ROSA architectuurscan Certificeringsschema

2017

Remco de Boer (Bureau Edustandaard)

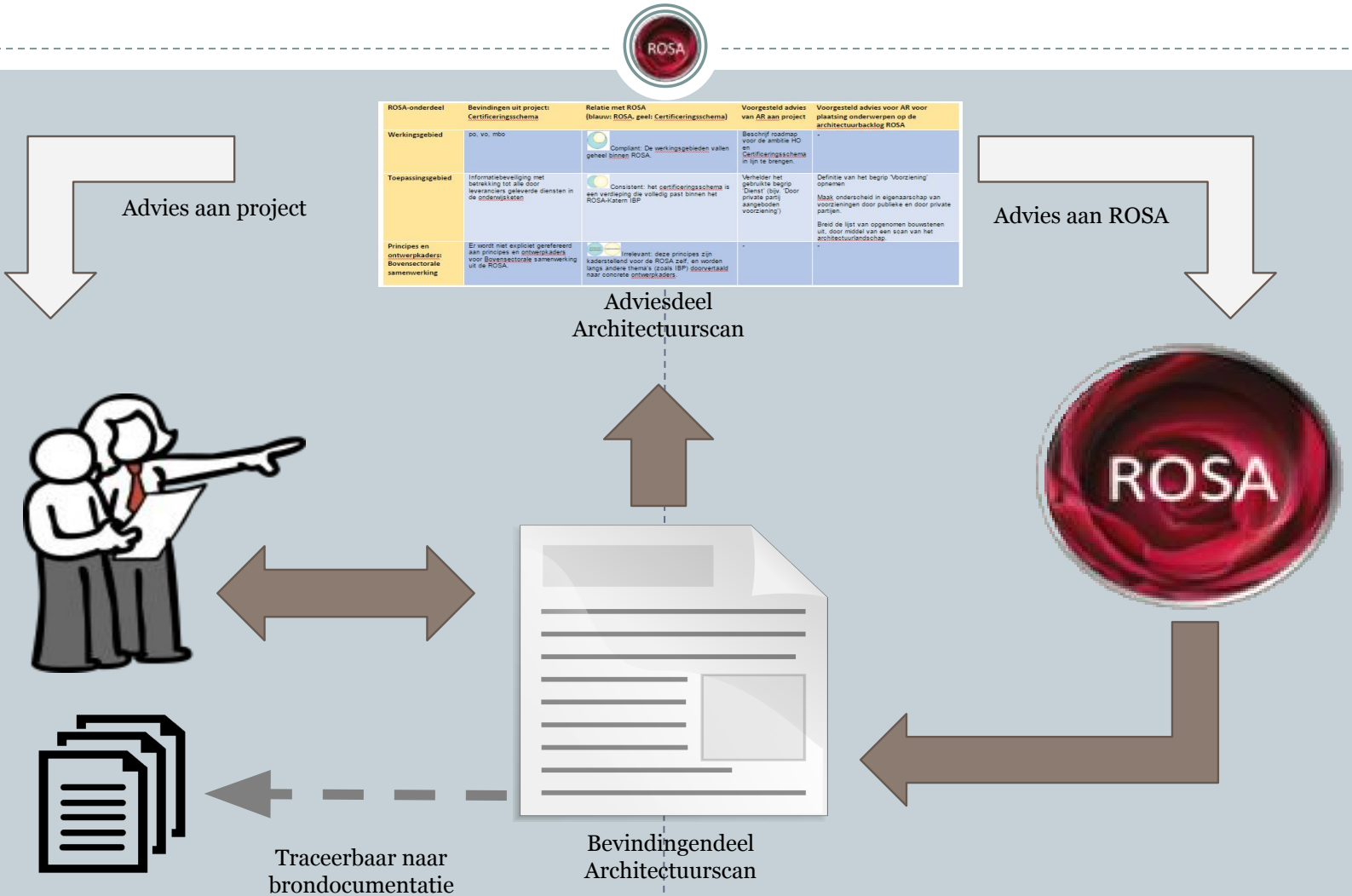
22 juni 2017
Architectuurraad

Agenda

- Doel:
  Besluit nemen: wel/niet positief advies geven aan de Standaardisatieraad over in-beheername van Certificeringsschema v.2017 bij Edustandaard.

- Vraagstelling:
  Is er iets in de architectuurscan van het CS dat het positieve advies aan de SR in de weg staat?

Architectuurscan



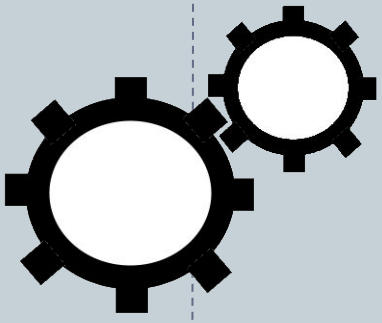
Uitgevoerde quickscan

Advies aan project

Advies aan ROSA

ROSA-onderdeel	Bevindingen uit project: Certificeringsschema	Relatie met ROSA (blauw: ROSA, geel: Certificeringsschema)	Voorgesteld advies van AR aan project	Voorgesteld advies voor AR voor plaatsing onderwerpen op de architectuurbacklog ROSA
Werkingsgebied	po, vo, mbo	Compliant: De werkingsgebieden vallen geheel binnen ROSA.	Beschrijf roadmap voor de ambitie HO en Certificeringsschema in lijn te brengen.	-
Toepassingsgebied	Informatiebeveiliging met betrekking tot alle door leveranciers geleverde diensten in de onderwijssfeer	Consistent: het certificeringsschema is een verdieping die volledig past binnen het ROSA-kaderm IBP.	Verhelder het gebruikte begrip 'Dienst' (bijv. 'Door private partij aangeboden voorziening')	Definitie van het begrip 'Voorziening' opnemen Maak onderscheid in eigenaarschap van voorzieningen door publieke en door private partijen. Breid de lijst van opgenomen bouwstenen uit, door middel van een scan van het architectuurlandschap.
Principes en ontwerpkaders: Bovensectorale samenwerking	Er wordt niet expliciet gerefereerd aan principes en ontwerpkaders voor Bovensectorale samenwerking uit de ROSA.	Irrelevant: deze principes zijn kaderstellend voor de ROSA zelf, en worden langs andere thema's (zoals IBP) doorvertaald naar concrete ontwerpkaders.	-	-

