centrum informatiebeveiliging en privacybescherming

Wie is er bang voor de privacywetgeving?

Wie is er bang voor de privacywetgeving?

Marcel Koers - marcel.koers@uwv.nl

Grip op privacy: hoe?

Een ogenschijnlijk eenvoudige vraag uit de CIP community:

Kunnen jullie eens opschrijven

hoe dat nou moet, met die privacy?

Hoe moeten organisaties er mee werken?

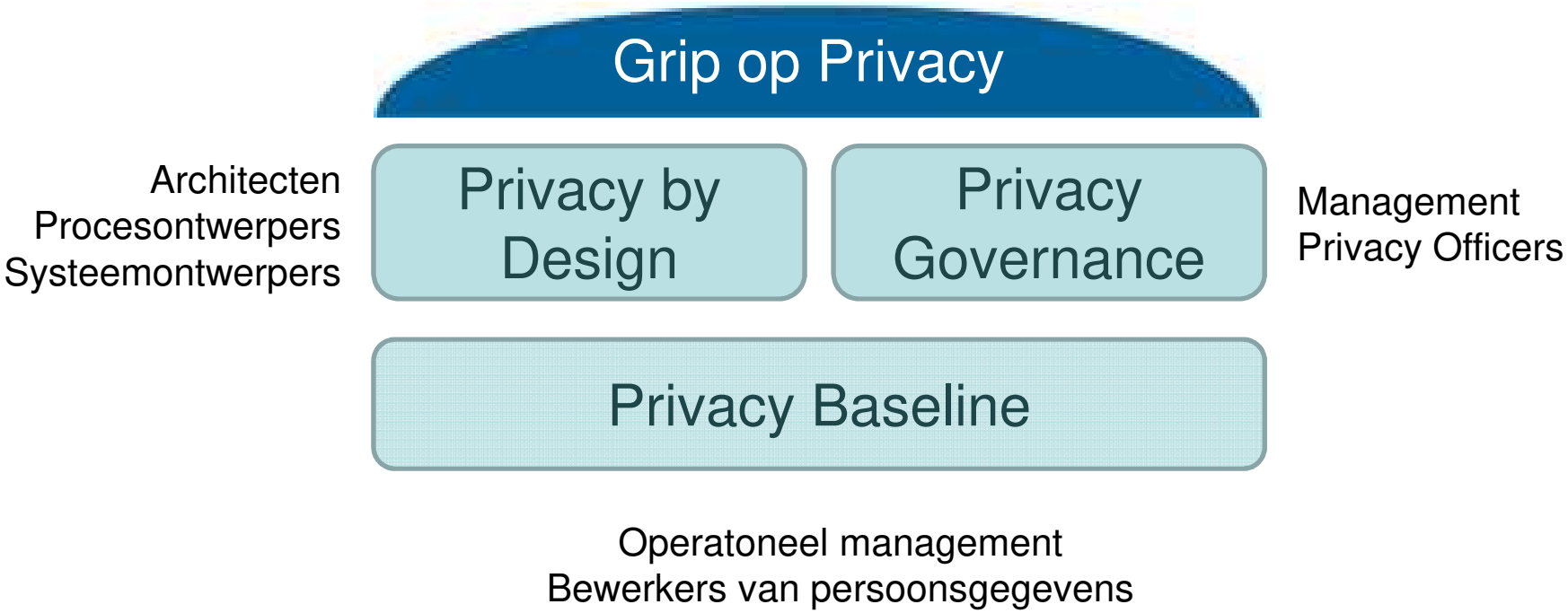
Hoe krijgen we duidelijkheid in de wirwar aan informatie en meningen?

Grip op privacy: versimpel!

- WBP = wet maar wollig;
- Voldoen aan WBP: hoe *doe* je dat?
  - Begint met helder begrip en heldere communicatie
- CIP idee: Privacy Baseline
  - ‘vertaal’ de WBP naar het format van een normenkader
  - gebruik SIVA format: eenduidig, ontdubbeld, compleet en uniform
- De boodschap: volg de aanwijzingen van de Privacy Baseline op en je voldoet ‘automatisch’ aan de WBP *en al voor een belangrijk deel aan de AVG*
- Hulpmiddelen bij uitvoering:
  - handleidingen design en governance, maturity model en quickscan voor managers

centrum informatiebeveiliging en privacybescherming

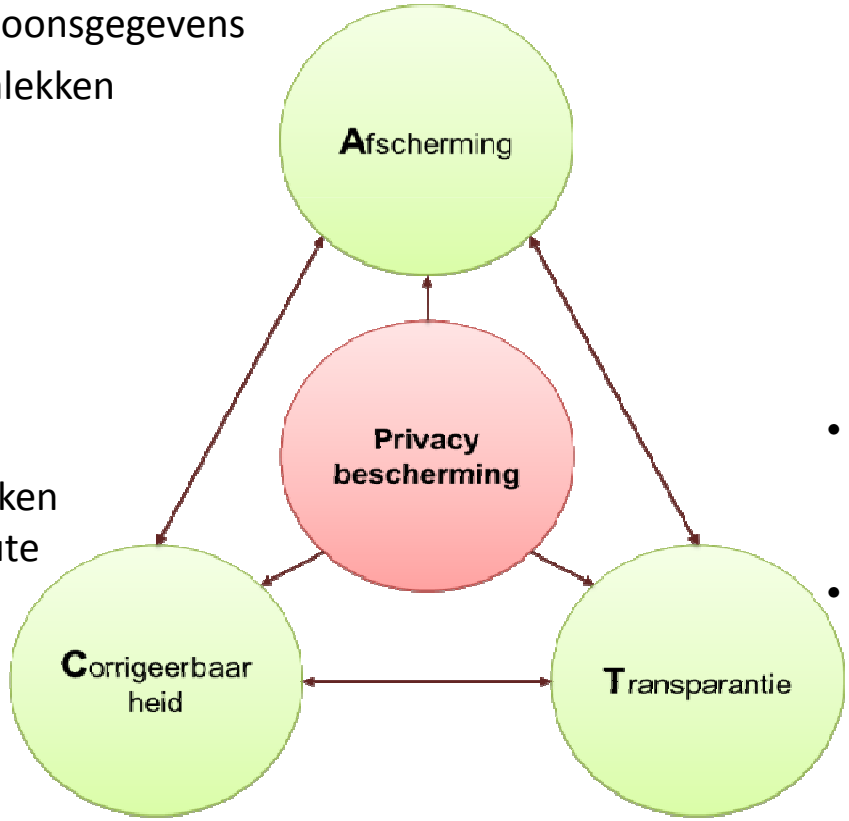
Grip op Privacy biedt handreikingen voor:



