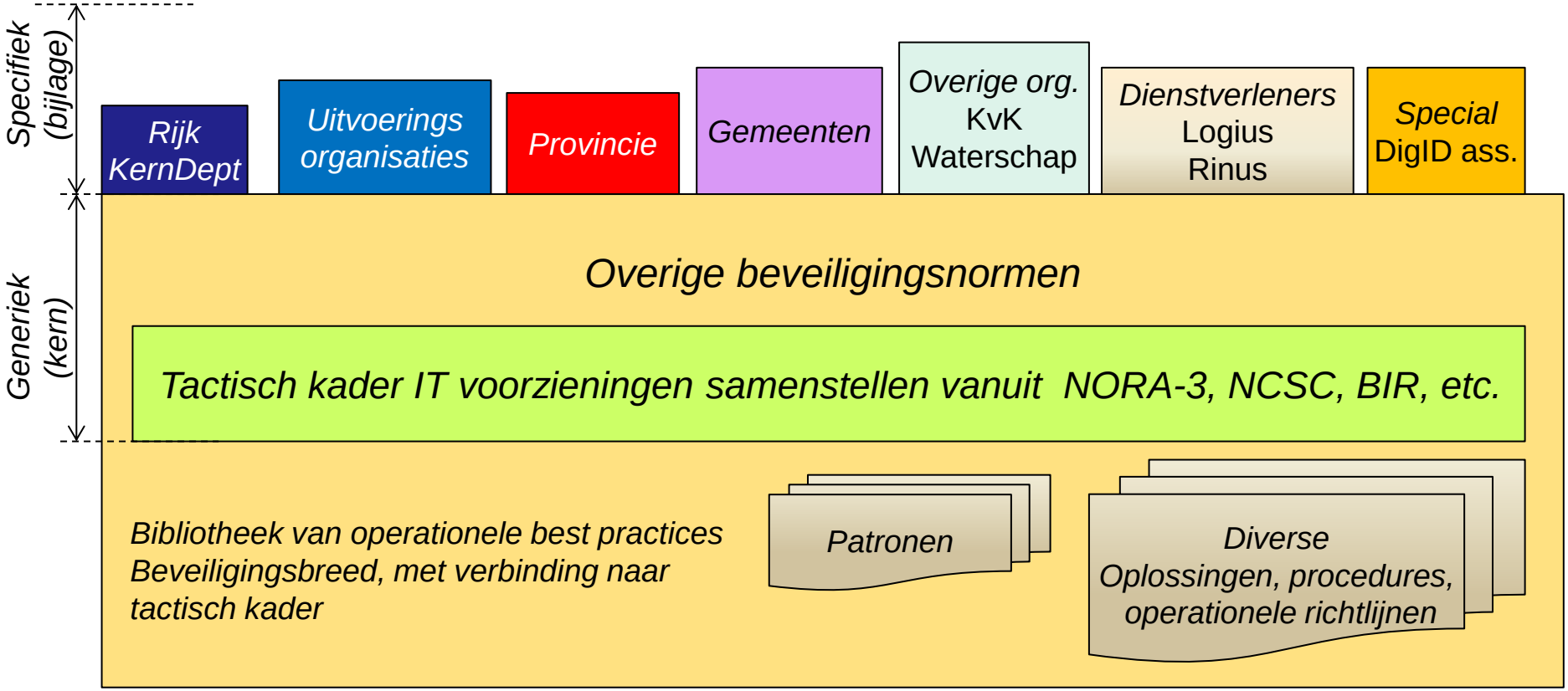
- Verdieping IB-functiemodel; beveiligingsbreed tot universeel referentiemodel
- Het te beveiligen object staat centraal, met verbinding naar beleid en control
- Samenwerking met CIP en NCSC
- Terugkoppeling resultaten met stakeholders

    - Baseline Overheid toepasbaar maken voor zowel ontwerp als audit

Doelstructuur

Baseline Beveiliging Overheden

Expertgroep NORA



Terugkoppeling
afstemming KING maart 2013

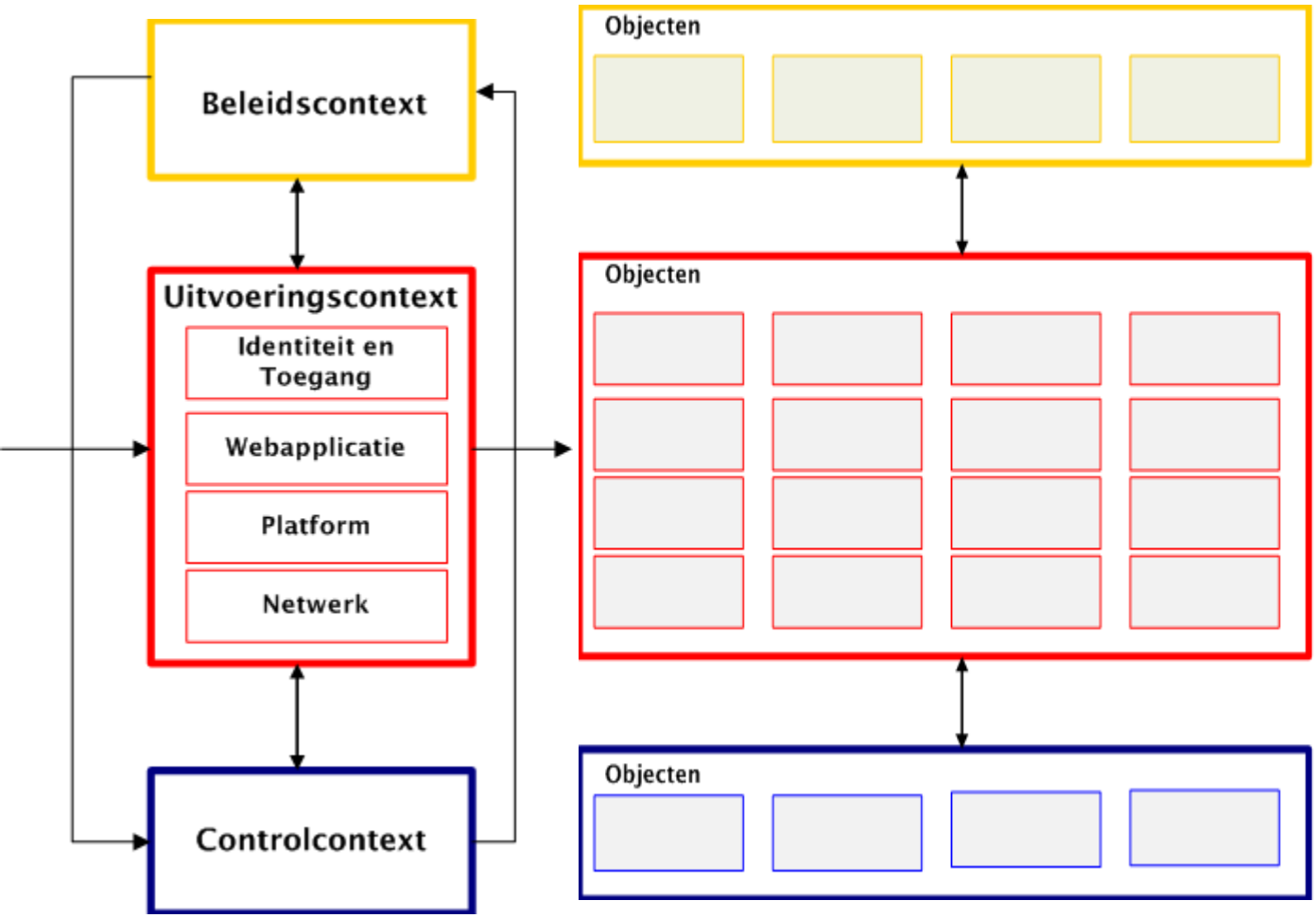
Samenvattende punten..