Adviesdeel
Architectuurscan



Analyse
door Bureau Edustandaard;
geen separaat bevindingendeel

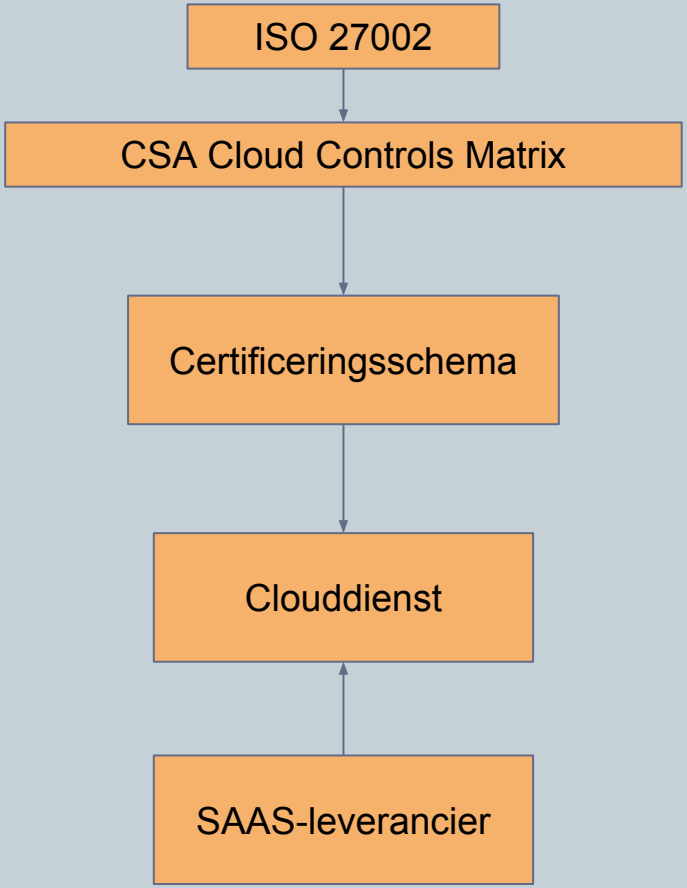
Selectie relevante onderdelen

Geraadpleegde brondocumentatie

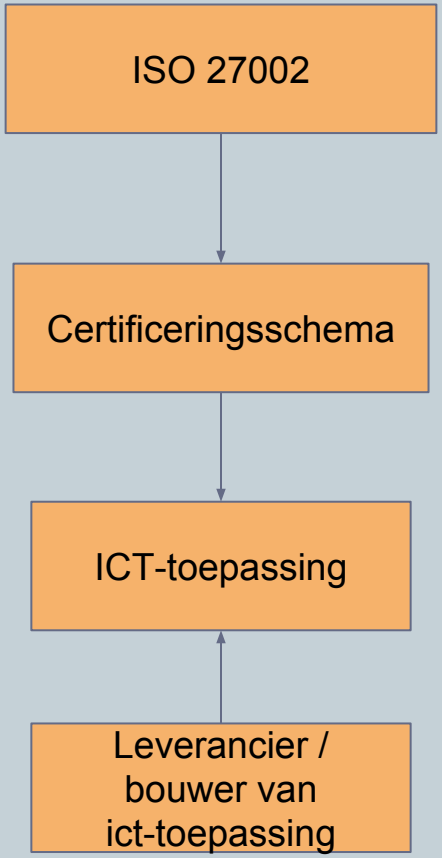
- *Certificeringsschema algemene beschrijving v2.03*
- *Certificeringsschema proces v2.03*
- *Certifceringsschema classificatie v1.7*
- *Certificeringsschema toetsingskader v0.9*
- *Certificeringsschema toezicht v2.02*

Belangrijke verschillen

Certificeringsschema v1.1



Certificeringsschema 2017



Opbouw Certificeringsschema

Certificeringsschema

Algemene beschrijving

Proces
Toepassing van het CS

Classificatieschema
Bepaling gewenste niveaus

Toetsingskader
Bepaling te nemen maatregelen

Toezicht
Beoordeling genomen maatregelen

Overzicht resultaten

ROSA-onderdeel	Relatie met ROSA	Adviezen mbt product/context?	Adviezen mbt AR/ROSA?
Werkings-gebied 	**Fully conformant**		
Toepassings-gebied 	**Compliant**	✔	✔
Bovensectorale samenwerking 	*Onbepaald*		
Informatie-beveiliging en privacy (IBP) 	**Compliant**	✔	✔
IAA 	*Onbepaald*		
Gegevens-uitwisseling in de keten 	*Onbepaald*		
Zeggen-schappen en gegevenssoorten 	**Nonconformant**	✔	
Keten-processen 	**Fully conformant**		
Bouwstenen en voorzieningen 	**Fully conformant**		
Architecturele randvoorwaarden	*Edukoppeling*	✔	✔
Beheer en (door)ontwikkeling	*Kortcyclische aanpassingen*		✔

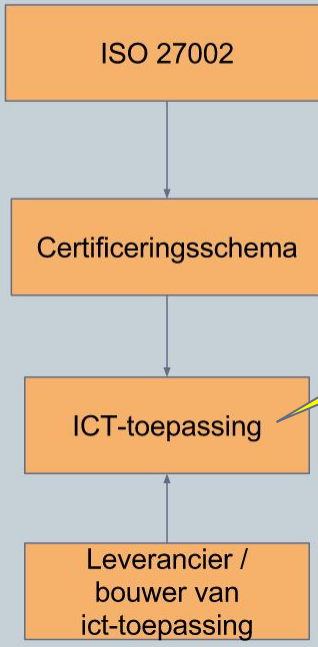
Werkingsgebied: Fully conformant

Het certificeringsschema is van toepassing op het gehele onderwijsdomein.

Implementatie vindt op dit moment voornamelijk plaats in de sectoren po, vo, mbo. Daarnaast is het certificeringsschema onlosmakelijk verbonden aan implementaties van de Edukoppeling Transactiestandaard.

Toepassingsgebied: Compliant

Certificeringsschema 2017



Toepassingsgebied: alle ict-toepassingen in het onderwijs

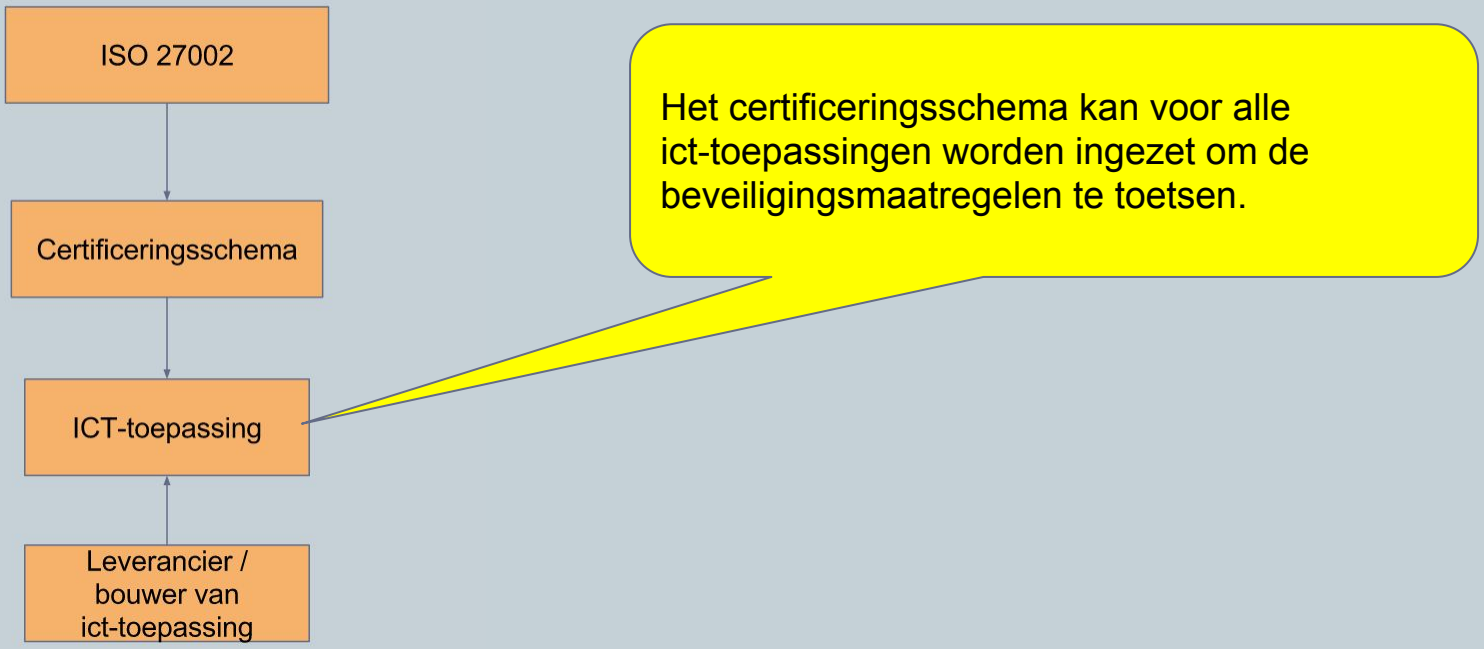
Adviezen

CS: Definieer het begrip “ict-toepassing”

ROSA: Overweeg het ROSA-begrip “voorziening” te vervangen door het begrip “ict-toepassing” - Binnen het certificeringsschema is bewust gekozen voor gebruik van het begrip “ict-toepassing” in plaats van “voorziening”. De herkenbaarheid van het begrip “ict-toepassing” blijkt namelijk groter. De strekking van beide begrippen is gelijkaardig.