Privacy beschermen = ACT-doelen realiseren

Voorkomen van:

- onrechtmatige verwerking van persoonsgegevens
- datalekken



- Voorkomen van benadeling betrokken personen door foute registratie

- Bieden van inzicht aan betrokkene omtrent juistheid registratie
- In control brengen betrokkene en organisatie

centrum informatiebeveiliging en privacybescherming

Candleproblem

Grip op Privacy

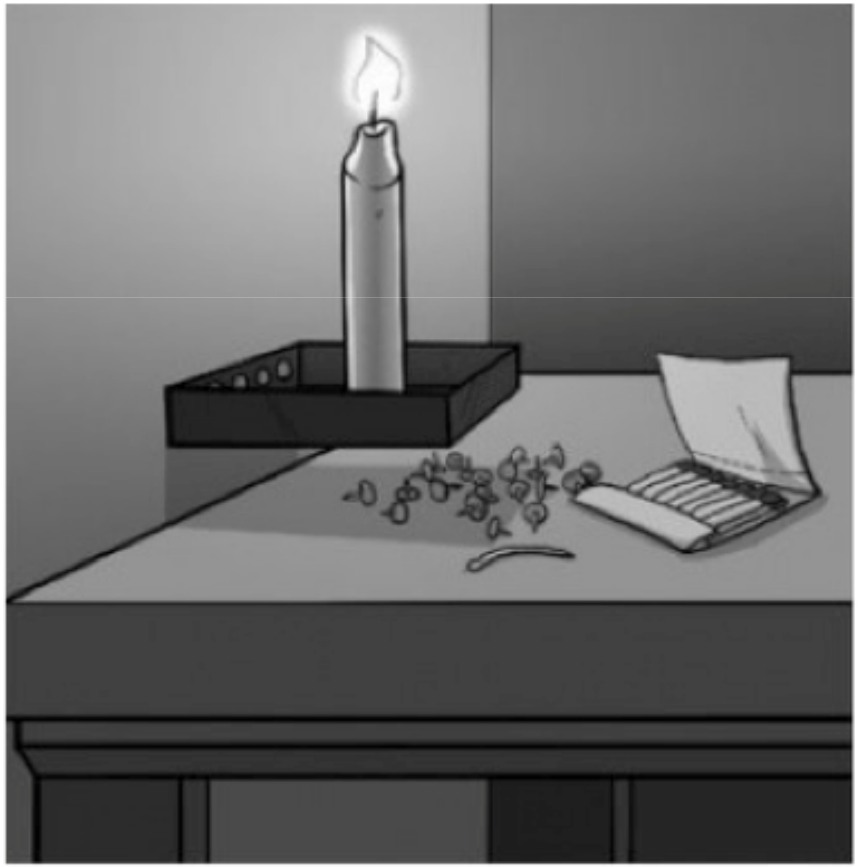
Privacy by Design

Privacy Governance

Privacy Baseline

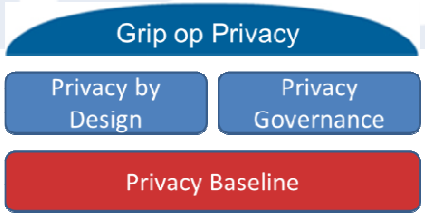
Problem: Fix the lit candle to the wall so that it will not drip wax onto the table below.

Oplossing



Zelfde eisen, beter gestructureerd

Geen nieuw normenkader



Privacy Baseline

- CIP heeft de wet- en regelgeving ontrafeld
- De ACT-doelen zijn vertaald naar een normenkader voor privacy
- De ordening van de normen maakt privacy-governance mogelijk
- De nomen zijn in de SIVA schrijfstijl geschreven
  - (eenduidig, ontdubbeld, compleet en uniform)
- De normen maken de wet bespreekbaar:
  - Geven aan <u>wat</u> <u>waar</u> gedaan moet worden.
  - Beschrijven de doelstellingen, de risico's en de vereisten om de doelstellingen te bereiken.