- *NORA focust op interoperabiliteit en niet op de interne bedrijfsvoering*
- *Gezamenlijk beeld van baseline en doorwerking daarvan*
- *Bestuurlijk draagvlak bereiken*
- *Afspraken voor inzet CIP, TF-BID en NORA ontwikkelen oplossingen*

Ervaringen
case *revisie* NCSC kader

1. Problemen met toepassing NCSC kader voor DigID assessments
   a. Onduidelijkheden en variaties in detaillering normen bij aanvang audits
   b. Verschillen in interpretaties normen en uitvoering audits
   c. Geen rekening gehouden met context/situatie van organisatie en de gelaagdheid van beveiligingsmaatregelen.

2. Uitgevoerde acties CIP/NORA i.r.t. NCSC kader; case en ‘pilot’ voor NORA
   a. NORA IB-functies geanalyseerd
   b. Relatie gelegd met “DFGS” concepten bibliotheek
   c. Presentatie bij NCSC over:
      - SIVA raamwerk,
      - Analyses NCSC normenkader op basis van dit raamwerk
      - Verbeteringsvoorstellen gedaan
   d. Ter review eerste concept delen van herziene versie NCSC normenkader.



Algemene Randvoorwaarden

Waarom en Wat moet op hogere management niveau gebeuren voor implementatie doeleinden

Implementatie van IT diensten

Hoe moet wat op specifiek niveau geimplementeerd worden

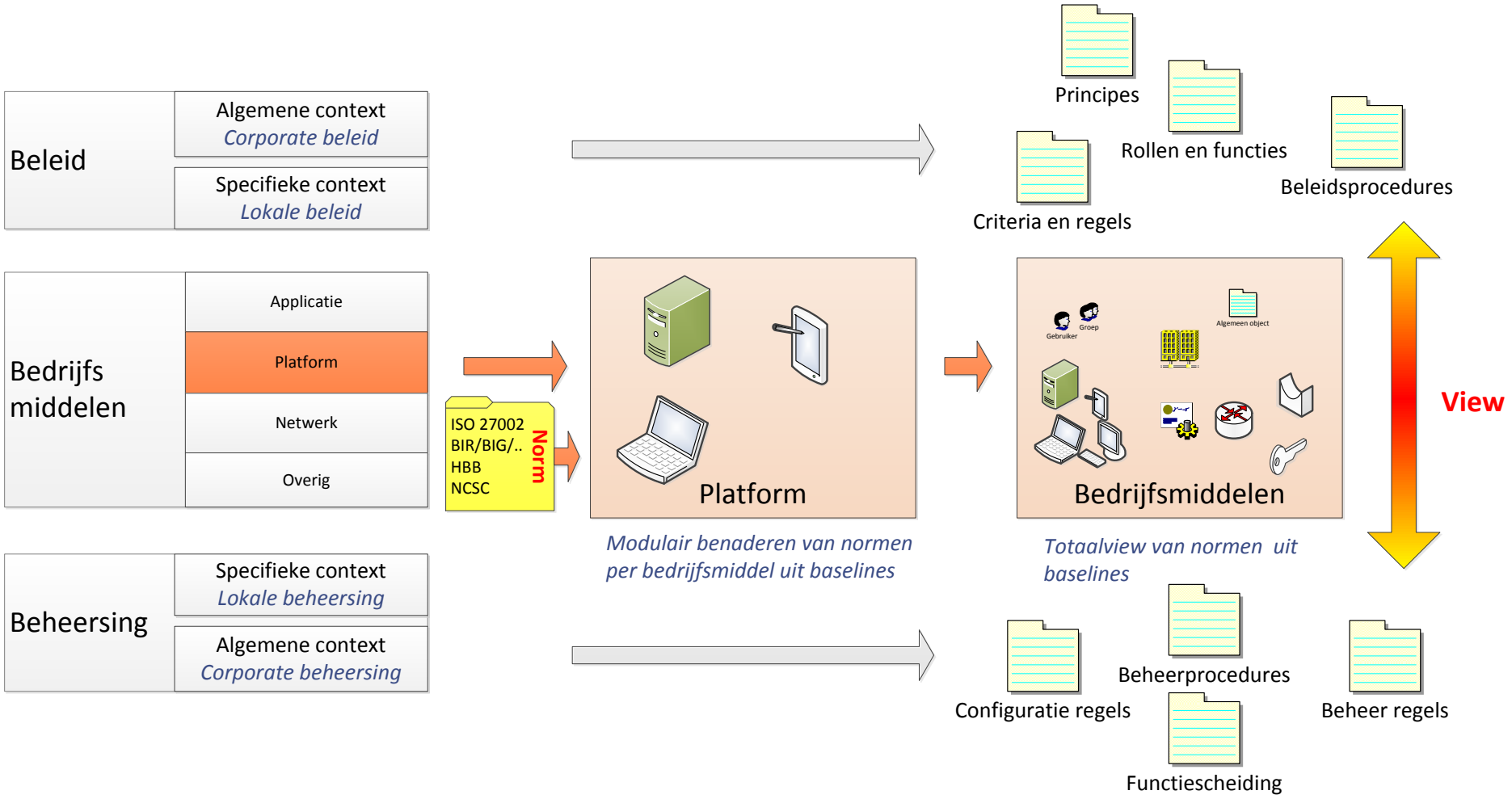
Beheersing

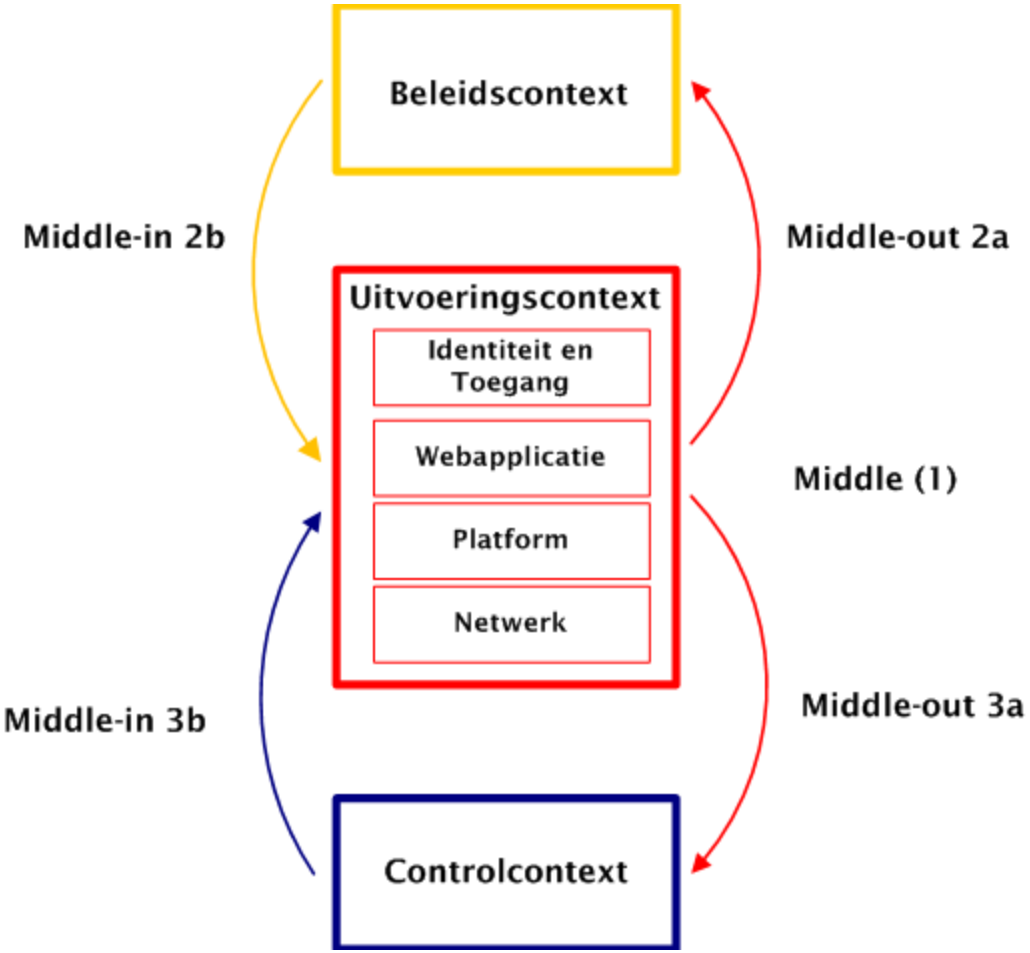
Hoe en Wat moet op het IT niveau beheerst worden