Bouwstenen en voorzieningen
Fully Conformant

Certificeringsschema 2017

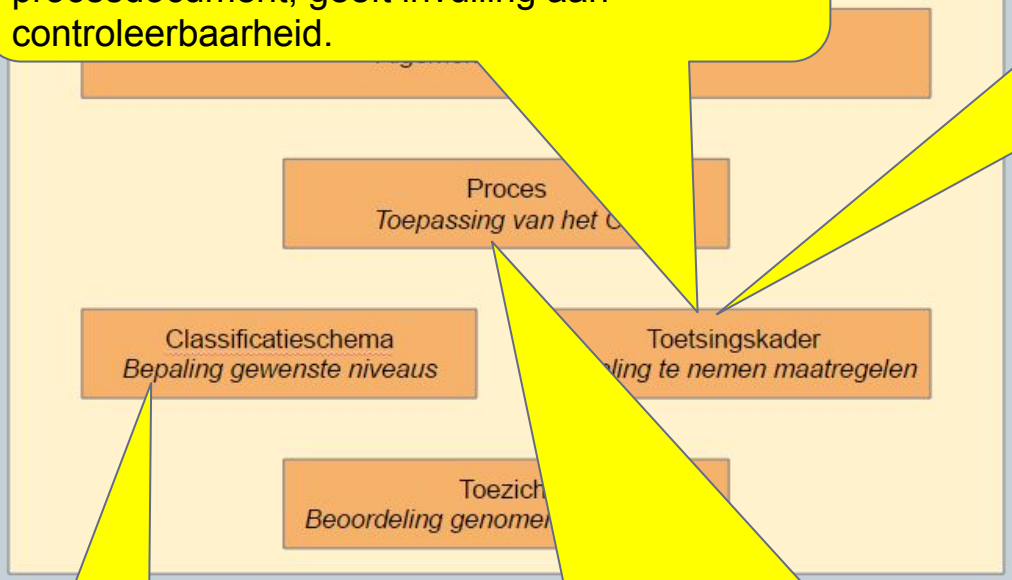


Ketenprocessen: Fully conformant

IBP (ROSA): Compliant

Het aspect ‘Controleerbaarheid’ is niet (apart) opgenomen in het toetsingskader CS. De rapportage, beschreven in het procesdocument, geeft invulling aan controleerbaarheid.

Het certificeringsschema (CS) hanteert in het toetsingskader (iets) andere definities voor BIV dan het ROSA-katern IBP



Adviezen

CS: Beargumenteer waarom de BIV-definities en -classificaties in het certificeringsschema afwijken van die in het ROSA-katern IBP. Deze rationale kan mogelijk leiden tot aanpassing van het katern IBP. Het uitgangspunt zou moeten zijn in ieder geval gelijke definities en classificaties te hanteren.

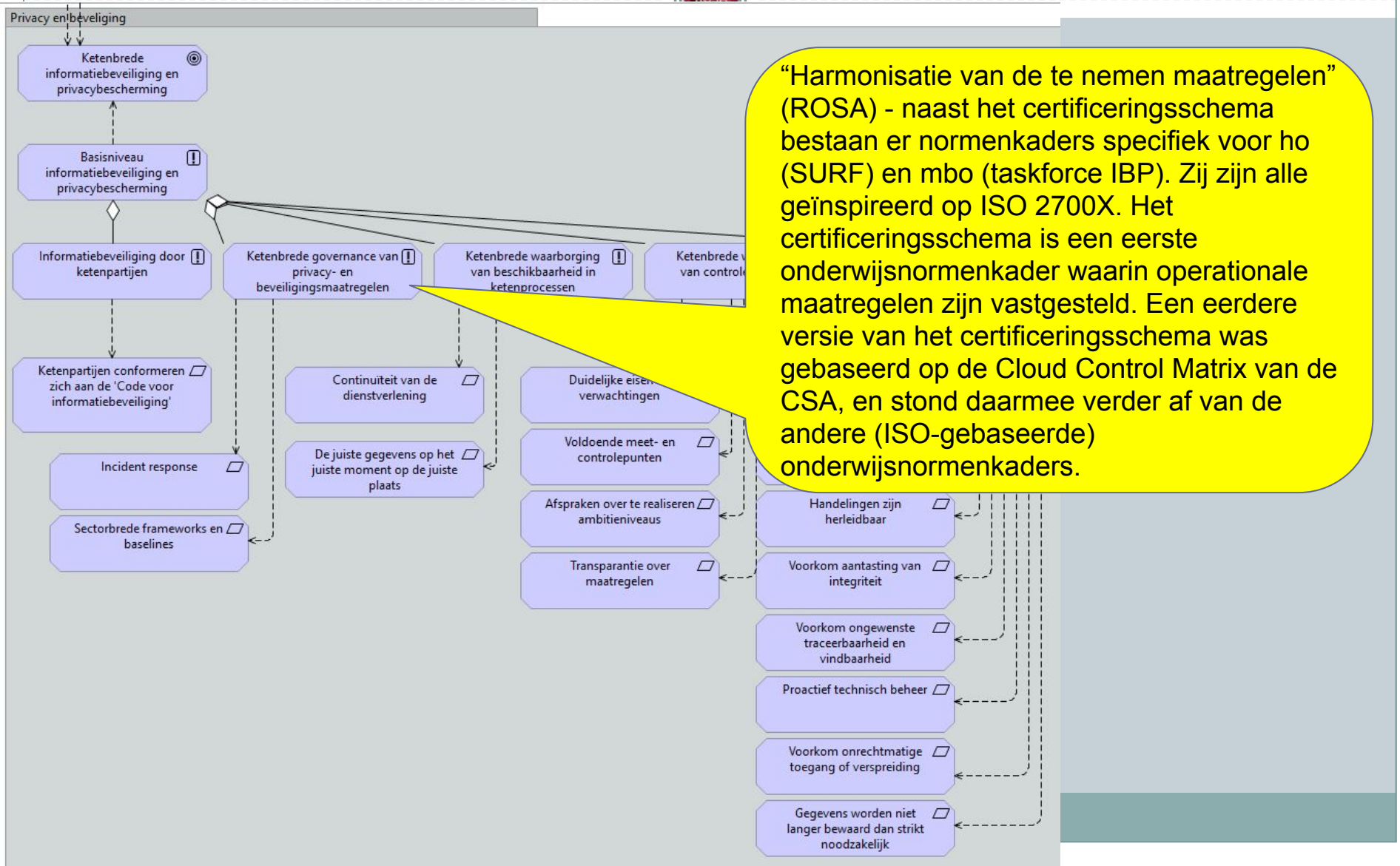
ROSA: Overweeg
- Overnemen/vervangen definities BIV en BIV classificatie

(vereist uitleg waarom afgeweken is)

BIV-classificatie in CS (Basis / Standaard / Hoog) wijkt af van ROSA katern IBP (L/M/H)

Het ROSA-katern IBP beschrijft risicoanalyse vanuit (keten)processen, het CS vanuit voorziening/ICT-toepassing. In de procesbeschrijving van het CS lopen teksten over het proces van toepassing van CS en het (keten)proces waarbinnen de desbetreffende ict-toepassing wordt gebruikt wat door elkaar. Noodzakelijkerwijs wordt de ict-toepassing als vertrekpunt genomen, maar wel beschouwd in zijn context (waaronder het ketenproces en de eisen die dat proces stelt).