centrum informatiebeveiliging en privacybescherming

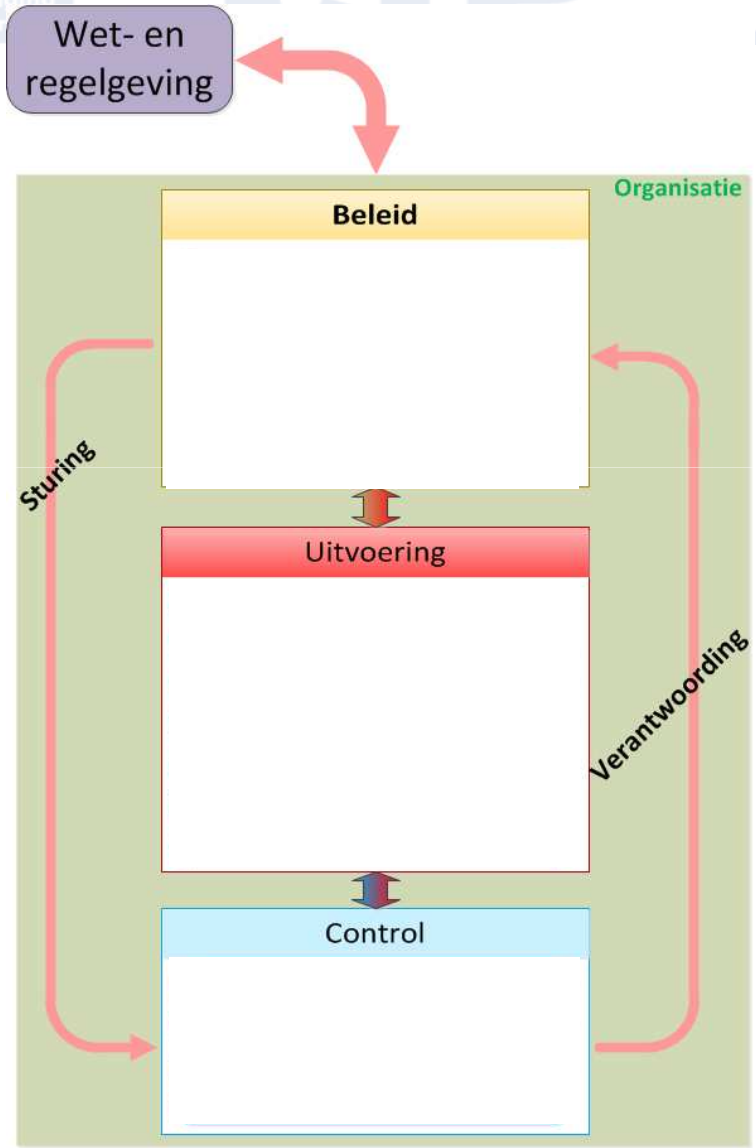
Privacy Baseline

Criteria zijn opgedeeld naar:

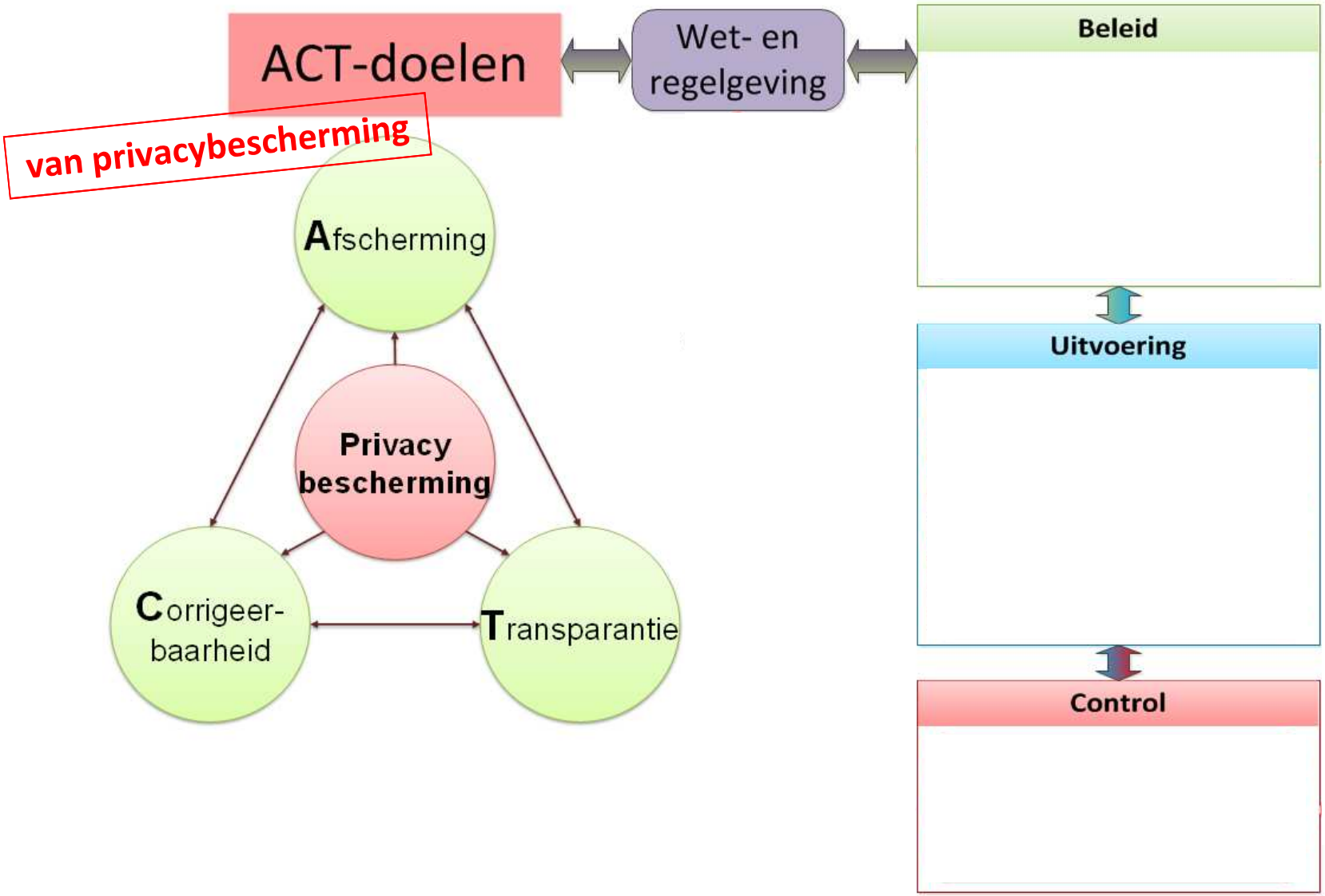
- **Beleid:**
  Geeft richting en kaders
- **Uitvoering:**
  Verwerkt persoonsgegevens
- **Control:**
  Toont compliancy aan

Resultaat:

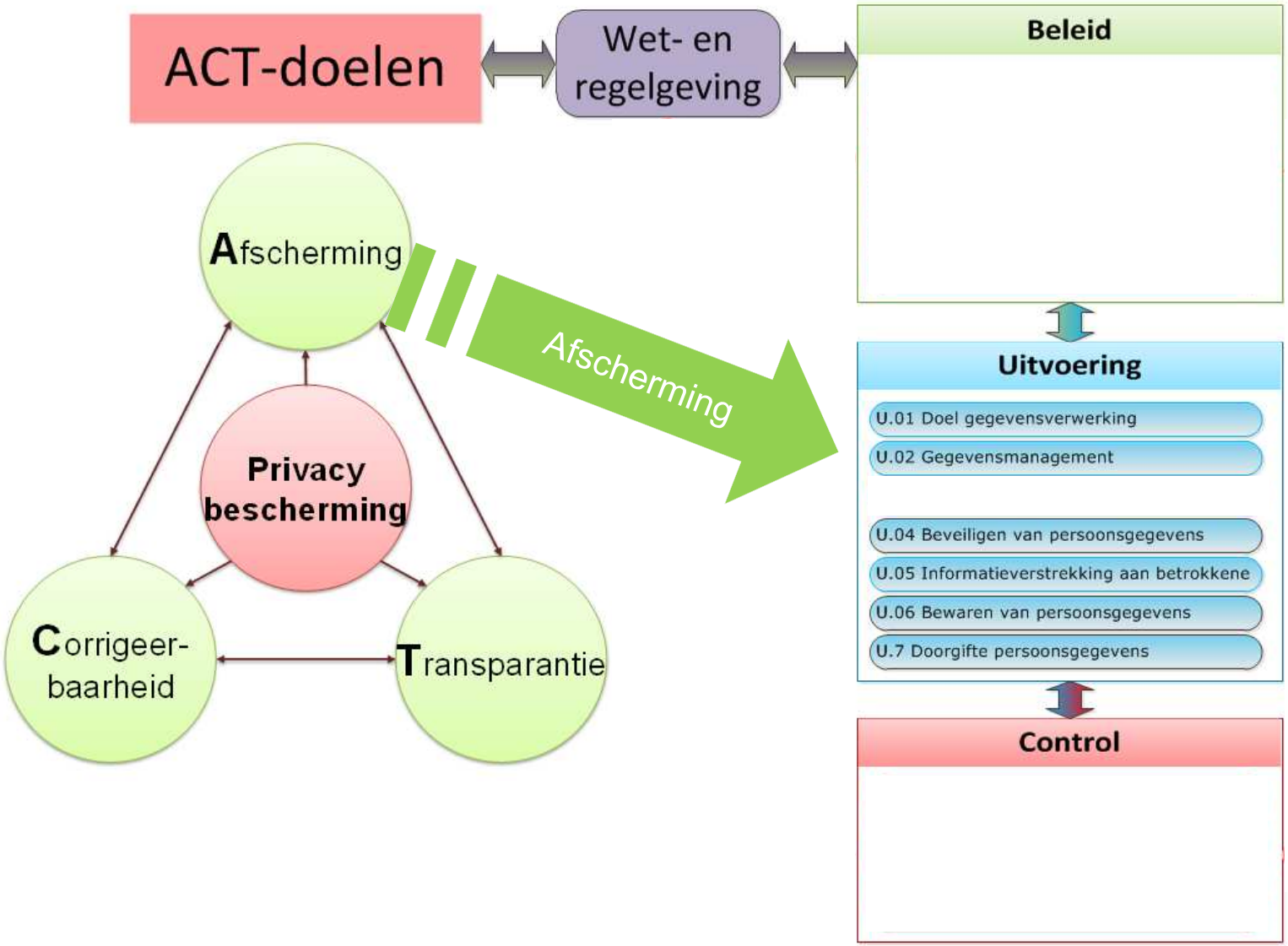
- Lerende organisatie
- Intern en extern toezicht en verantwoording
- Betere kwaliteit van dienstverlening



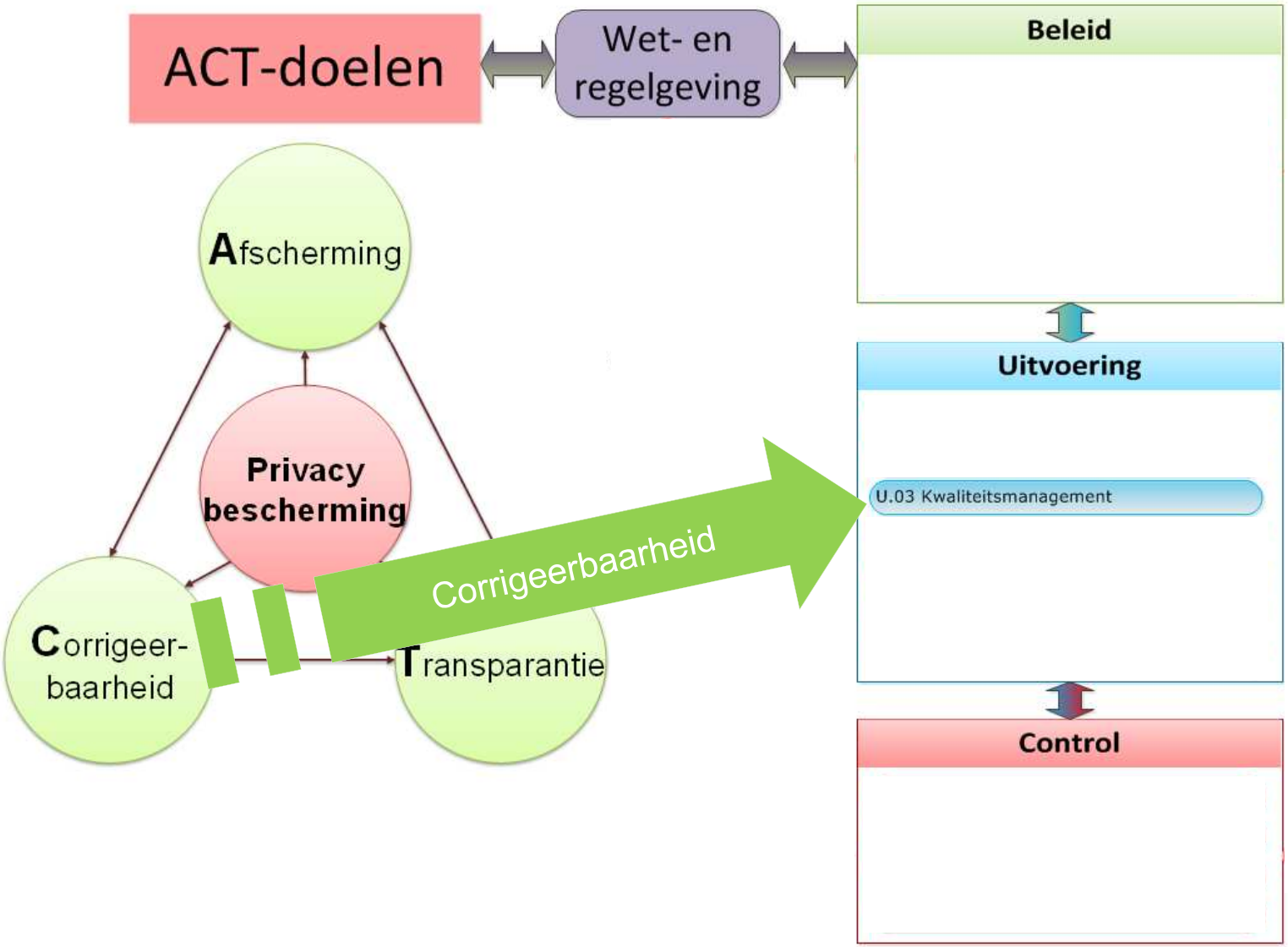
centrum informatiebeveiliging en privacybescherming