Inhoud *Ontwerp -en auditgebieden uit baselines*

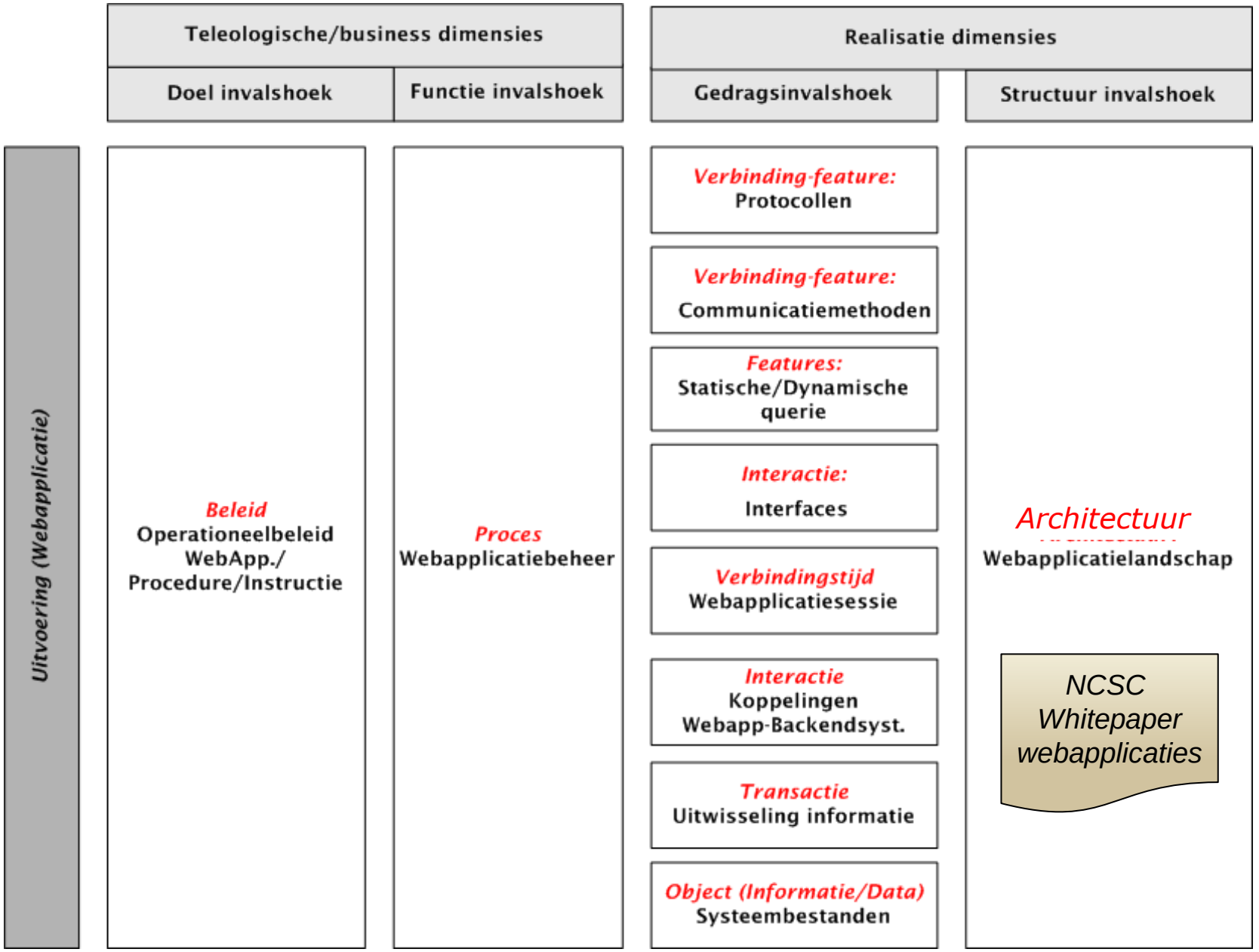
Overzicht Eenvoud

Expertgroep NORA

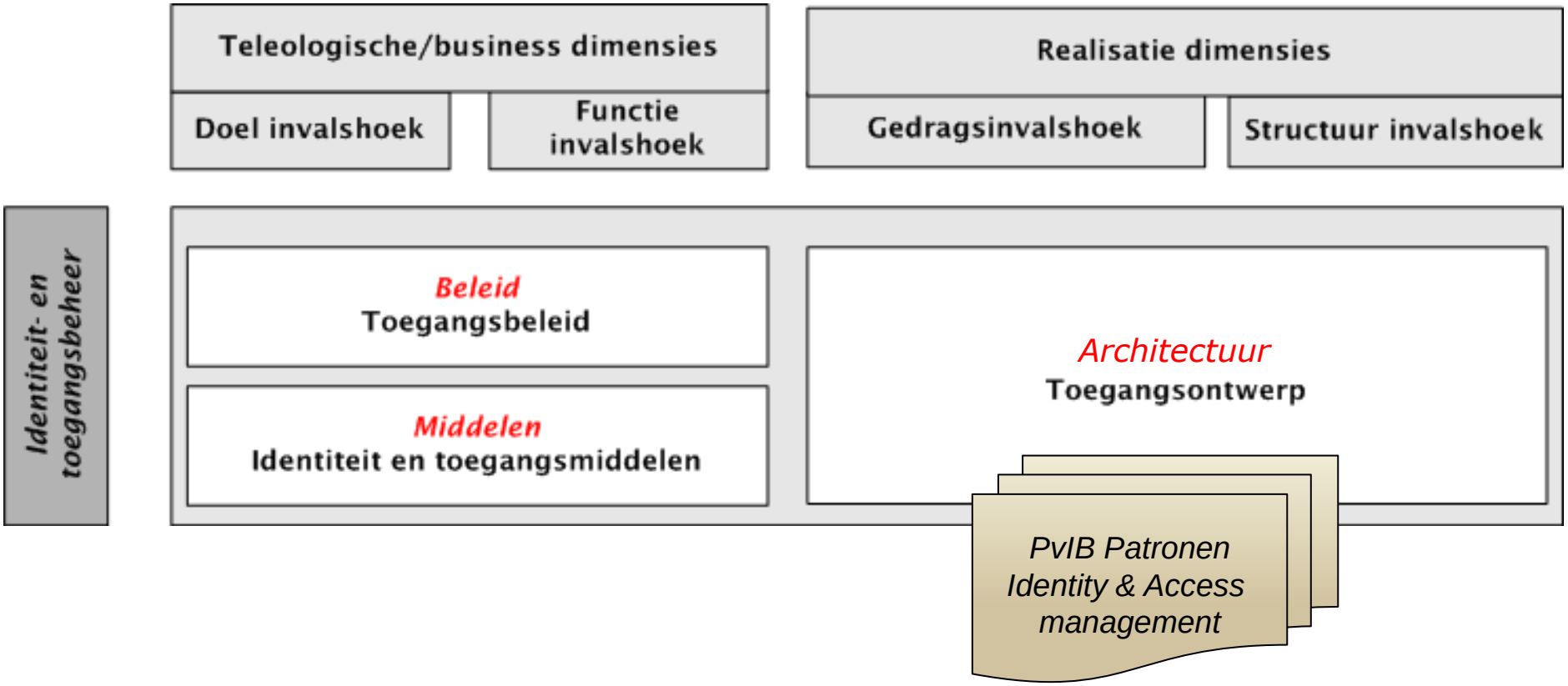



Beleidscontext
Middle-in 2b
Middle-out 2a
Uitvoeringscontext
Identiteit en Toegang
Webapplicatie
Platform
Netwerk
Middle (1)
Middle-in 3b
Middle-out 3a
Controlcontext