IBP (ROSA): Compliant



"Harmonisatie van de te nemen maatregelen" (ROSA) - naast het certificeringsschema bestaan er normenkaders specifiek voor ho (SURF) en mbo (taskforce IBP). Zij zijn alle geïnspireerd op ISO 2700X. Het certificeringsschema is een eerste onderwijsnormenkader waarin operationale maatregelen zijn vastgesteld. Een eerdere versie van het certificeringsschema was gebaseerd op de Cloud Control Matrix van de CSA, en stond daarmee verder af van de andere (ISO-gebaseerde) onderwijsnormenkaders.

IBP (ROSA): Compliant

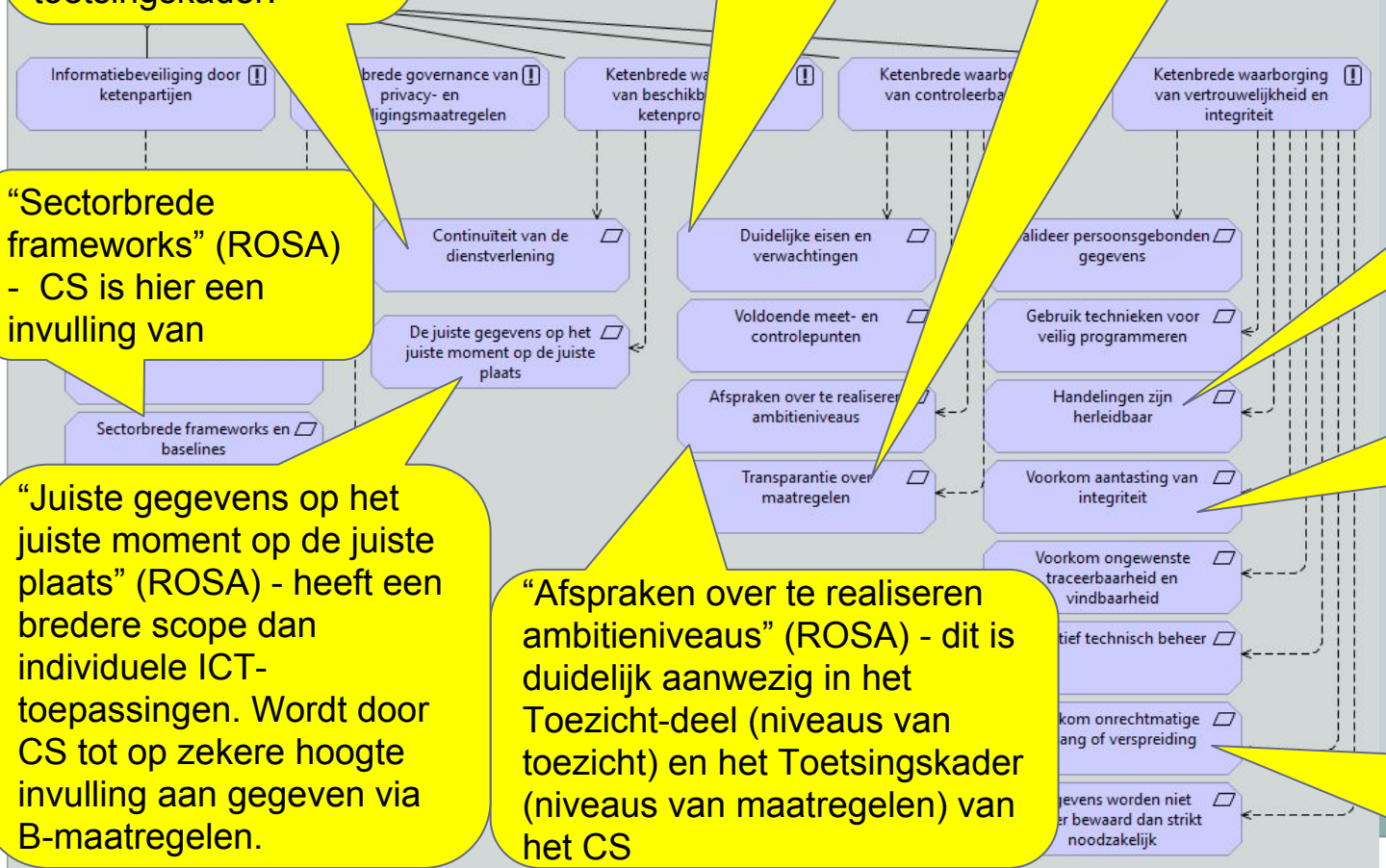
“Continuiteit vd dienstverlening” (ROSA) - is een aparte kolom (business continuity) in het CS toetsingskader.

“Duidelijke eisen en verwachtingen” (ROSA) - CS geeft invulling aan eisen en verwachtingen op een specifiek toepassingsgebied (nl. ICT-toepassingen)

“Transparantie over maatregelen” (ROSA) - het CS maakt de te nemen maatregelen transparant, de auditverklaring de genomen maatregelen.

“Handelingen zijn herleidbaar” (ROSA) - komt terug in de kolommen logging en onweerlegbaarheid in BIV

“Sectorbrede frameworks” (ROSA) - CS is hier een invulling van



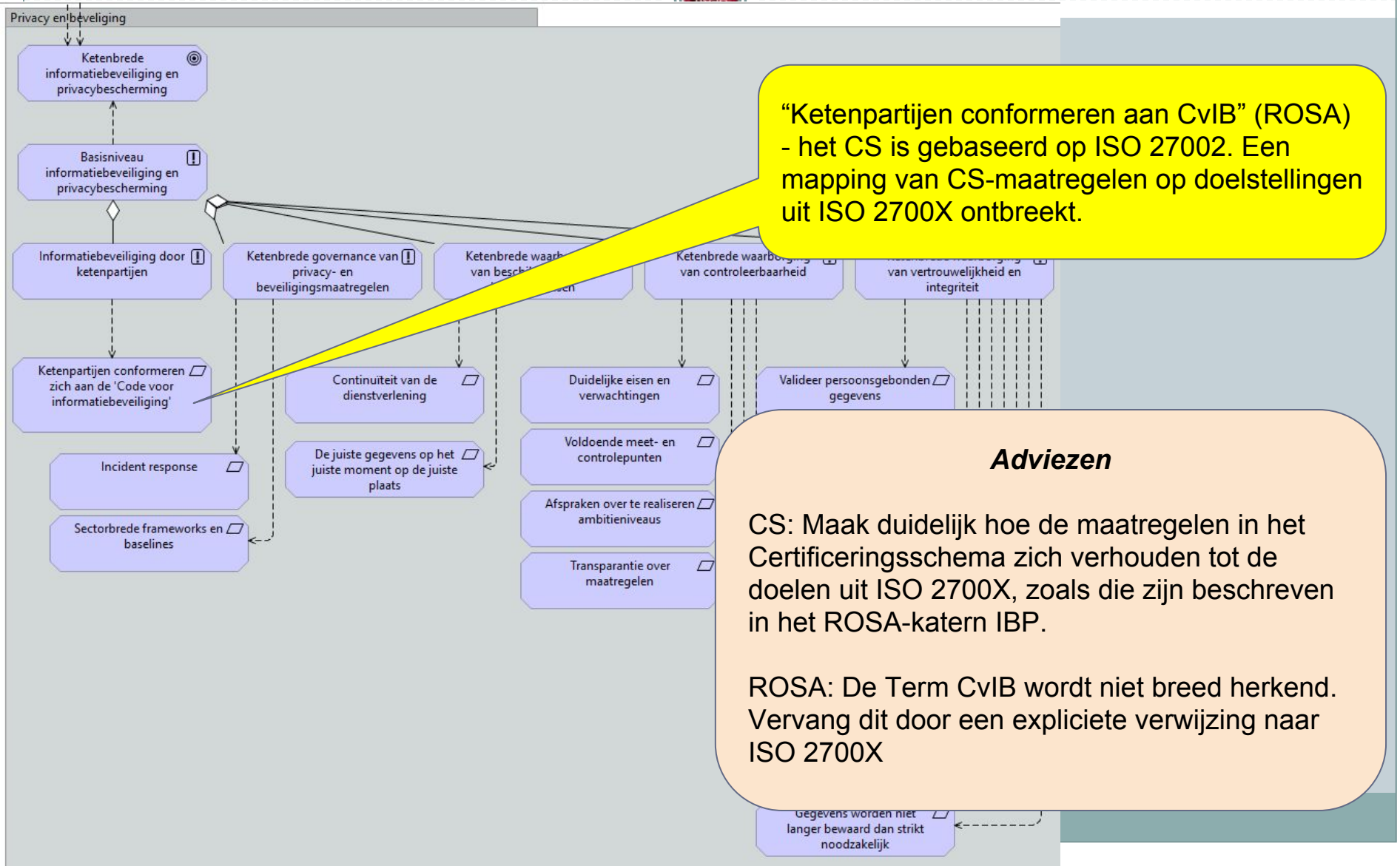
“Voorkom aantasting van integriteit” (ROSA) - komt in het CS terug in de I-maatregelen

