Naar een nieuw Privacy Control Framework (PCF)

Ali Ougajou

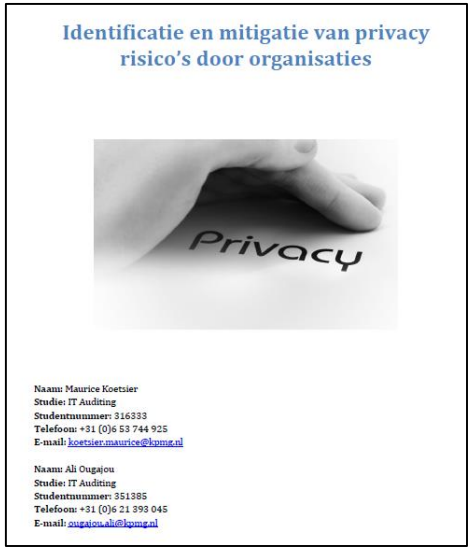
22 november 2017]

KENNISGROEP P R I V A C Y

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

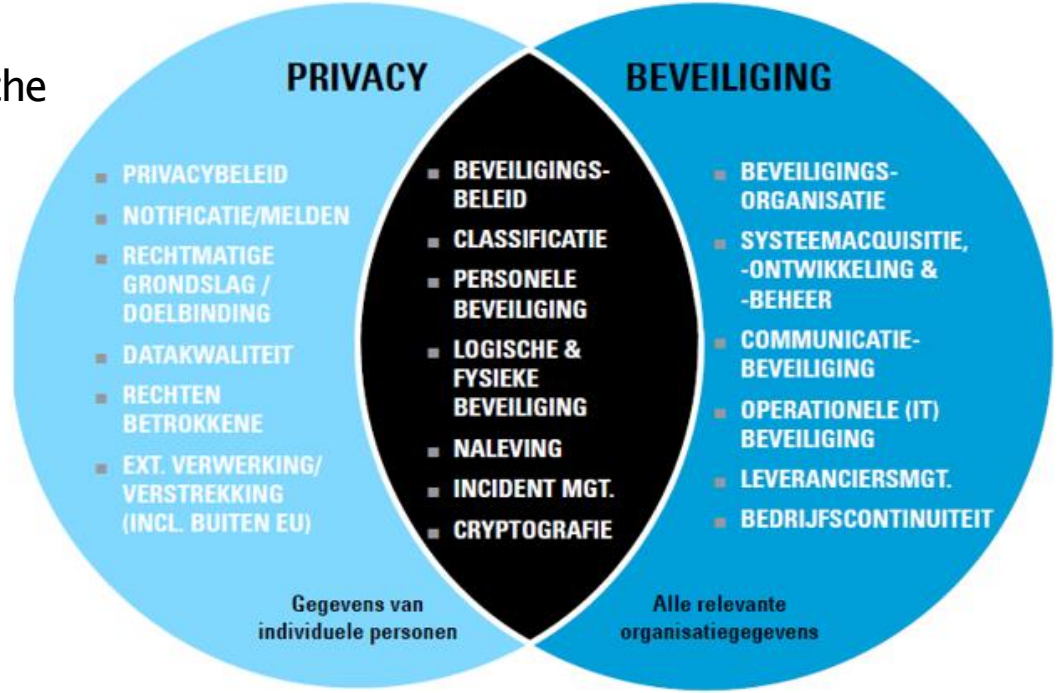
Introductie privacy control framework

- Referaat in het kader van afstuderen RE–studie
- Ontwikkeling van een privacy control framework
- Totstandkoming