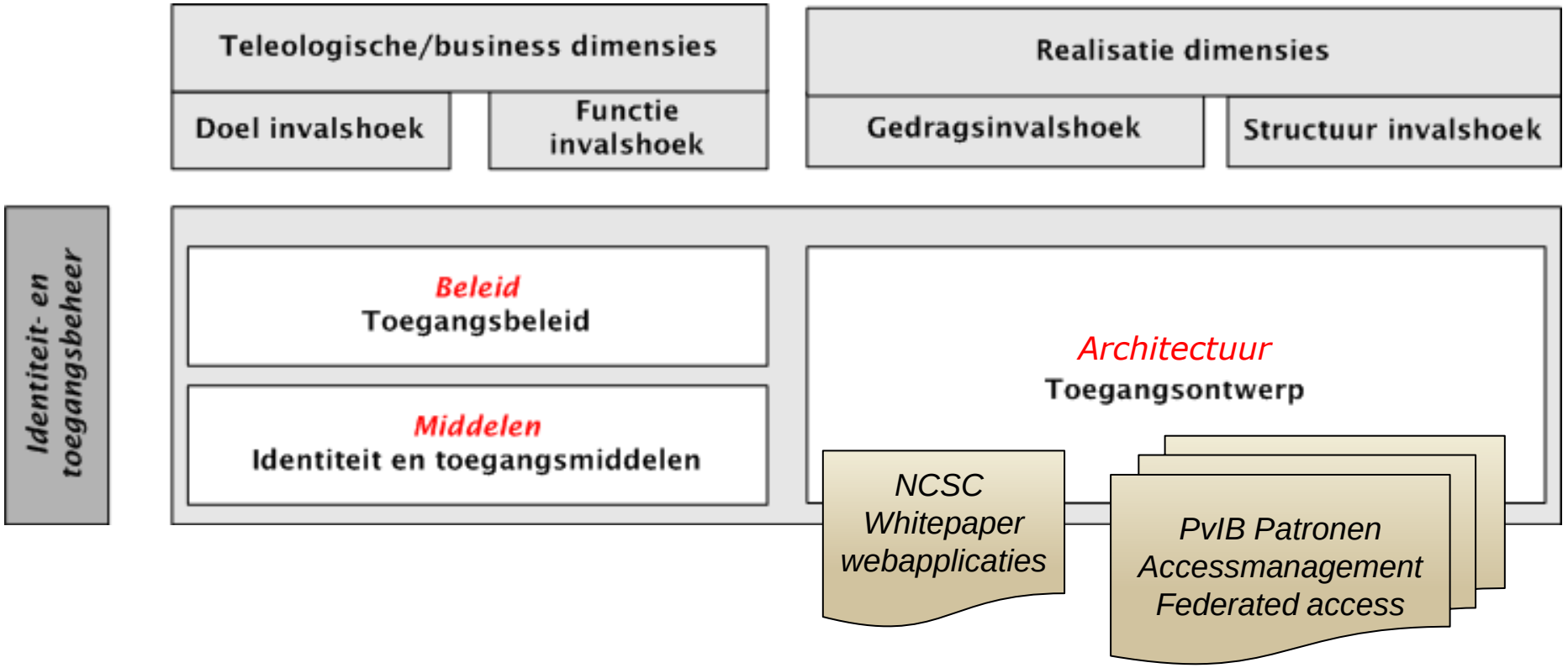
Middle: *Webapplicatie*



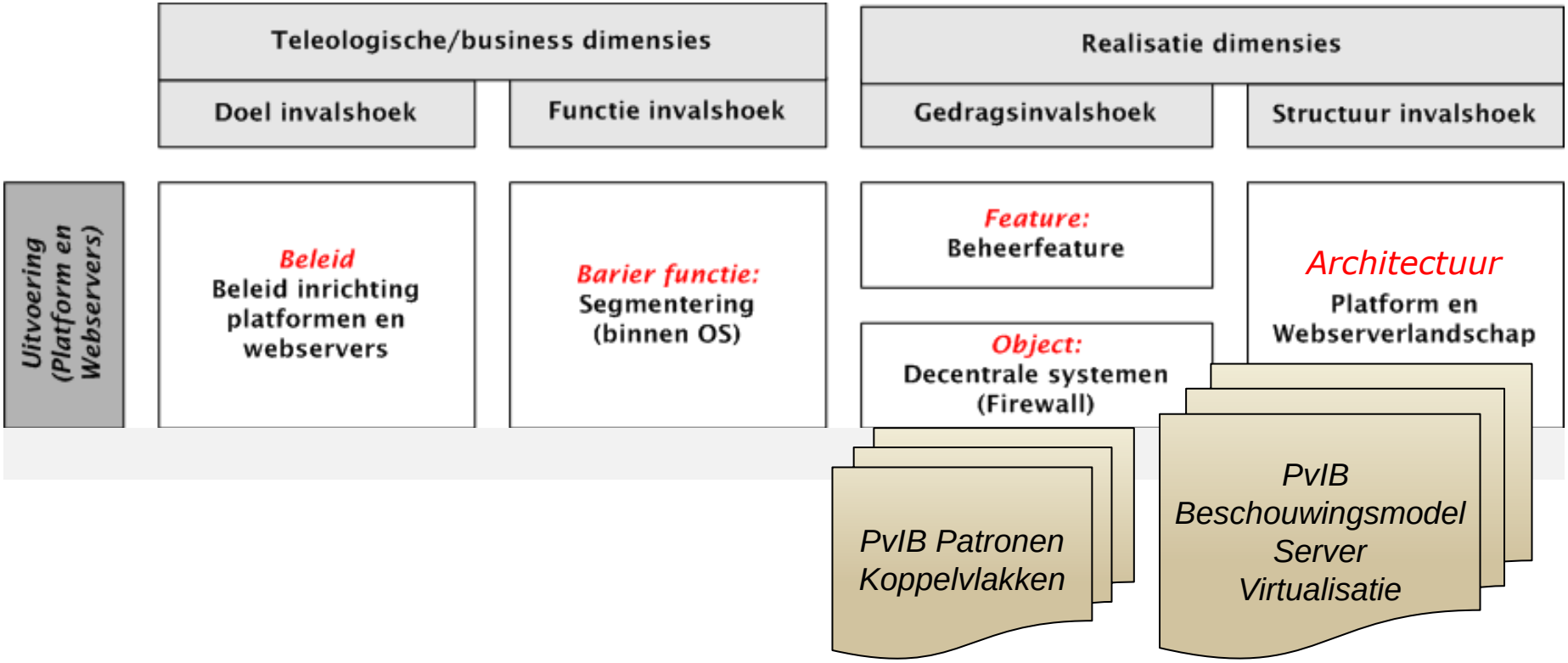
Middle: *Identiteit en Toegang*



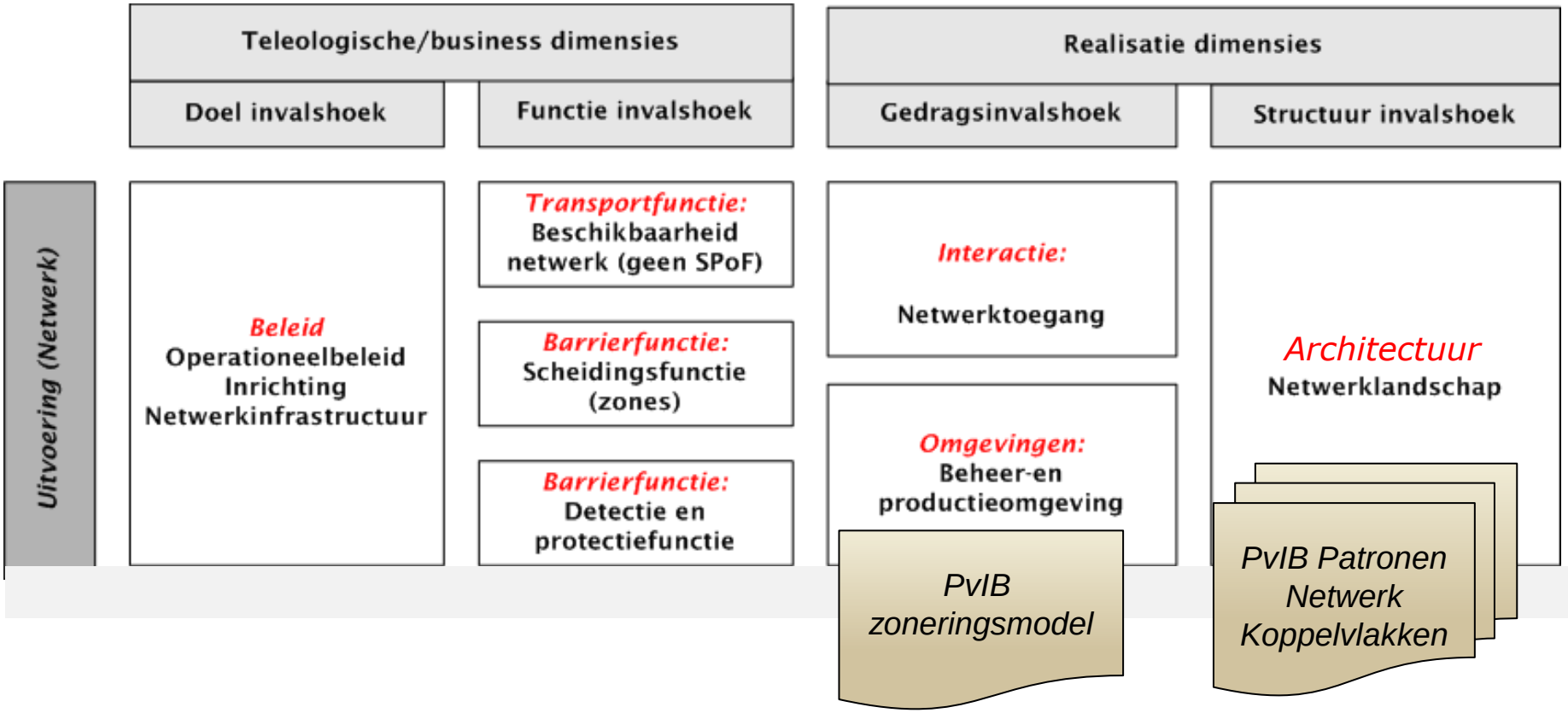
Middle: *Webapplicatie*



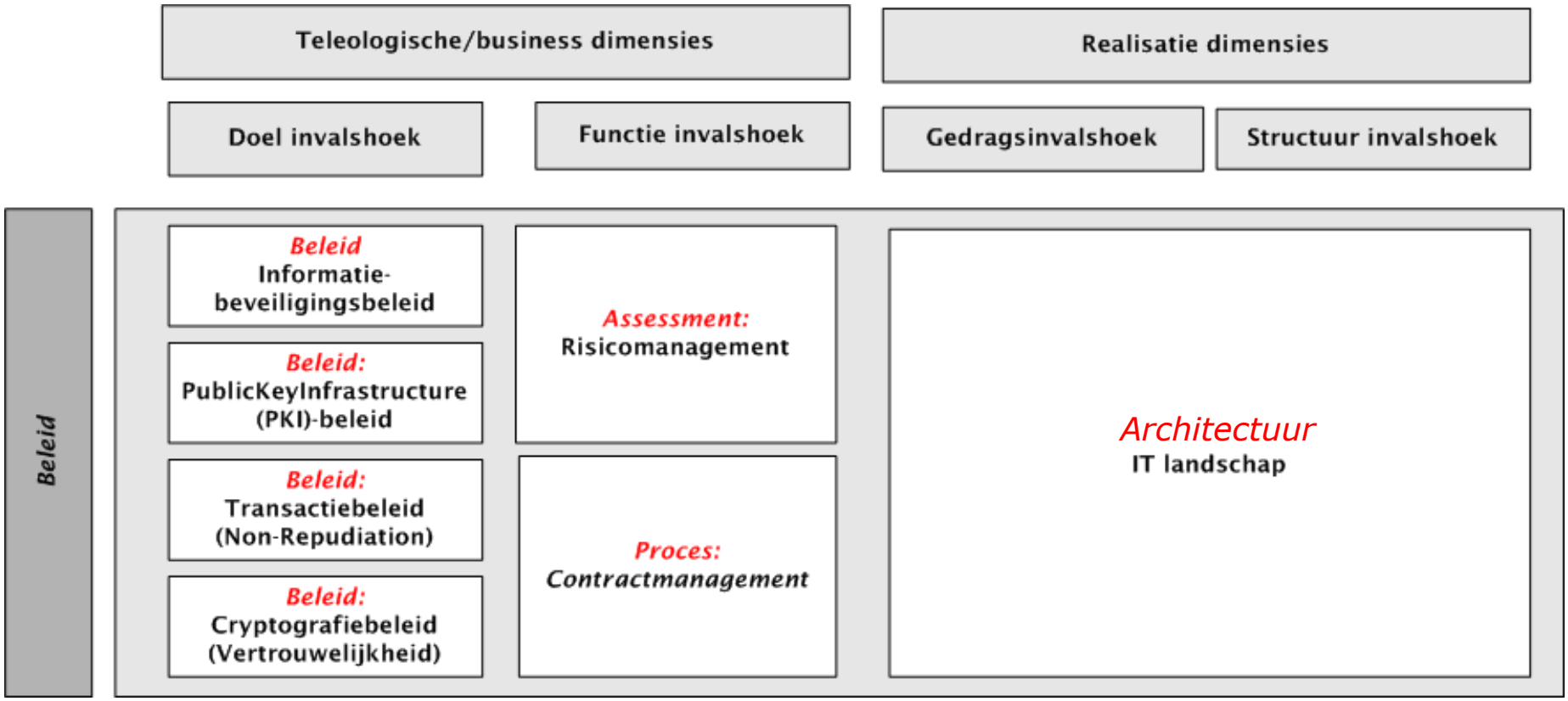
Middle: *Platform en Webserver*



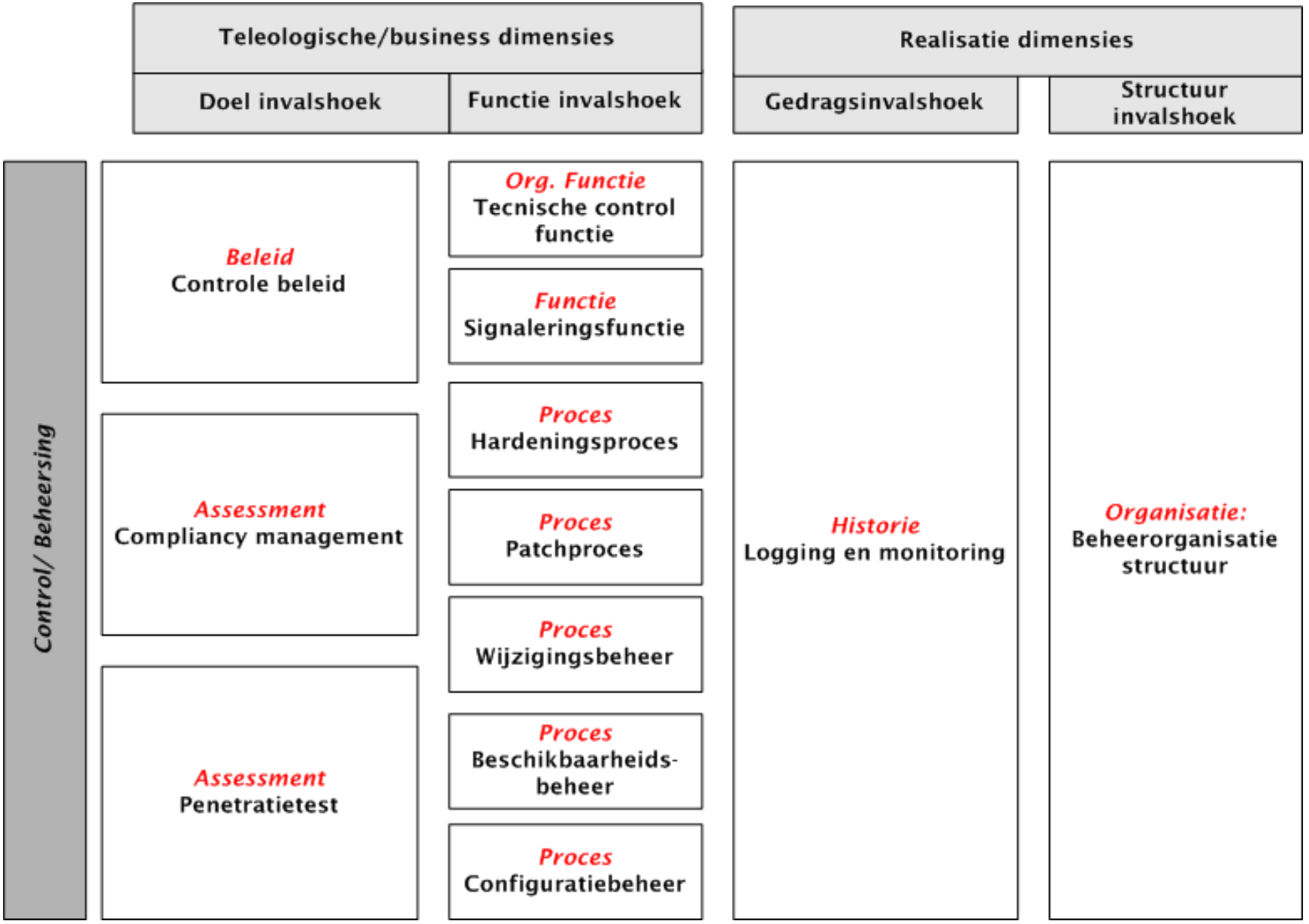
Middle: *Netwerk*

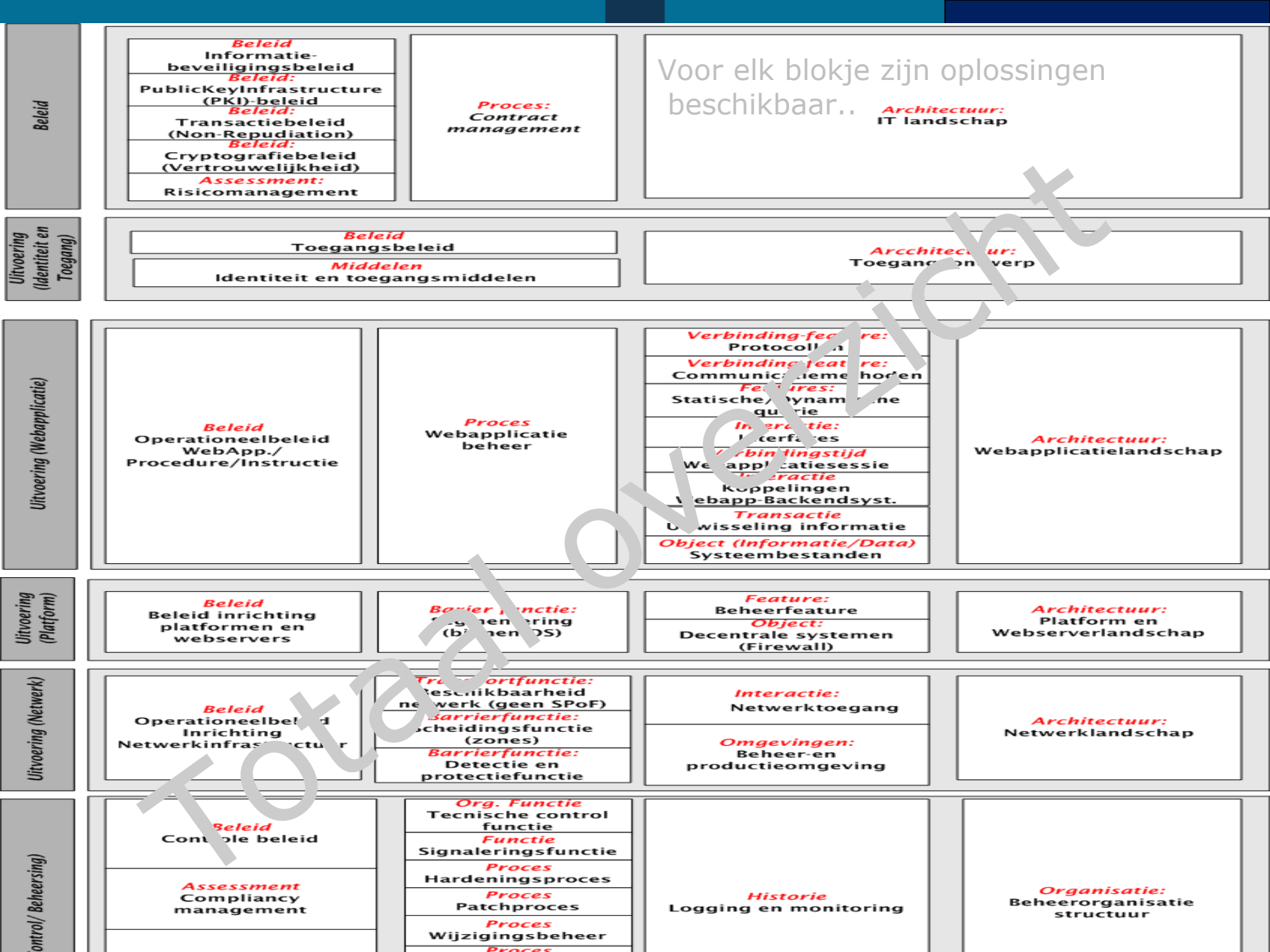


Middle-out/in: *Beleid*

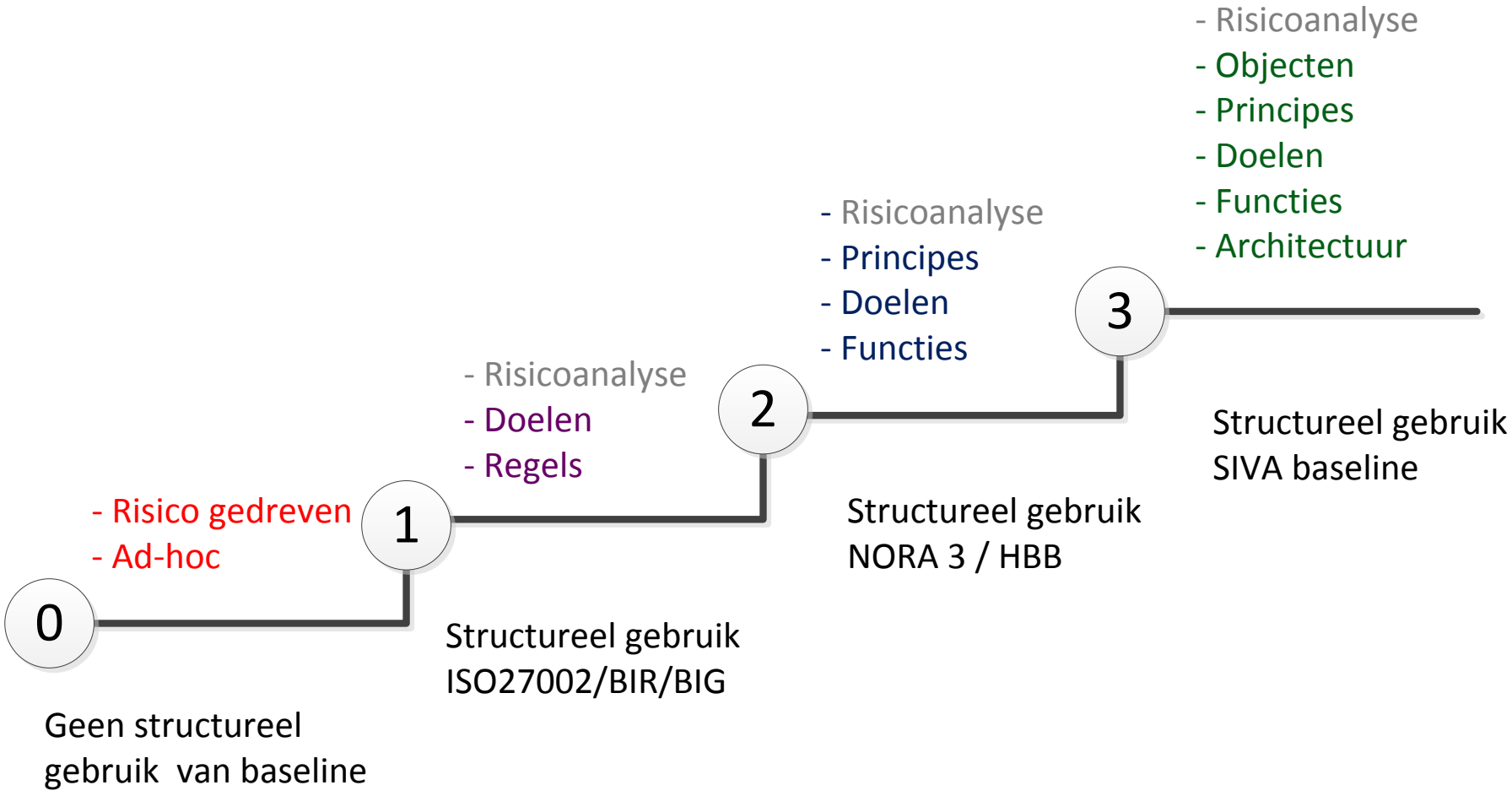


Middle-out/in: *Beheersing*

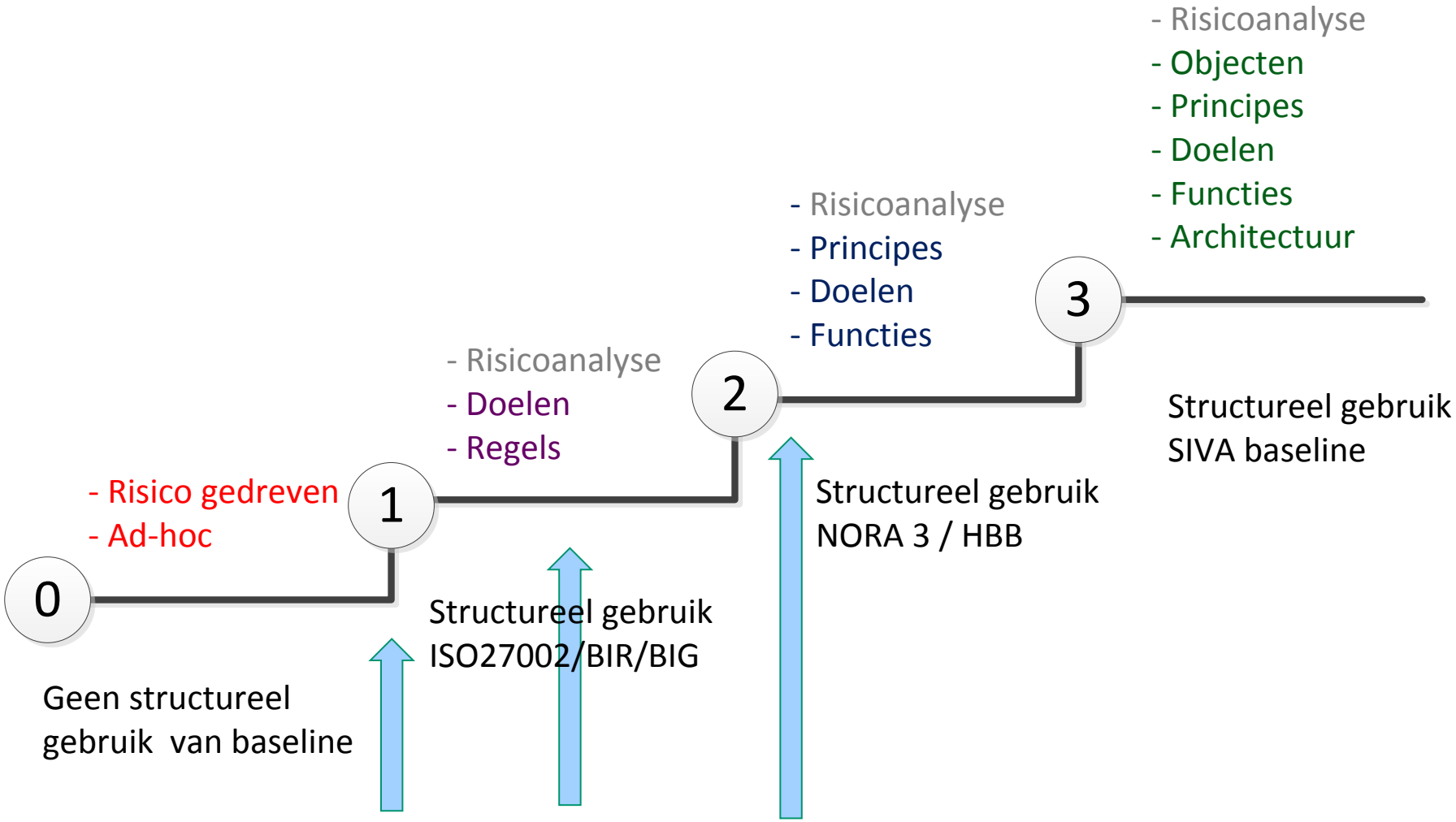



Beleid
Beleid
Informatie-beveiligingsbeleid
Beleid:
PublicKeyInfrastructure (PKI)-beleid
Beleid:
Transactiebeleid (Non-Repudiation)
Beleid:
Cryptografiebeleid (Vertrouwelijkheid)