“Juiste gegevens op het juiste moment op de juiste plaats” (ROSA) - heeft een bredere scope dan individuele ICT-toepassingen. Wordt door CS tot op zekere hoogte invulling aan gegeven via B-maatregelen.

“Afspraken over te realiseren ambitieniveaus” (ROSA) - dit is duidelijk aanwezig in het Toezicht-deel (niveaus van toezicht) en het Toetsingskader (niveaus van maatregelen) van het CS

“Voorkom onrechtmatige toegang” (ROSA) - komt in het CS terug via I/V maatregelen

IBP (ROSA): Compliant



"Ketenpartijen conformeren aan CvIB" (ROSA) - het CS is gebaseerd op ISO 27002. Een mapping van CS-maatregelen op doelstellingen uit ISO 2700X ontbreekt.

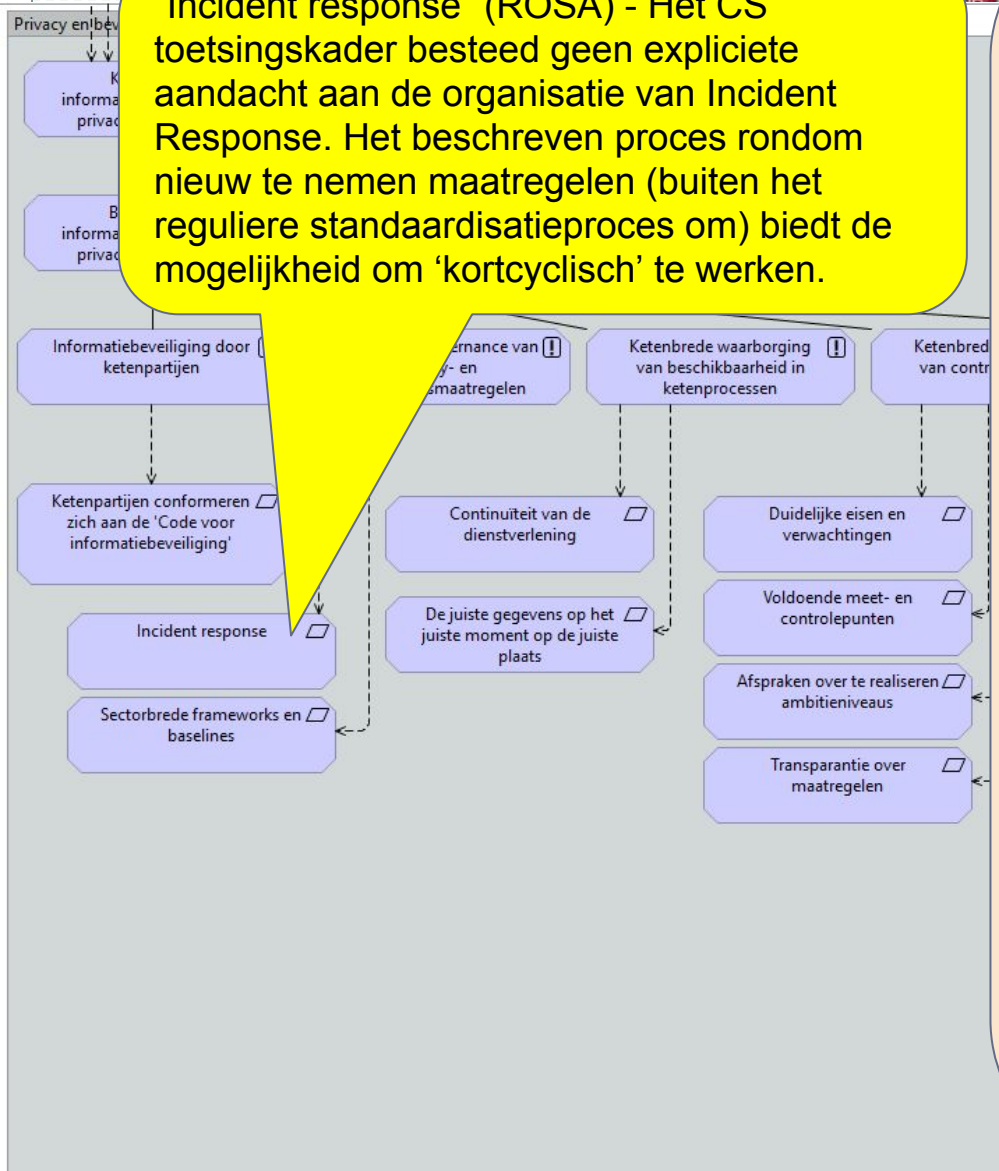
Adviezen

CS: Maak duidelijk hoe de maatregelen in het Certificeringsschema zich verhouden tot de doelen uit ISO 2700X, zoals die zijn beschreven in het ROSA-katern IBP.

ROSA: De Term CvIB wordt niet breed herkend. Vervang dit door een expliciete verwijzing naar ISO 2700X

IBP (ROSA): Compliant

“Incident response” (ROSA) - Het CS toetsingskader besteed geen expliciete aandacht aan de organisatie van Incident Response. Het beschreven proces rondom nieuw te nemen maatregelen (buiten het reguliere standaardisatieproces om) biedt de mogelijkheid om ‘kortcyclisch’ te werken.