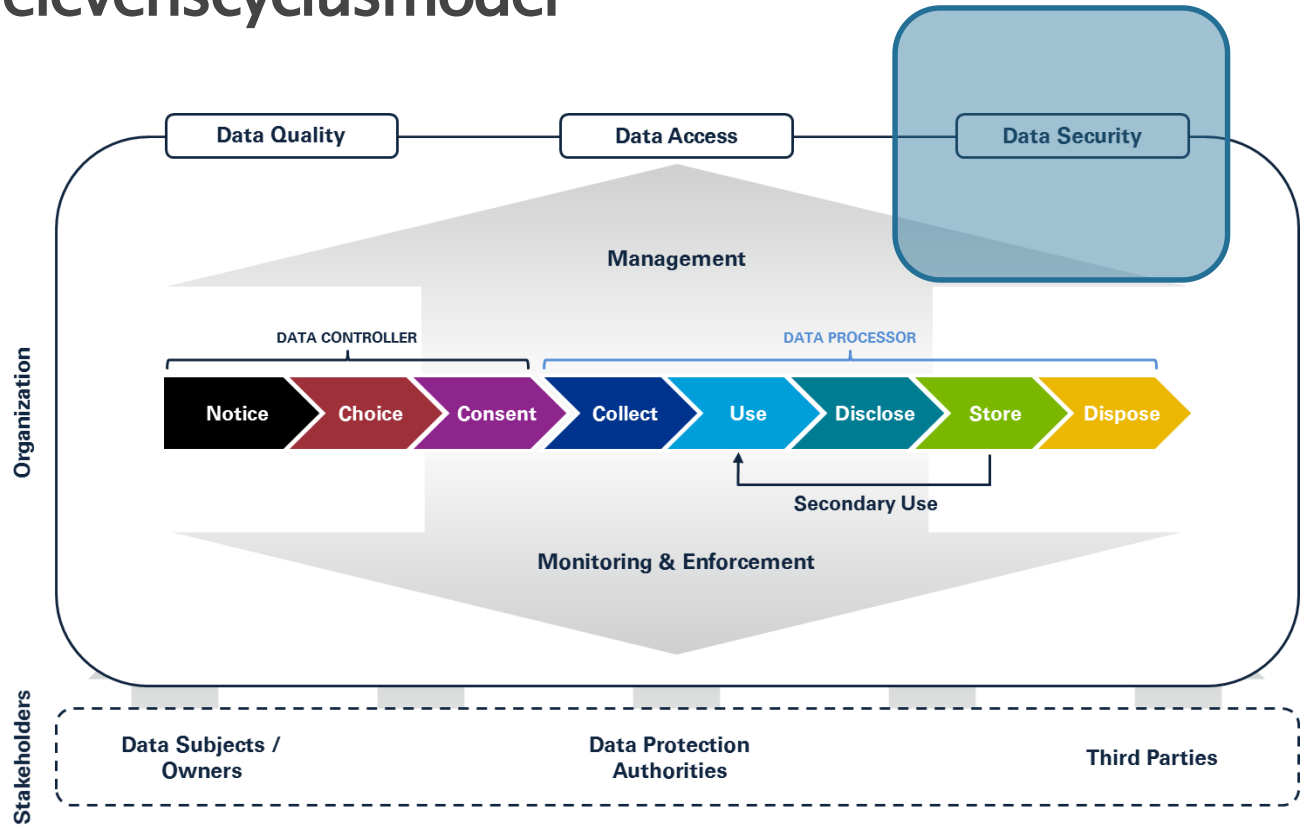


Informatiemanagement als uitgangspunt

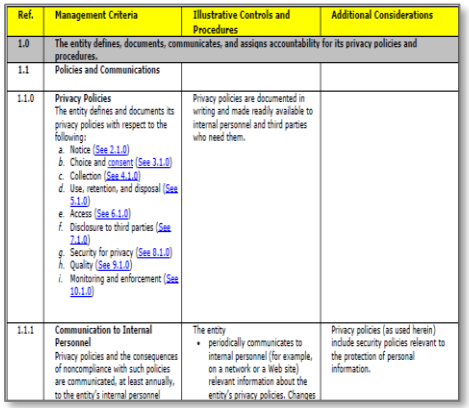
- Visie op privacy:
  - dient breder te zijn dan alleen juridische of technische perspectief
- Nadruk op praktisch implementatie
  - Focus op techniek
- Dient Informatiemanagement te zijn:
  - Schakel tussen IT en bedrijfsvoering
  - Dataflow staat hierin centraal