Assessment:
Risicomanagement
Proces:
Contract management
Voor elk blokje zijn oplossingen beschikbaar..
Architectuur:
IT landschap
Uitvoering (Identiteit en Toegang)
Beleid
Toegangsbeleid
Middelen
Identiteit en toegangsmiddelen
Arcchitectuur:
Toegangsontwerp
Uitvoering (Webapplicatie)
Beleid
Operationeelbeleid WebApp./ Procedure/Instructie
Proces
Webapplicatie beheer
Verbinding-feature:
Protocollen
Verbinding feature:
Communicatiemethoden
Features:
Statische/dynamische query
Interactie:
Interfaces
Verbindingstijd
Webapplicatiesessie
Interactie
Koppelingen Webapp-Backendsyst.
Transactie
Uitwisseling informatie
Object (Informatie/Data)
Systeembestanden
Architectuur:
Webapplicatielandschap
Uitvoering (Platform)
Beleid
Beleid inrichting platformen en webservers
Barrierfunctie:
(beheer OS)
Feature:
Beheerfeature
Object:
Decentrale systemen (Firewall)
Architectuur:
Platform en Webserverlandschap
Uitvoering (Netwerk)
Beleid
Operationeelbeleid Inrichting Netwerkinfrastructuur
Transportfunctie:
Beschikbaarheid netwerk (geen SPoF)
Barrierfunctie:
Scheidingsfunctie (zones)
Barrierfunctie:
Detectie en protectiefunctie
Interactie:
Netwerktoegang
Omgevingen:
Beheer-en productieomgeving
Architectuur:
Netwerklandschap
Control/ Beheersing)
Beleid
Controle beleid
Assessment
Compliancy management
Org. Functie
Tecnische control functie
Functie
Signaleringsfunctie
Proces
Hardeningsproces
Proces
Patchproces
Proces
Wijzigingsbeheer