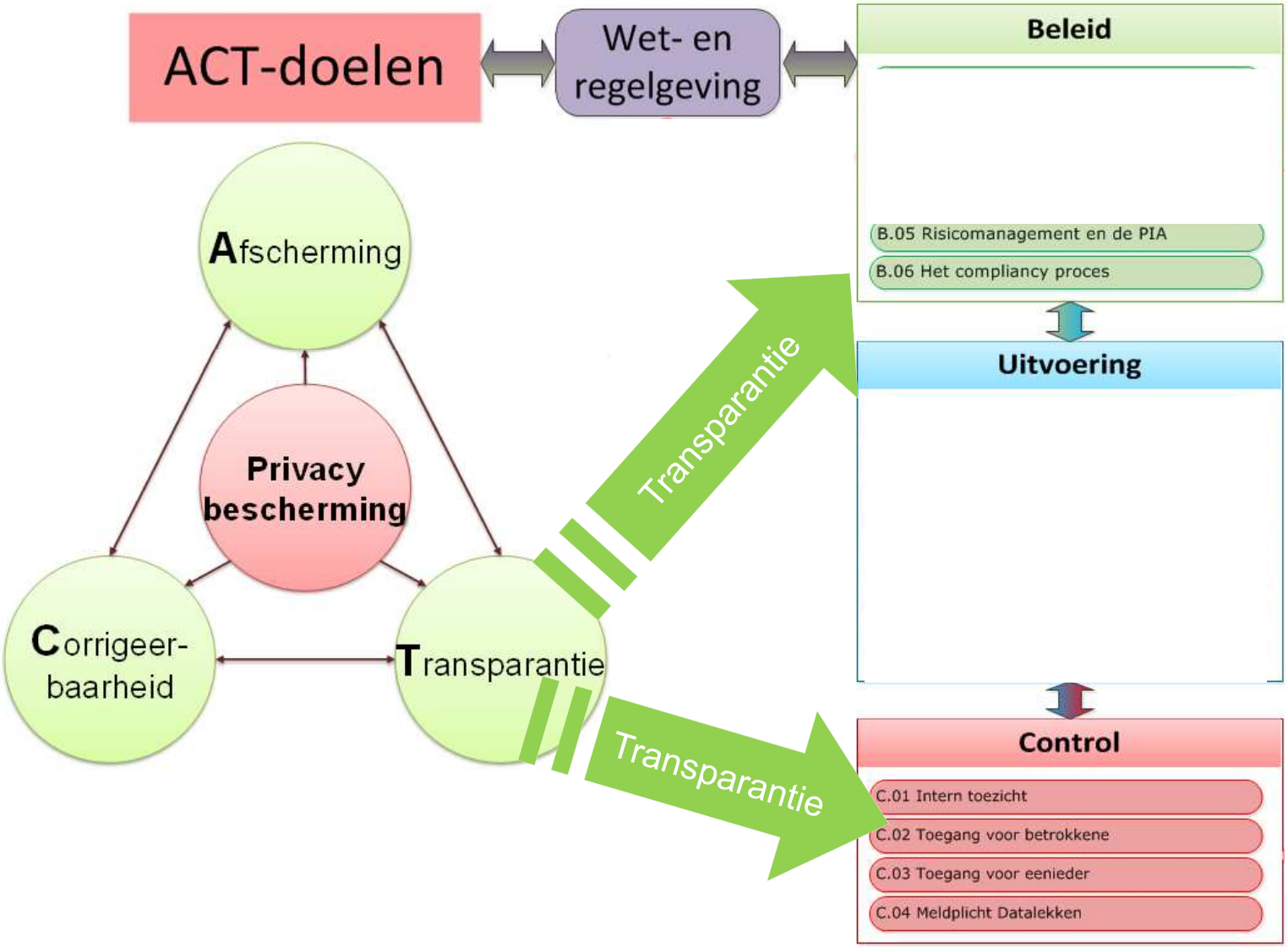
centrum informatiebeveiliging en privacybescherming