Adviezen

CS

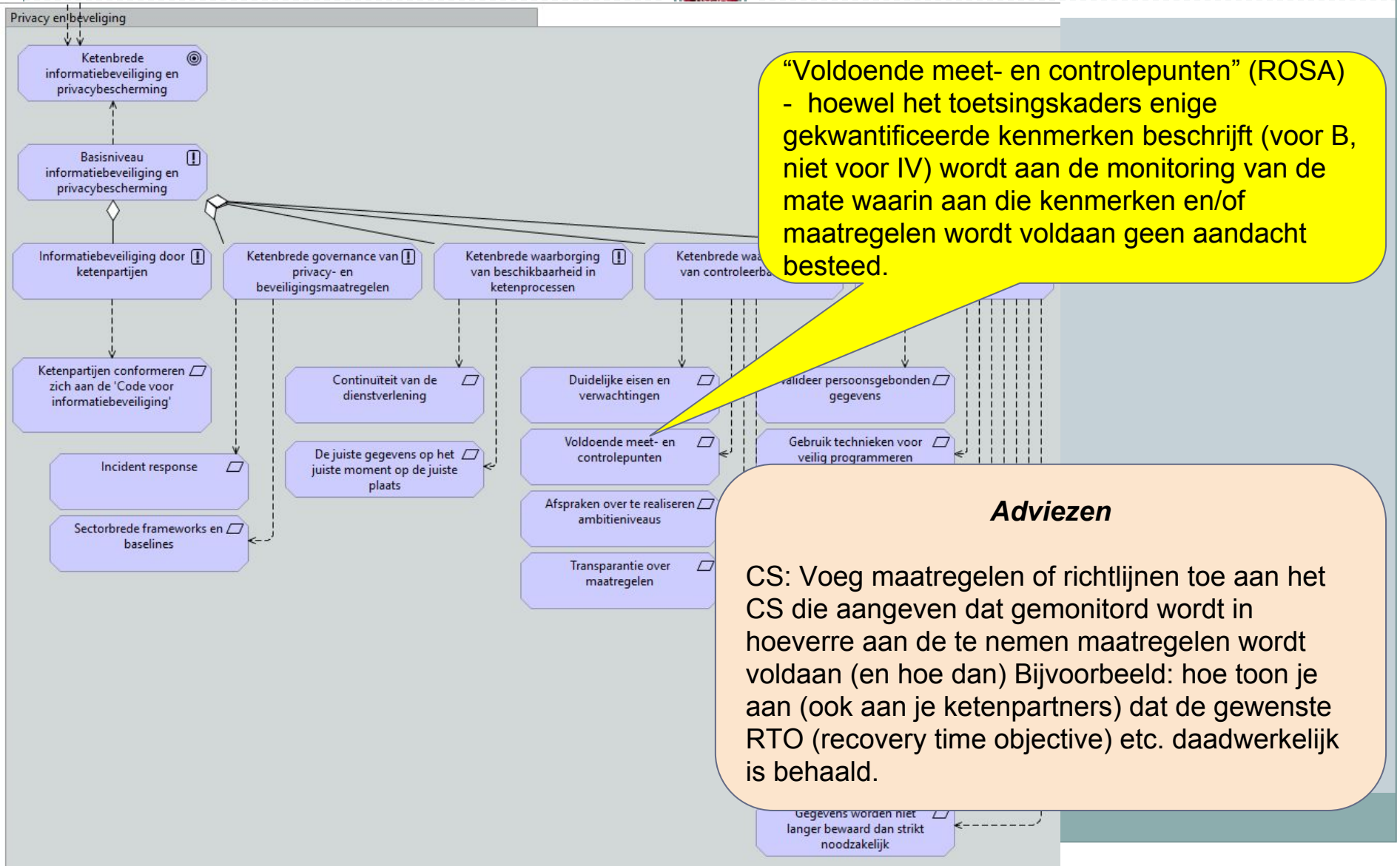
Overweeg maatregelen toe te voegen mbt incident response (detectie + opvolging)
Overweeg maatregelen te koppelen aan fasen in PDRC-cyclus

Definieer communicatielijnen en proces bij (acute) dreigingen en gewijzigde dreigingsbeelden die nopen tot nieuwe/aanvullende maatregelen
Bijeenroepen WG en besluitvorming
Actieve communicatie nieuwe maatregelen aan gebruikers van het certificeringsschema (leverancier, instellingen, organisaties aangesloten op Edukoppeling)
Termijn voor opstellen nieuwe auditverklaring? (cf. Auditverklaring punt 3, nu alleen voor ingrijpende wijzigingen IN DE DIENST zelf)

ROSA

Besteed bij het ontwerpkader Incident Response aandacht aan de zgn. PDRC-cyclus (preventie, detectie, repressie, correctie).Incident Response begint bij het gestructureerd kunnen herkennen en vervolgens reageren op incidenten

IBP (ROSA): Compliant

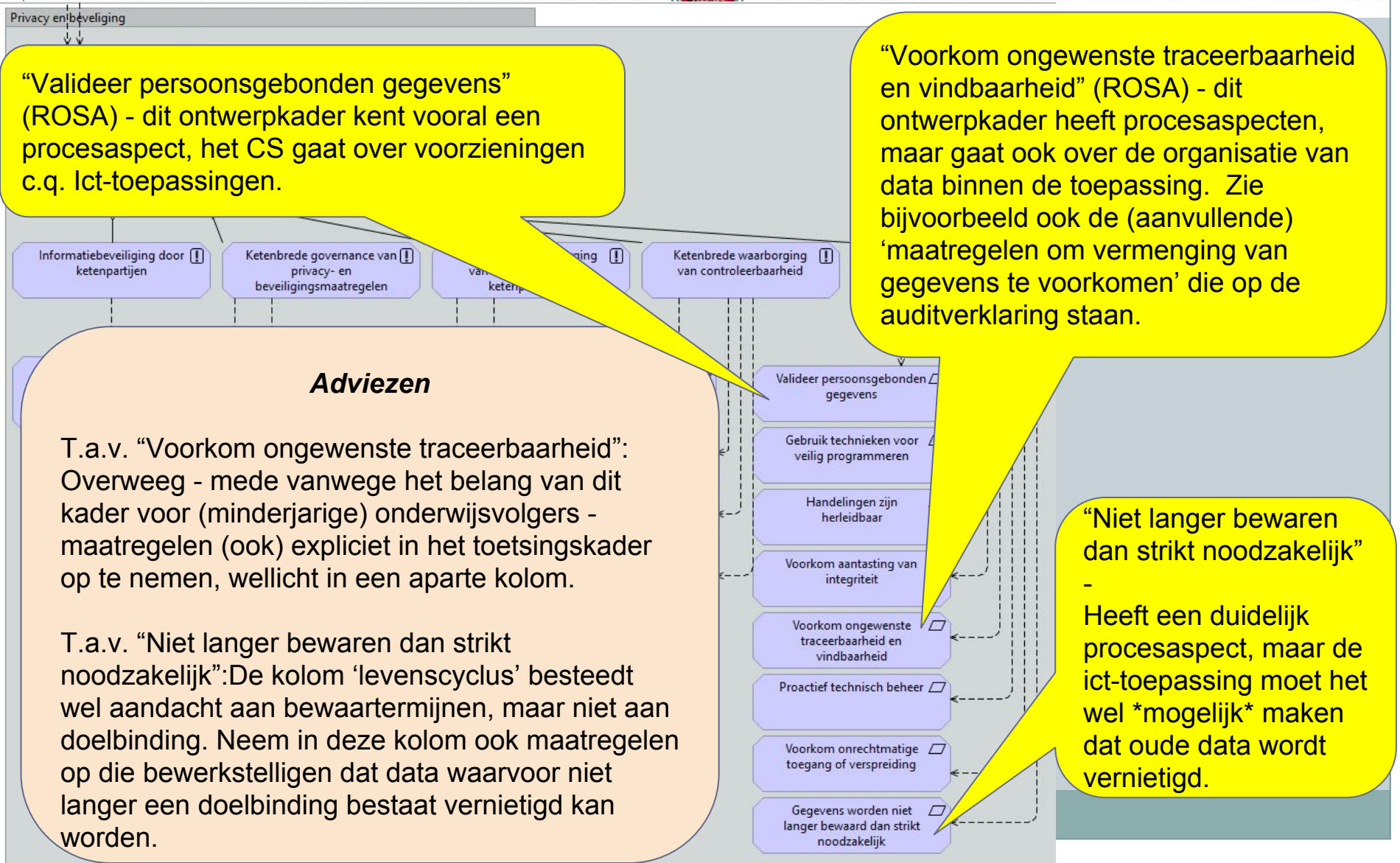


"Voldoende meet- en controlepunten" (ROSA) - hoewel het toetsingskaders enige gekwantificeerde kenmerken beschrijft (voor B, niet voor IV) wordt aan de monitoring van de mate waarin aan die kenmerken en/of maatregelen wordt voldaan geen aandacht besteed.

Adviezen

CS: Voeg maatregelen of richtlijnen toe aan het CS die aangeven dat gemonitord wordt in hoeverre aan de te nemen maatregelen wordt voldaan (en hoe dan) Bijvoorbeeld: hoe toon je aan (ook aan je ketenpartners) dat de gewenste RTO (recovery time objective) etc. daadwerkelijk is behaald.

IBP (ROSA): Compliant



"Valideer persoonsgebonden gegevens" (ROSA) - dit ontwerpkader kent vooral een procesaspect, het CS gaat over voorzieningen c.q. Ict-toepassingen.