Historie
Logging en monitoring
Organisatie:
Beheerorganisatie structuur
Totaal overzicht

Volwassenheid van baselines

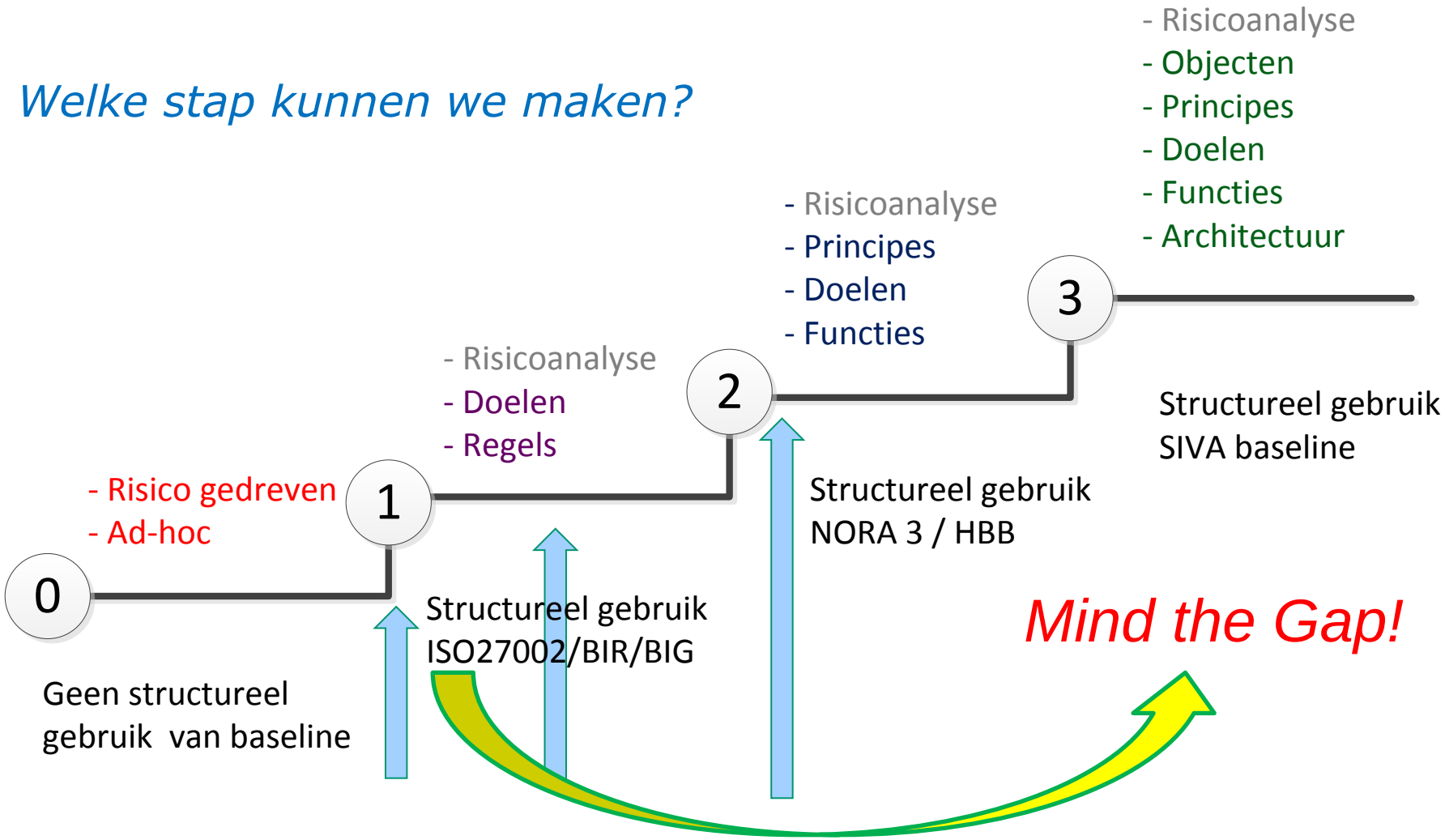


Volwassenheid van baselines



Volwassenheid van baselines

Welke stap kunnen we maken?



Conclusie sessie 4:

1. Stap voor baseline-volwassenheid van 1 naar 3 is te groot.
2. Aan verder ontwikkelde (tactische) normen en modellen bestaat geen behoefte.
3. Er is vooral behoefte aan *oplossingen* zoals *patronen* etc. (beveiligingsbreed). Een *cafetaria* model of *menukaart*
4. NORA baseline met *beleid-uitvoering-control* lagen fungeert als 'kapstok' voor een oplossingen bibliotheek.

Werkafspraken sessie 4:

Wat?

1. Cafetariamodel van operationele baseline heeft prioriteit
2. Oplossingen ontsluiten voor kleine en grote organisaties.
3. De werking van best practices op de werkvloer beproeven.
4. NORA baseline krijgt een gelaagdheid met beleid, uitvoering en control laag, geflankeerd door oplossingenarchitectuur.

Acties expertgroep

a) Opstellen menukaart: Welke patronen / oplossingen zijn er nodig?
b) Uploaden van best practices naar centrale plek / NORA-online Wiki
c) Bruikbaarheid oplossingen toetsen in kleine en grote organisaties
d) Oplossingen verankeren in een te actualiseren tactische NORA baseline voor interoperabiliteit (focus op IT voorzieningen) en in de BIR en BIG.

Werken in subgroepen, volgende plenaire NORA sessie eind mei.