

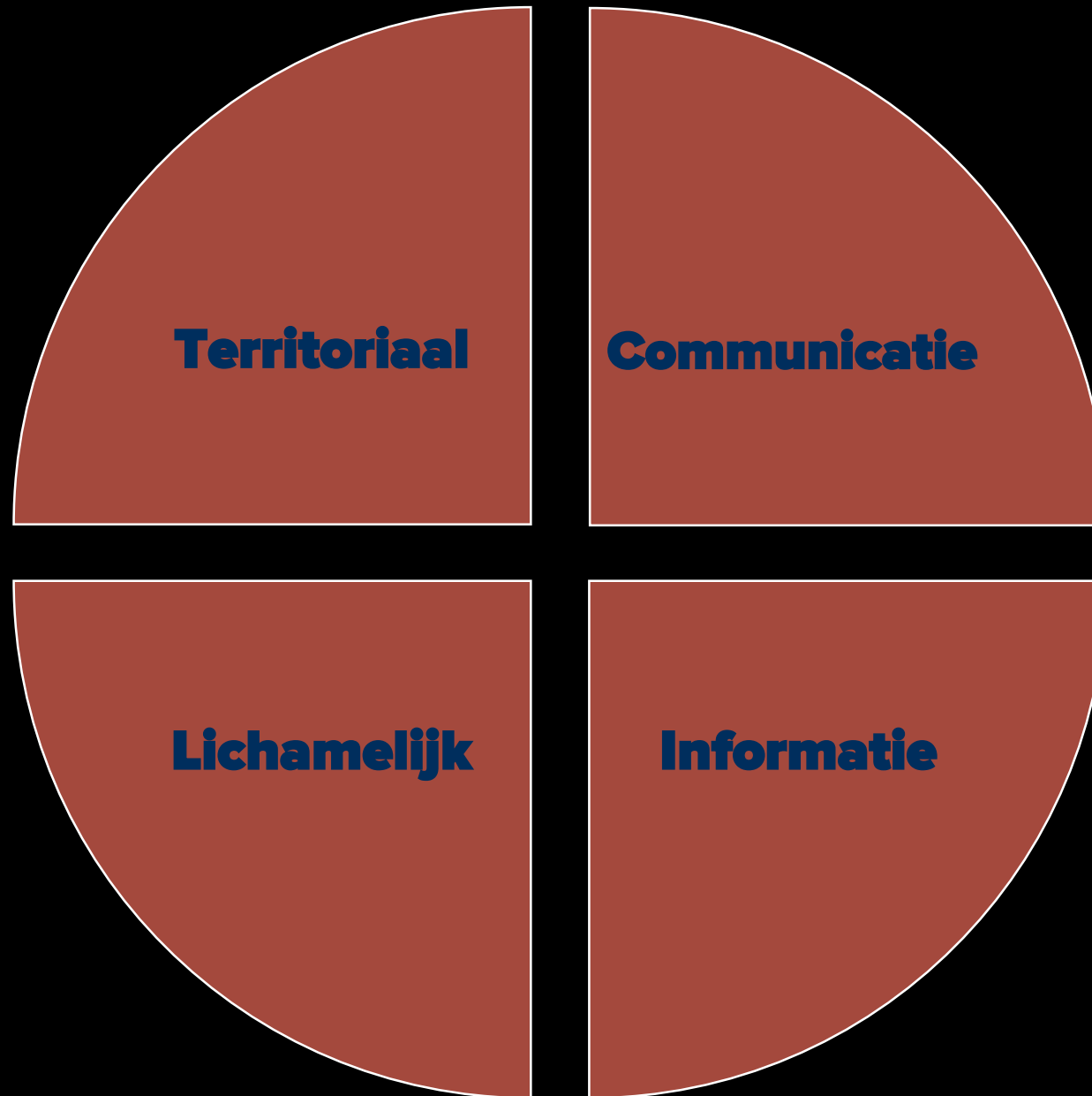


Isaca Round Table Privacy en IT-audit

Martine van de Merwe

Breukelen, 12 december 2016

Soorten privacy



FIP: Fair information practices

Rechten van individuen

Kennisgeving

Keuze en toestemming

Toegang

Beheersing van informatie

Informatiebeveiliging

Informatiekwaliteit

Levenscyclus van informatie

Verzameling

Gebruik en retentie

Openbaarmaking

Management

Management / governance

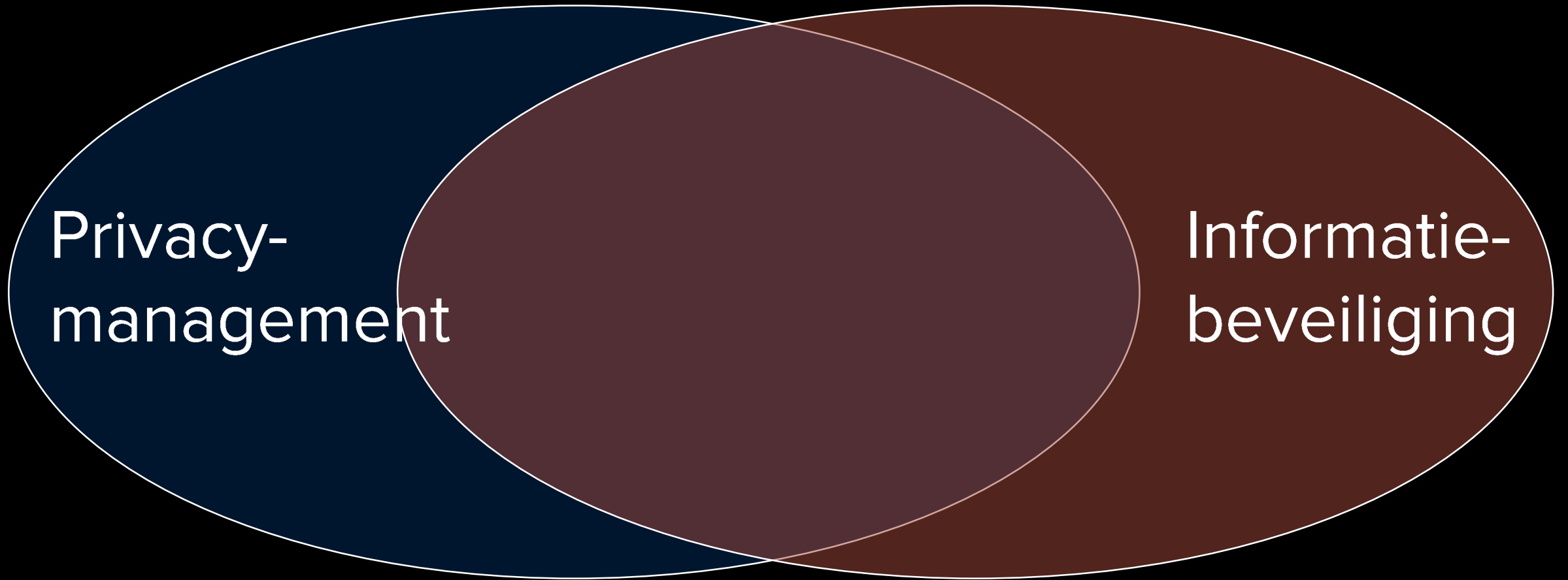
Monitoring en handhaving

Toestemming

- Vrij
- Specifiek
- Geïnformeerd

<https://youtu.be/KgeVsBSfI9A>





Raamwerk Assurance-opdrachten door IT-auditors

Toepasbare toetsingsnormen