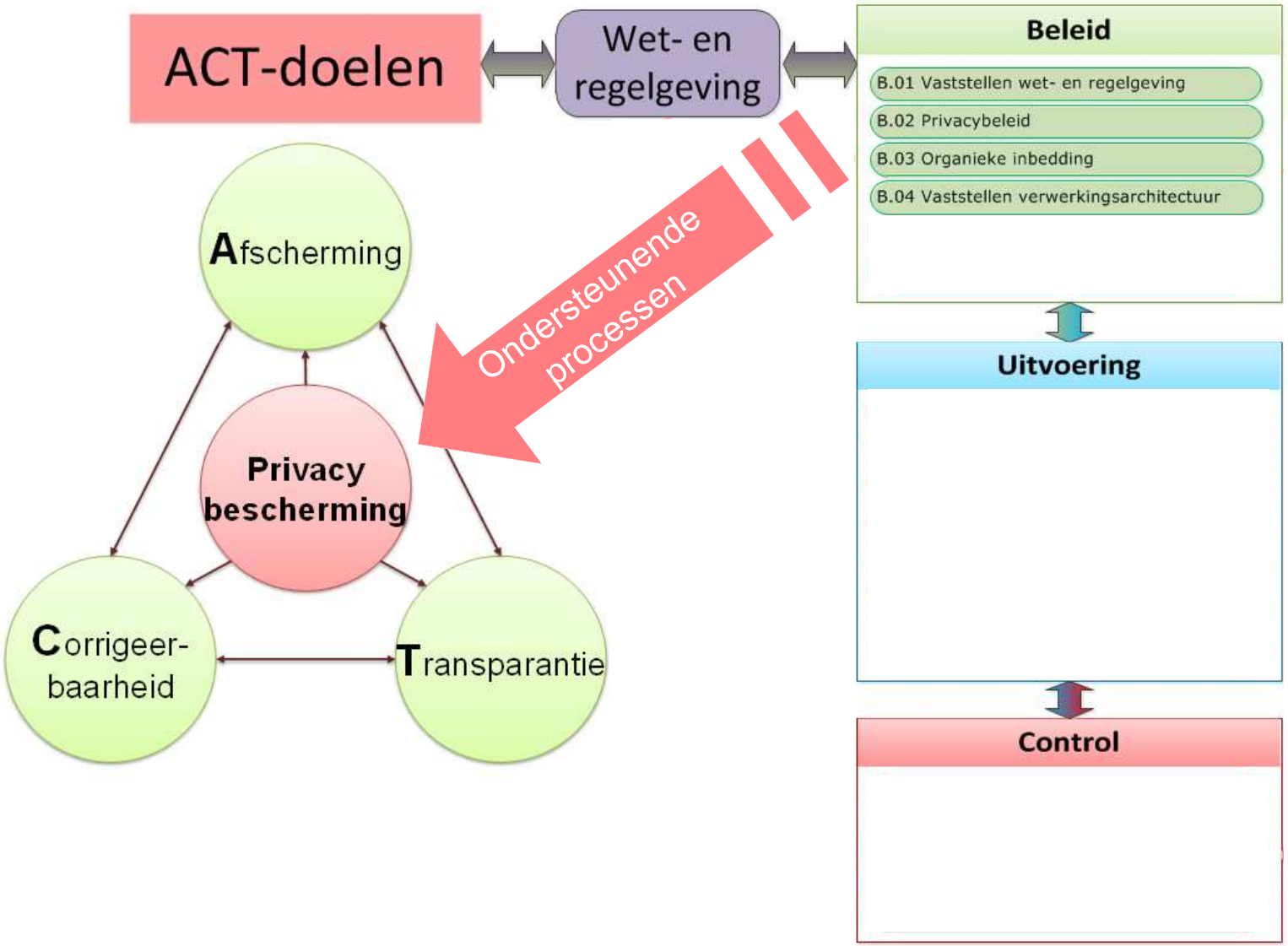
centrum informatiebeveiliging en privacybescherming



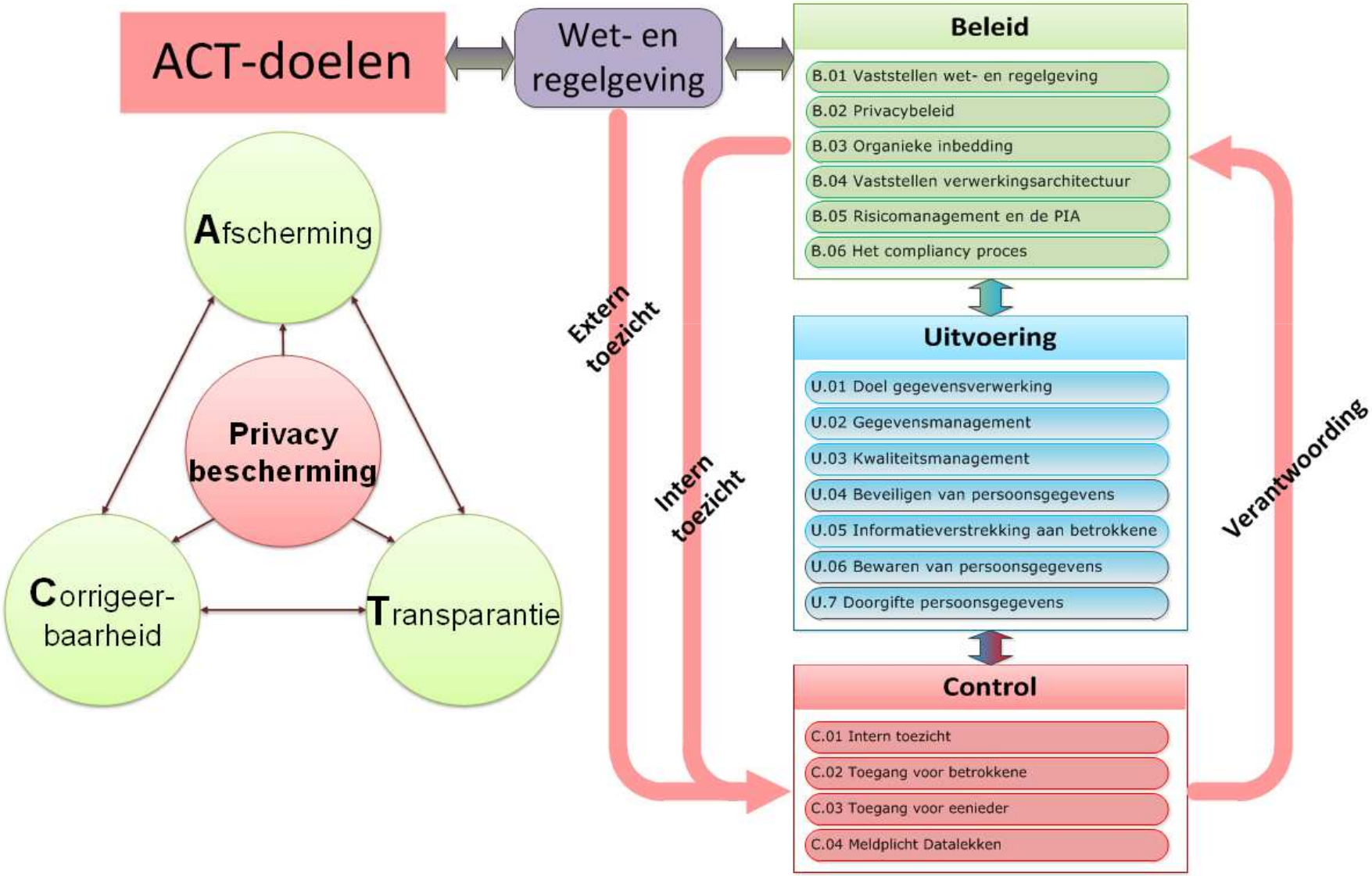
centrum informatiebeveiliging en privacybescherming



centrum informatiebeveiliging en privacybescherming



centrum informatiebeveiliging en privacybescherming



Hoe komen de handleidingen tot stand?