Informatielevenscyclusmodel

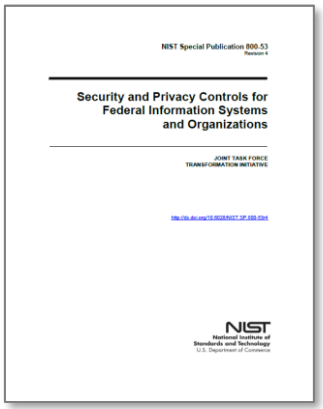


Analyse Frameworks en Good Practices



Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
1.0	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.		
1.1	Policies and Communications		
1.1.0	Privacy Policies The entity defines and documents its privacy policies with respect to the following: a. Notice (See 2.1.0) b. Choice and consent (See 3.1.0) c. Collection (See 4.1.0) d. Use, retention, and disposal (See 5.1.0) e. Access (See 6.1.0) f. Disclosure to third parties (See 7.1.0) g. Security for privacy (See 8.1.0) h. Quality (See 9.1.0) i. Monitoring and enforcement (See 10.1.0)	Privacy policies are documented in writing and made readily available to internal personnel and third parties who need them.	
1.1.1	Communication to Internal Personnel Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel	The entity • periodically communicates to internal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies. Changes	Privacy policies (as used herein) include security policies relevant to the protection of personal information.