- Relevant
- Volledig
- Betrouwbaar
- Neutraal
- Begrijpelijk

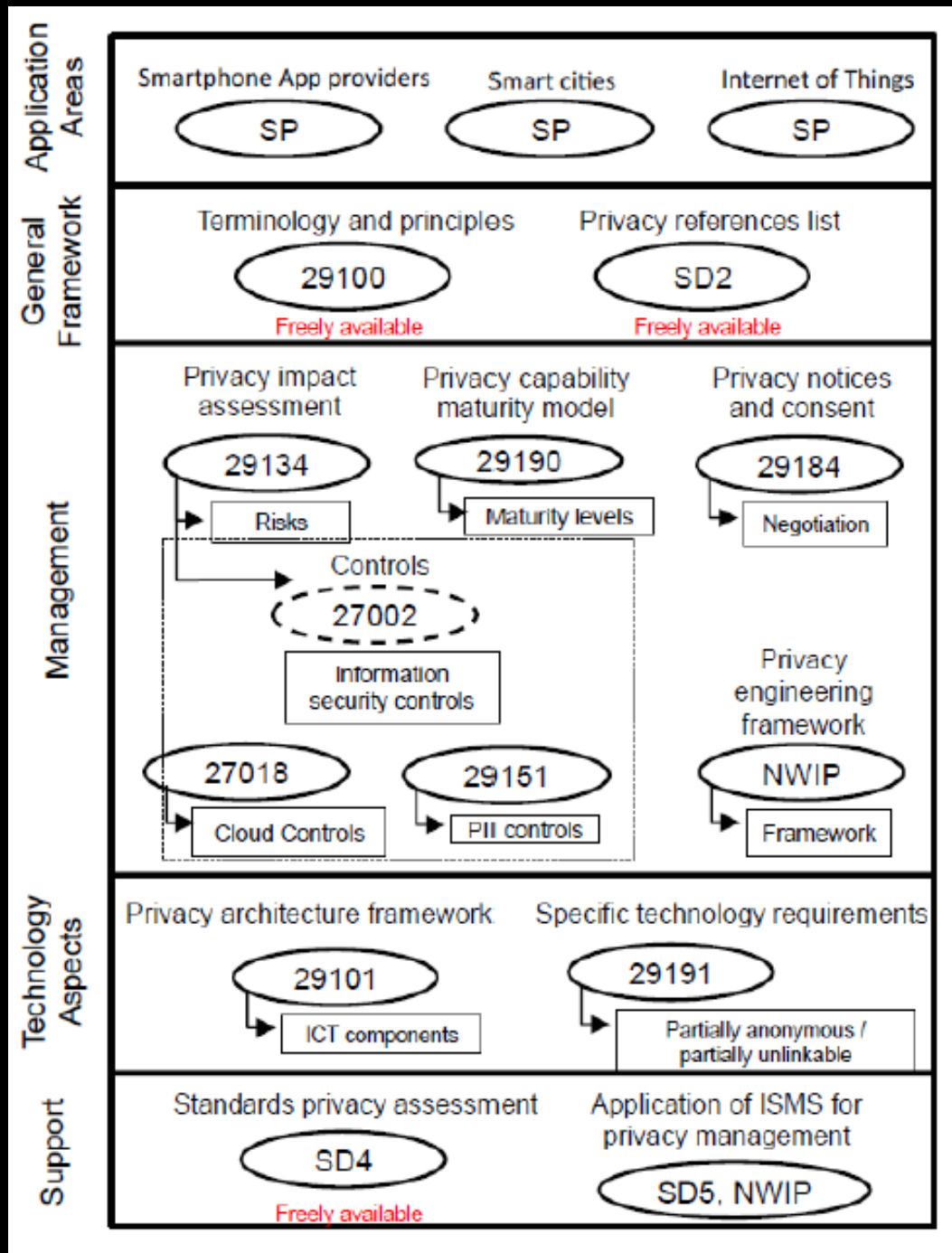
Do you think consumers today should feel confident that organizations are adequately protecting their personal information?

ISACA Personally Identifiable Information Audit/Assurance Program

V. Executive Summary of PII Audit/Assurance	
VI. Audit/Assurance Program	
1. Planning and Scoping the Audit	
2. Risk Management	
3. Policies	
4. Legal	
5. Governance	
6. Training	
7. PII-related Information Security	

VII. Appendix A: Audit/Assurance Program

ISO 29000-serie



ISO 29100 Privacy framework

5	The privacy principles of ISO/IEC 29100.....
5.1	Overview of privacy principles
5.2	Consent and choice
5.3	Purpose legitimacy and specification
5.4	Collection limitation
5.5	Data minimization
5.6	Use, retention and disclosure limitation
5.7	Accuracy and quality
5.8	Openness, transparency and notice
5.9	Individual participation and access.....
5.10	Accountability
5.11	Information security
5.12	Privacy compliance

ISO 27001:2013

A.18.1.4 Privacy and protection of personally identifiable information

Control

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

NEN 7510:2011

Behoudens wettelijke uitzonderingen, behoort een zorginstelling toestemming te hebben van de patiënt voor het uitwisselen van zijn gegevens.