- Werkgroep met 20-tal deelnemers uit de CIP community
- Samenstelling kan wisselen
- Veel kennis voorhanden
- Inhoud aangedragen en gevraagd door:
  - leden van de werkgroep
  - interviews bij organisaties
  - Privacy Vraagbaak

RCJ

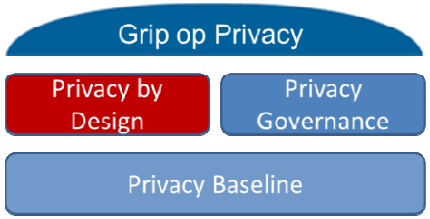
Vraaggericht
en
Aanbodgericht

Dia 18

RCJdB1 snap ik hier niet
Bruijn, Ruud de (R.C.J.) -CIP-; 17-10-2016

centrum informatiebeveiliging en privacybescherming

Handleiding Privacy by Design



Maakt ontwerpers bewust van het belang van privacy

Handvaten om de bescherming om de ACT-doelen mee te nemen in de ontwerpfasen en het ontwerp

Ondersteunt zowel het formele als het creatieve proces

Proactieve aanpak, voorkomt hoge kosten van aanpassingen achteraf

Een betere bedrijfsvoering is het resultaat. Dit leidt tot win-win

Privacy by Design gaat verder dan techniek.
De scope is de gehele verwerking van persoonsgegevens: systemen én bedrijfsprocessen.

Privacy by design

Gaat eigenlijk over:

Houding en gedrag ontwerpers

maar ook:

Waar in het ontwerpproces moet aan welk criterium gedacht worden

Principes in het ontwerpproces

Houding en gedrag ontwerpers

1. Proactief i.p.v. reactief; Preventief i.p.v. herstellend
2. Privacy als standaard
3. Privacy geïntegreerd in het ontwerp
4. Volledige functionaliteit – win-win in plaats van compromissen
5. Bescherming tijdens de volledige levenscyclus
6. Zichtbaarheid en transparantie – hou het open
7. Respect voor de privacy – laat de gebruiker centraal staan

Maar ook:
Waar in het ontwerpproces moet aan welk criterium gedacht worden

Inrichtingsprincipes voor het ontwerp

Principes voor de "bouw"

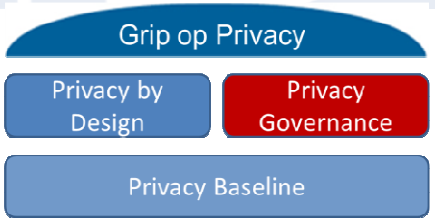
- Architectuurprincipes: Hoe wordt het ontwerp een succes?
  - Waar moet op gelet worden om aan de criteria te voldoen
  - Reduceren van de complexiteit
  - Beschikbare technologieën
- Extra principes bij de inzet van mobiele apparaten

De principes helpen de ontwerper bewust keuzen te maken

centrum informatiebeveiliging en privacybescherming

Handleiding Privacy Governance

Deze maand eerste conceptversie



Privacybescherming verhoogt de kwaliteit van de bedrijfsvoering door het leveren van betere diensten. Dit vraagt om sturing en een groeipad.

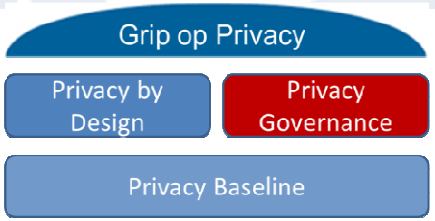
De Handleiding Privacy Governance geeft u handvaten om grip te krijgen op de privacybescherming.

Het Privacy Volwassenheidsmodel helpt u het ambitieniveau te kiezen en als organisatie daar naartoe te groeien.

De handleiding en het volwassenheidsmodel geven sturing aan een veranderperspectief, waarbij de kracht van de organisatie wordt benut.

Iedere organisatie bepaalt zelf het ambitieniveau

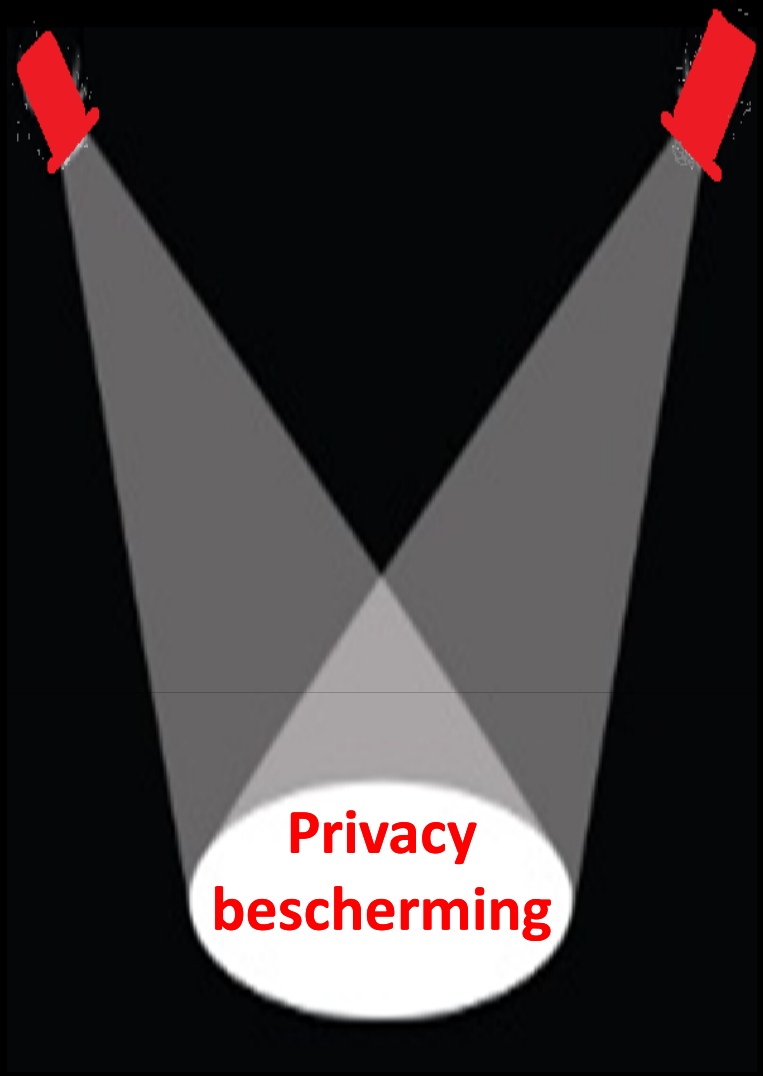
Privacy Governance: hoe?