"Voorkom ongewenste traceerbaarheid en vindbaarheid" (ROSA) - dit ontwerpkader heeft procesaspecten, maar gaat ook over de organisatie van data binnen de toepassing. Zie bijvoorbeeld ook de (aanvullende) 'maatregelen om vermenging van gegevens te voorkomen' die op de auditverklaring staan.

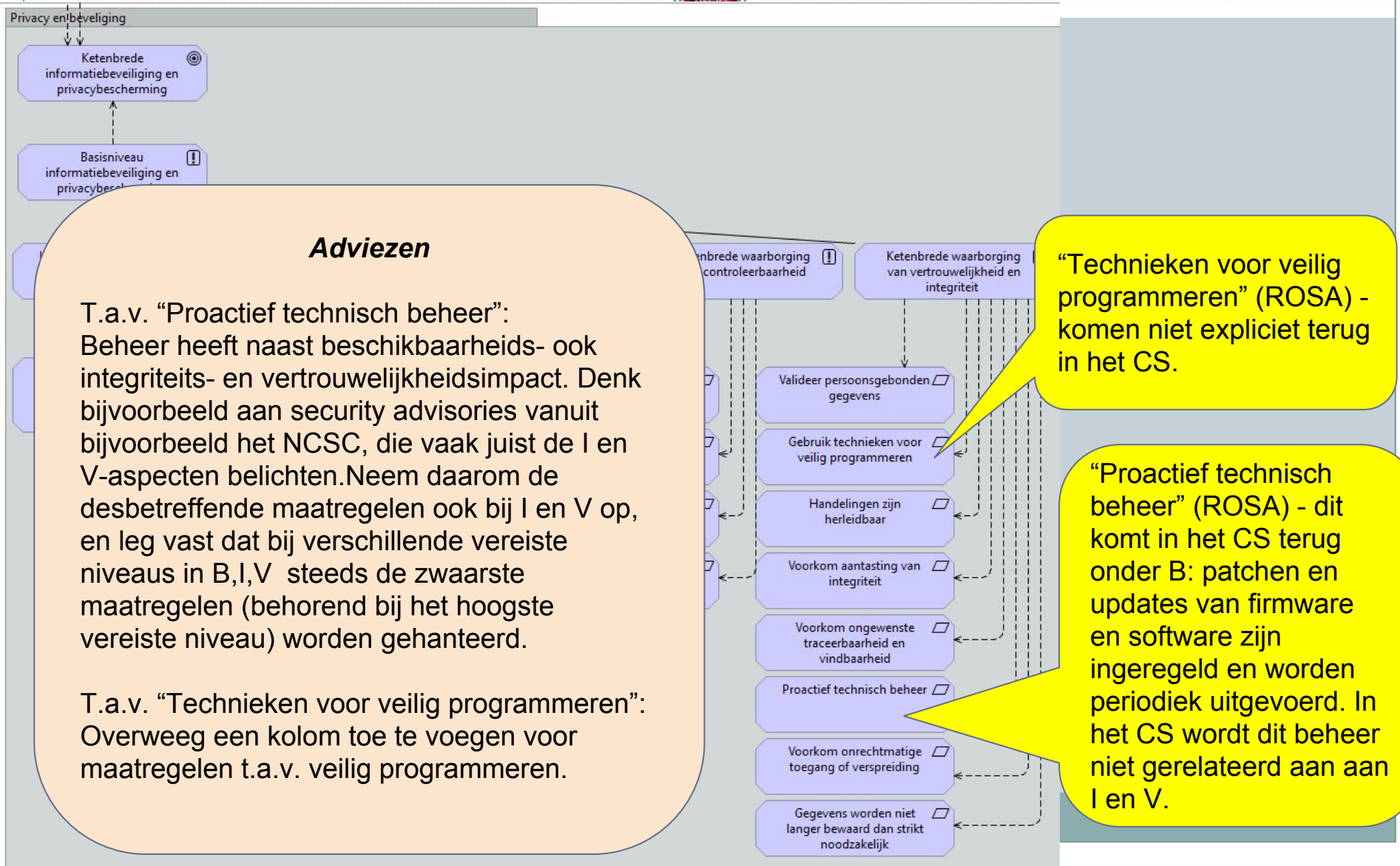
Adviezen

T.a.v. "Voorkom ongewenste traceerbaarheid": Overweeg - mede vanwege het belang van dit kader voor (minderjarige) onderwijsvolgers - maatregelen (ook) expliciet in het toetsingskader op te nemen, wellicht in een aparte kolom.

T.a.v. "Niet langer bewaren dan strikt noodzakelijk":De kolom 'levenscyclus' besteedt wel aandacht aan bewaartermijnen, maar niet aan doelbinding. Neem in deze kolom ook maatregelen op die bewerkstelligen dat data waarvoor niet langer een doelbinding bestaat vernietigd kan worden.

"Niet langer bewaren dan strikt noodzakelijk"
-
Heeft een duidelijk procesaspect, maar de ict-toepassing moet het wel *mogelijk* maken dat oude data wordt vernietigd.

IBP (ROSA): Compliant



Adviezen

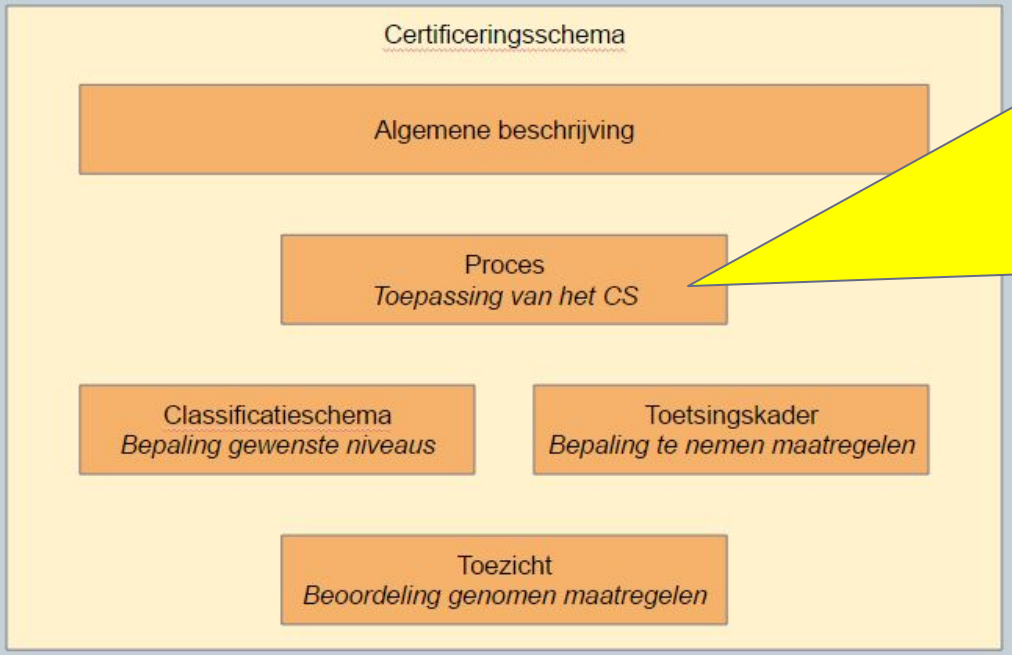
T.a.v. “Proactief technisch beheer”:
Beheer heeft naast beschikbaarheids- ook integriteits- en vertrouwelijkheidsimpact. Denk bijvoorbeeld aan security advisories vanuit bijvoorbeeld het NCSC, die vaak juist de I en V-aspecten belichten.Neem daarom de desbetreffende maatregelen ook bij I en V op, en leg vast dat bij verschillende vereiste niveaus in B,I,V steeds de zwaarste maatregelen (behorend bij het hoogste vereiste niveau) worden gehanteerd.

T.a.v. “Technieken voor veilig programmeren”:
Overweeg een kolom toe te voegen voor maatregelen t.a.v. veilig programmeren.