Richtlijn 3600 NBA/NOREA

- Richtlijn 3600 Privacy-audits
- Raamwerk Privacy Audit
- Handreiking bij het Raamwerk Privacy Audit
- Keurmerk 'Privacy-audit-proof'

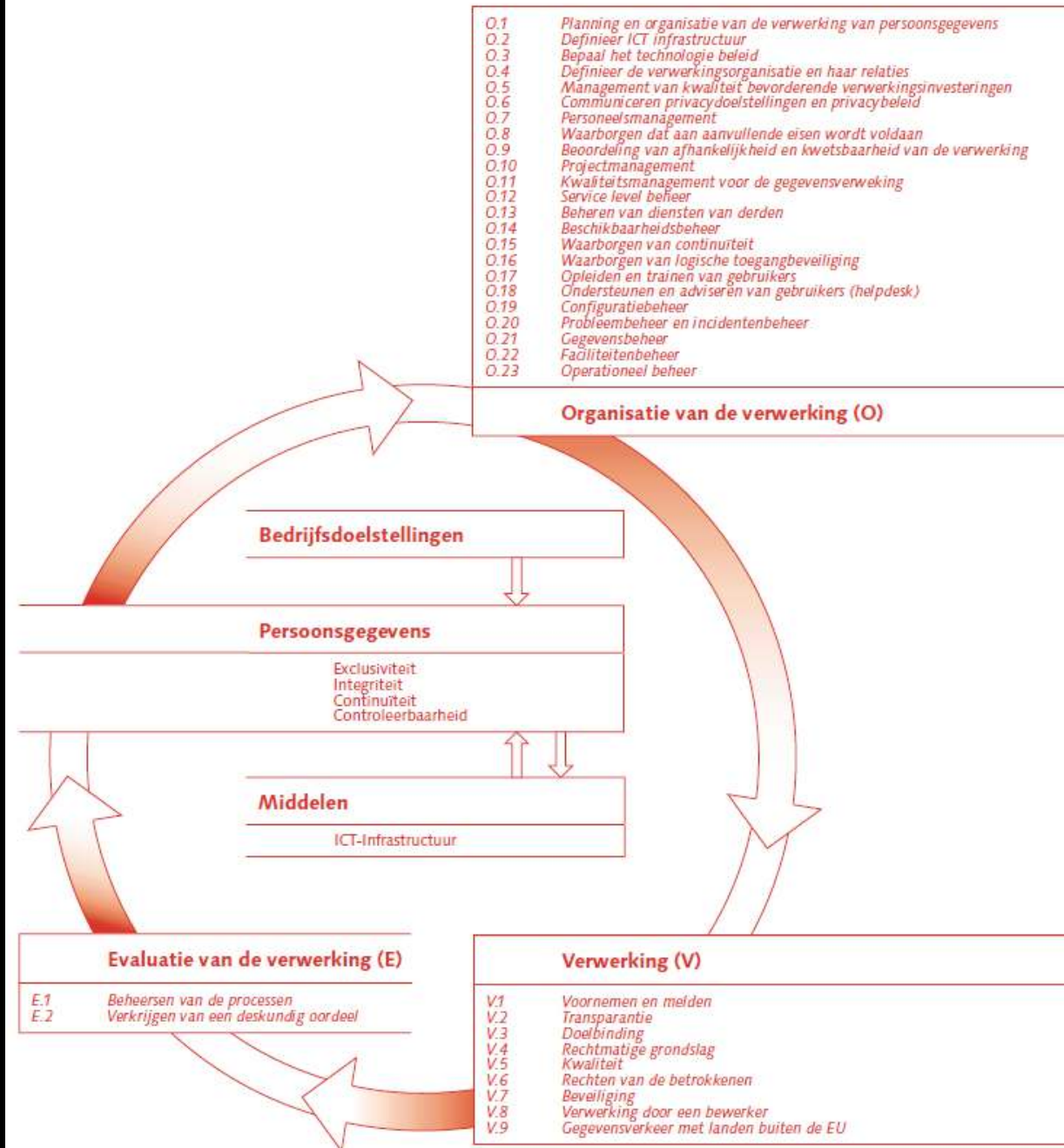


https://youtu.be/5oAa2a_vBY0

Richtlijn 3600 NBA/NOREA

Raamwerk Privacy Audit

Managementcyclus



Richtlijn 3600 NBA/NOREA

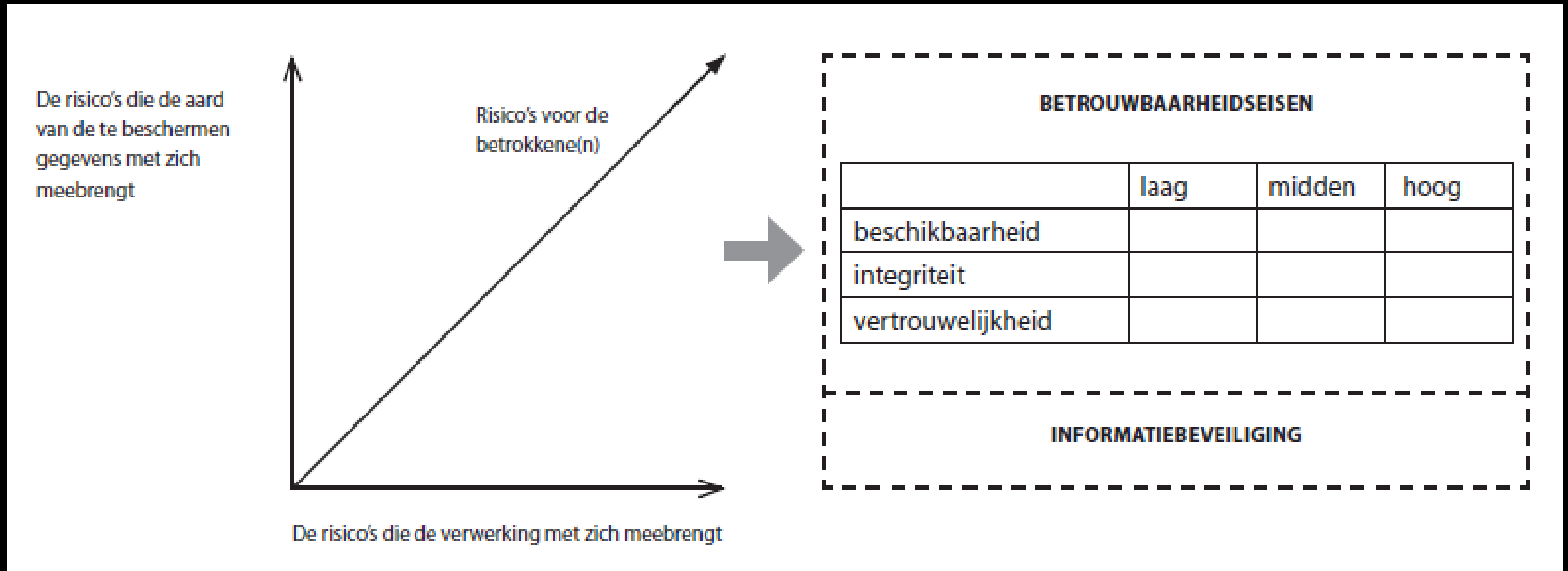
Raamwerk Privacy Audit

Schema voor het bepalen van de risicoklasse

Hoeveelheid persoonsgegevens	Aard van de verwerking (complexiteit)	Aard van de persoonsgegevens		
		Algemeen	Bijzonder art. 16 WBP	Financieel/economisch
Weinig	Laag	Risicoklasse 0	Risicoklasse II	Risicoklasse II
Veel	Hoog	Risicoklasse I	Risicoklasse III	

Richtlijn 3600 NBA/NOREA

Risicoklasse conform Richtsnoeren Beveiliging van Persoonsgegevens (CBP 2013)



Richtlijn 3600 NBA/NOREA

Handreiking bij het Raamwerk Privacy Audit

Toleranties bij beoordeling

Non-conformiteit – structureel materieel

Deficiëntie – structureel niet materieel

Incident – incidenteel niet materieel

Non-conformiteit => afkeuring

Deficiënties en incidenten:

Deficiëntie				Incident			
Punten per risicoklasse							
0	I	II	III	0	I	II	III
1	2	4	8	1	1	2	3

Richtlijn 3600 NBA/NOREA

Handreiking bij het Raamwerk Privacy Audit

Voorbeeld

V.4 **Rechtmatige grondslag** (artikel 6, 8, 16, 17, 18, 19, 20, 21, 22, 23, 24)

Persoonsgegevens mogen alleen worden verzameld en verwerkt wanneer de grondslag daarvoor in de WBP kan worden gevonden. Voor bijzondere persoonsgegevens gelden specifieke regels.

Non-conformiteiten

- De verantwoordelijke verwerkt persoonsgegevens zonder een wettelijke grondslag.
- De verantwoordelijke verwerkt bijzondere gegevens zonder dat daarvoor een ontheffing van het wettelijke verbod is.
- Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt door de verantwoordelijke verwerkt buiten de uitvoering van die wet dan wel buiten de doeleinden bij wet- of regelgeving bepaald.
-

Vorbereiding
op de komst
van de auditor

<https://youtu.be/UZ9n1x9YjjY>



Bedankt!

Martine van de Merwe RE CISA CIPP/E
martine@privacylabnederland.nl
www.privacylabnederland.nl
06-53418807



Martine van de Merwe



@privacylab



Privacylab Nederland