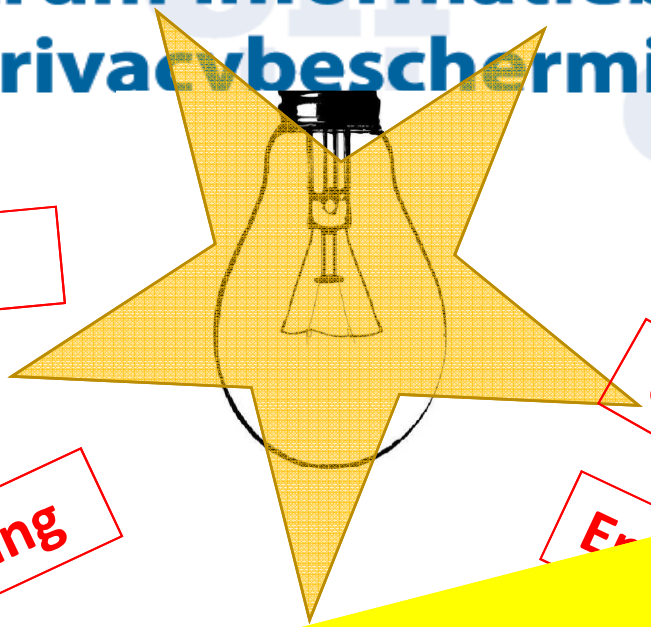
Principes van verandermanagement om de kracht van de organisatie te benutten.

Toegespitst op de ‘zachte’ veranderfactoren: een wet maakt niet vanzelf goede privacybescherming.

Wel: kritische succesfactoren: je wil natuurlijk wel ergens komen en dat kunnen vaststellen.


Privacy
bescherming

centrum informatiebeveiliging en privacybescherming



Procesontwerp

Ketenafspraken

Beleidsvorming

Informatiebeveiliging

centraal

Ex

dur

nagement

keting

omanagement

Audits

Externe invloeden

Security by Design

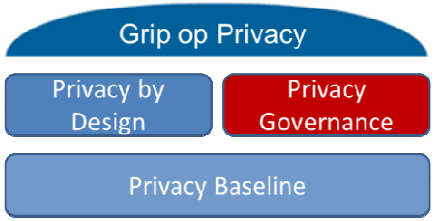
Governance

Privacybescherming:

De organisatie heeft meestal al veel op eigen kracht geregeld

centrum informatiebeveiliging en privacybescherming

Handleiding Privacy Governance



Deze maand eerste conceptversie

Privacybescherming verhoogt de kwaliteit van de bedrijfsvoering door het leveren van betere diensten. Dit vraagt om sturing en een groeipad.

De Handleiding Privacy Governance geeft u handvaten om grip te krijgen op de privacybescherming.

Het Privacy Volwassenheidsmodel helpt u passende ambitieniveau's te kiezen en als organisatie daar naartoe te groeien

Handleiding+volwassenheidsmodel geven sturing aan een verander-perspectief, dat gebruik maakt van de kracht van de organisatie.

Handleiding Privacy Governance

Als voorbeeld: COBIT managementguidelines

1. Doelstelling van de processen
2. Key Succes Factoren
3. Key Goal Indicatoren

Deze staan als indicatoren in de Privacy Baseline

Principes van verandermanagement om de kracht van de organisatie te benutten.

Hulpmiddel: Privacy Volwassenheidsmodel

- Per criterium uit de Privacy Baseline zijn 5 niveaus beschreven
- Volwassenheidsniveaus zijn meetbaar gemaakt
- Iedere organisatie bepaald zijn eigen ambitieniveau

norm: minimaal niveau 3

- Voor (kleine,) middelgrote en grote organisaties

- **Ambitieniveau wordt bespreekbaar**

‘goed huisvaderschap’

Volwassenheidsniveaus:

Inside out groeien

SIVA Lagenstructuur/Levels CMM	Level 0 Ad hoc	Level 1 Informeel	Level 2 Beheerst	Level 3 Vastgesteld	Level 4 Kwantitatief beheerst	Level 5 Geoptimaliseerd
Algemeen beleid domein						
Specifiek beleid domein						
Uitvoerend domein						
Specifiek control domein						
Algemeen control domein						

Hulpmiddel: Privacy Gap Analyse

Gekoppeld aan Privacy volwassenheidsmodel:

- Ontdek op welke punten privacy (on)voldoende aandacht krijgt binnen uw organisatie
- Ontdek het volwassenheidsniveau van de organisatie

Binnenkort eerste conceptversie

formatiebeveiliging
scherming

www.cip-overheid.nl

https://cip.pleio.nl/

Nog steeds bang?

Grip op Privacy:
De architecten krijgen de principes om te sturen op de organisatorische inrichting
en
de inrichting van de gegevensverwerkingen!

Vragen ?