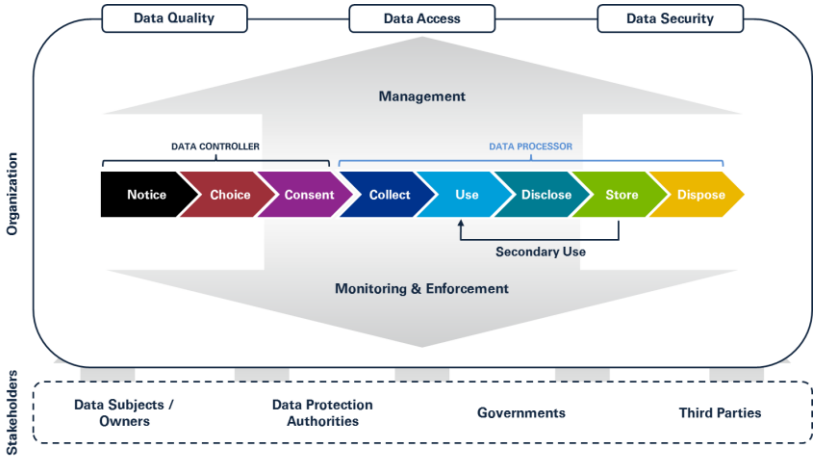
GAPP Framework



NIST SP800-R54 Privacy Control Catalog

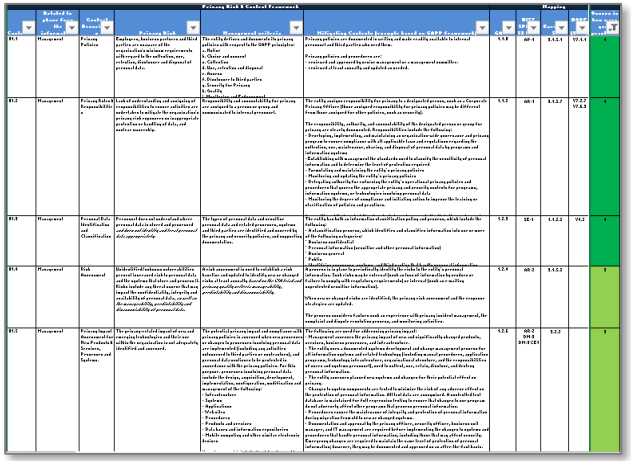
NOREA 3600

EuroPriSe Framework

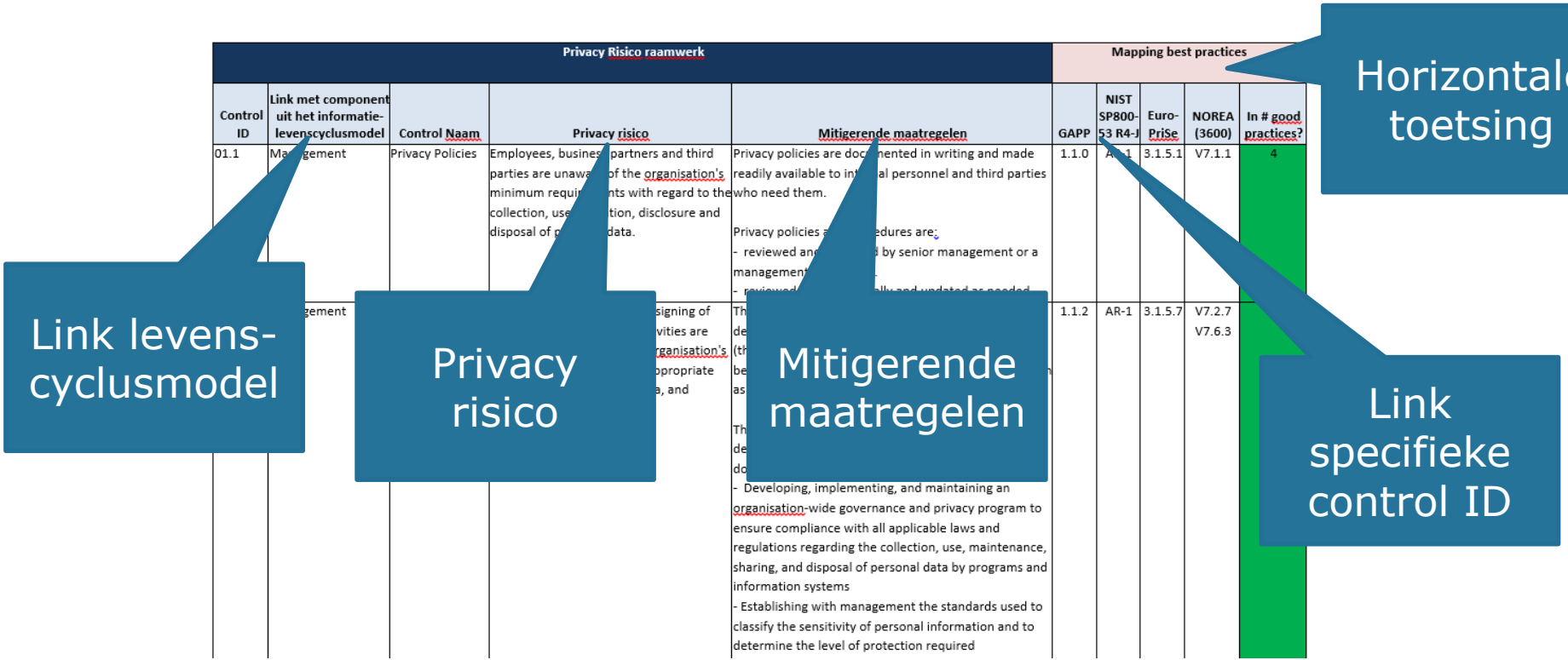


Structurering controls

o.b.v. risico's informatielevenscyclusmodel



Resultaat onderzoek: Privacy Control Framework



Privacy Risico raamwerk					Mapping best practices				
Control ID	Link met component uit het informatie-levenscyclusmodel	Control Naam	Privacy risico	Mitigerende maatregelen	GAPP	NIST SP800-53 R4-J	Euro-PriSe	NOREA (3600)	In # good practices?
01.1	Ma gement	Privacy Policies	Employees, busines partners and third parties are unawa of the organisation's minimum requi nts with regard to the collection, use tion, disclosure and disposal of p data.	Privacy policies are doc nented in writing and made readily available to in al personnel and third parties who need them. Privacy policies a edures are: - reviewed an by senior management or a management - reviewed lly and updated as needed	1.1.0	A 1	3.1.5.1	V7.1.1	4
	gement		signing of vities are rganisation's opropriate a, and	Th de (th be as Th de do - Developing, implementing, and maintaining an organisation-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personal data by programs and information systems - Establishing with management the standards used to classify the sensitivity of personal information and to determine the level of protection required	1.1.2	AR-1	3.1.5.7	V7.2.7 V7.6.3	

Privacy controldomeinen

Privacybeleid & strategie	Privacy By Design	Privacy Risk & Control Framework	Juridische Processen	
Privacy Officer & Overlegstructuur	Third Party Management	Privacy Processen	Security Management	
Training & Awareness	Informatielevens-cyclus management	Datalek Response Proces	Data Infrastructuur	Verantwoording & Auditing

Bedankt

Voor meer informatie kun je contact opnemen met:

Ali Ougajou
06-21393045
Ougajou.ali@kpmg.nl

22 november 2017