“Technieken voor veilig programmeren” (ROSA) - komen niet expliciet terug in het CS.

“Proactief technisch beheer” (ROSA) - dit komt in het CS terug onder B: patchen en updates van firmware en software zijn ingeregeld en worden periodiek uitgevoerd. In het CS wordt dit beheer niet gerelateerd aan aan I en V.

Zeggenschappen en gegevenssoorten:
Nonconformant



In de procesbeschrijving van het certificeringsschema wordt, waar het gaat over de te betrekken partijen, gesproken over “de eigenaar van de data”.

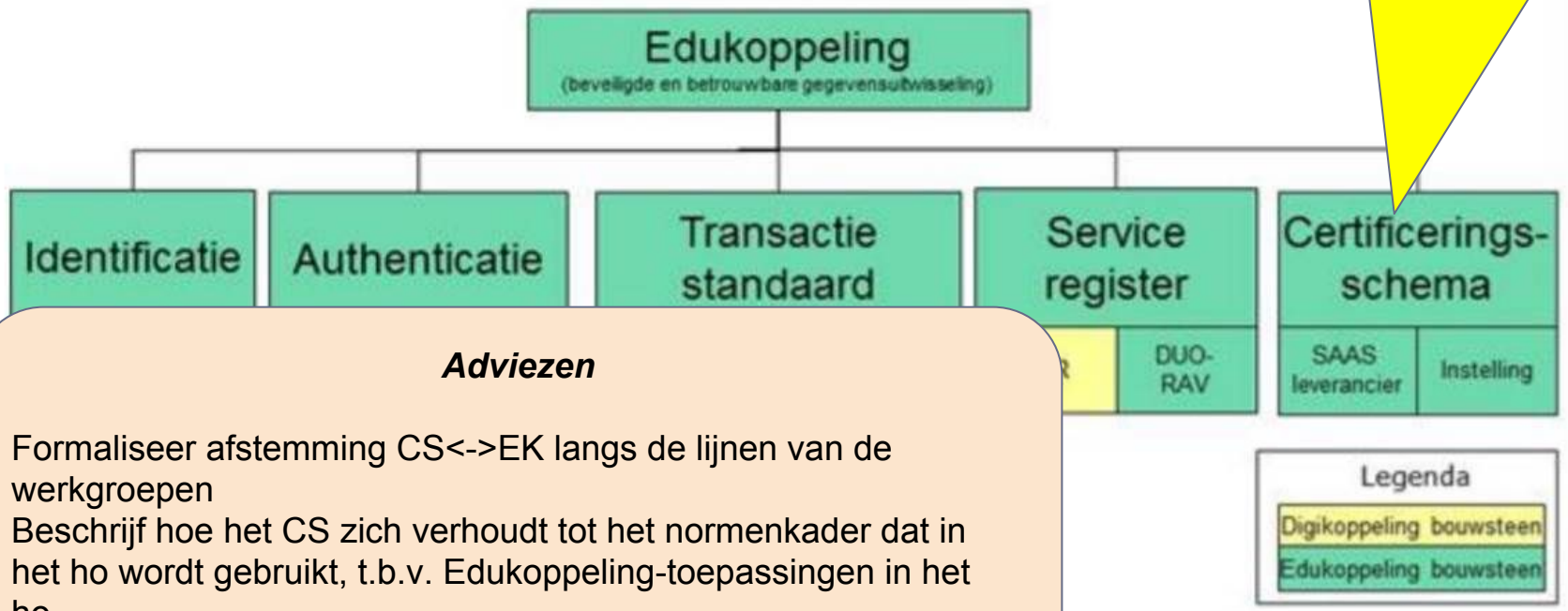
Eigenaarschap van gegevens is zowel juridisch als inhoudelijk lastig te duiden. Een formeel (juridisch) eigenaarschap van gegevens bestaat niet, omdat in formele zin eigenaarschap altijd over stoffelijke zaken gaat, en gegevens dat niet zijn. Bovendien zullen vanuit verschillende rollen verschillende partijen 'iets' met gegevens moeten doen - een absoluut eigenaarschap is dus, los van de juridische context, uitgesloten. In ROSA wordt daarom uitgegaan van zeggenschappen die partijen kunnen hebben over gegevens.

Adviezen

CS: Werk het bedoelde ‘eigenaarschap’ uit in termen van de relevante zeggenschap(pen): welke zeggenschappen maken dat partijen die die zeggenschap hebben betrokken dienen te worden bij de uitvoering van het in het certificeringsschema beschreven proces?

Relatie met Edukoppeling

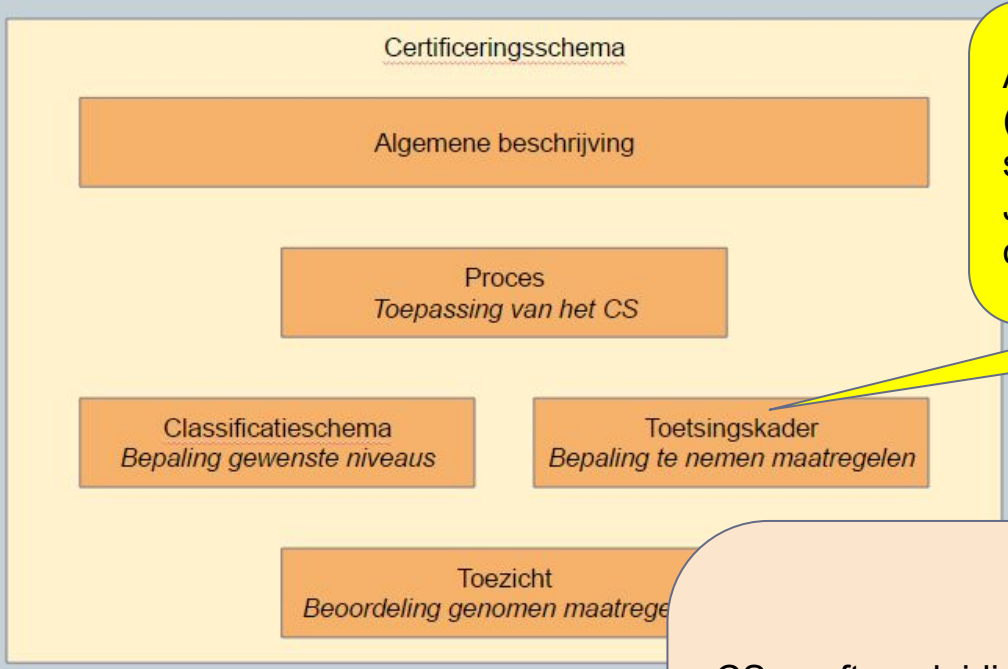
Edukoppeling maakt gebruik van het CS.



Adviezen

Formaliseer afstemming CS<->EK langs de lijnen van de werkgroepen
Beschrijf hoe het CS zich verhoudt tot het normenkader dat in het ho wordt gebruikt, t.b.v. Edukoppeling-toepassingen in het ho.
Bijwerken van EK-informatie in ROSA (‘SAAS-leverancier’ in dit diagram)

Beheer en doorontwikkeling



Aanpassingen aan het toetsingskader worden (in afwijking van het reguliere standaardisatieproces) direct gepubliceerd. Jaarlijks wordt de hele standaard als geheel opnieuw vastgesteld.

Adviezen

CS geeft aanleiding voor een herziening van (delen van) het ROSA katern IBP. In ieder geval moet de positie van het Certificeringsschema als toetsingskader (niet langer alleen voor cloud leveranciers) juist worden weergegeven.

Ten aanzien van (nieuwe versies van) het certificeringsschema: Voer vanuit de Architectuurraad niet vaker dan jaarlijks een architectuurscan uit voor het CS, namelijk bij aanbieding van de jaarlijkse nieuw vatsgestelde versie. Neem kennis van de tussentijdse wijzigingen.