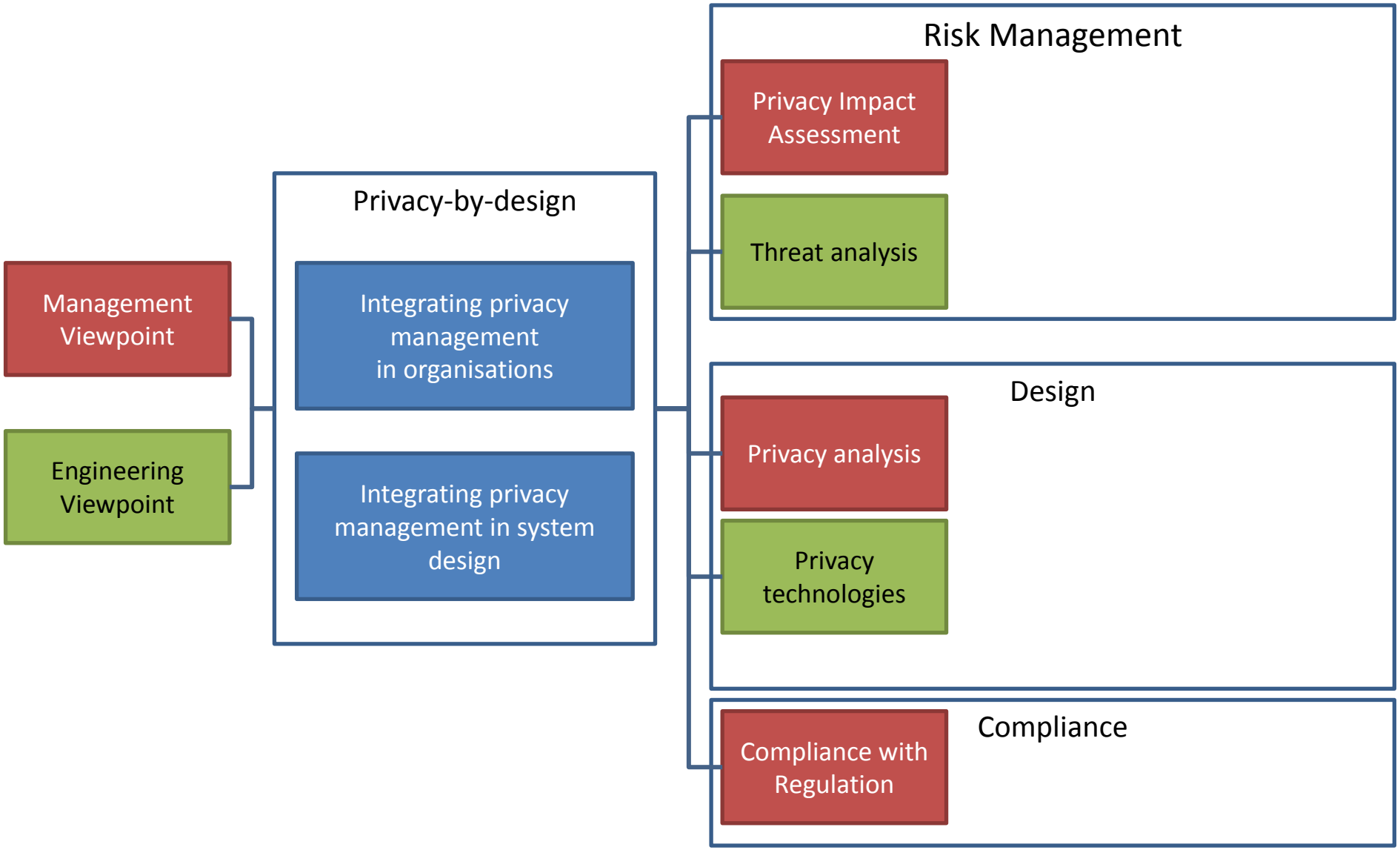
PRIPARE

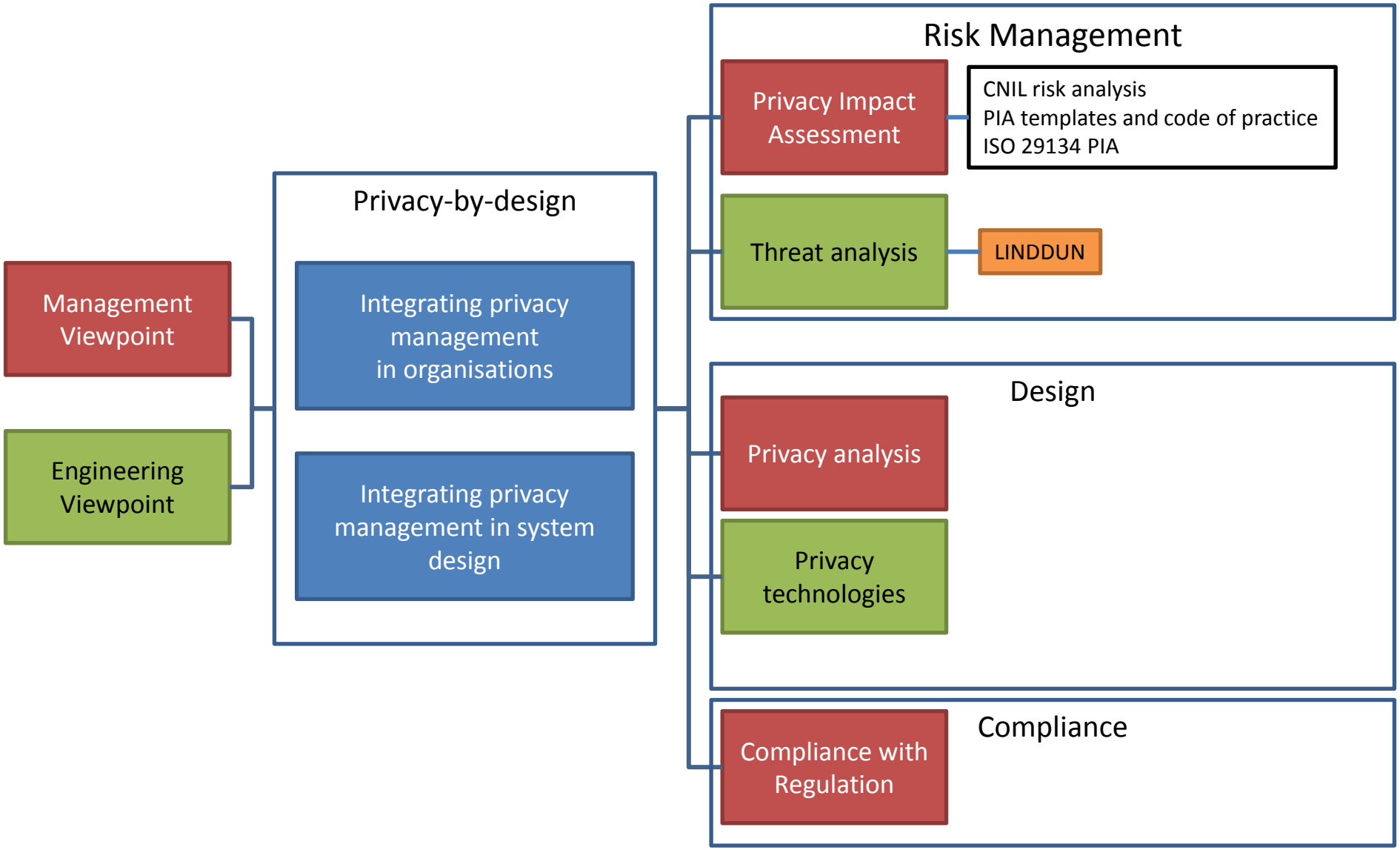
PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Engineering Privacy-by-design

Privacy-by-design



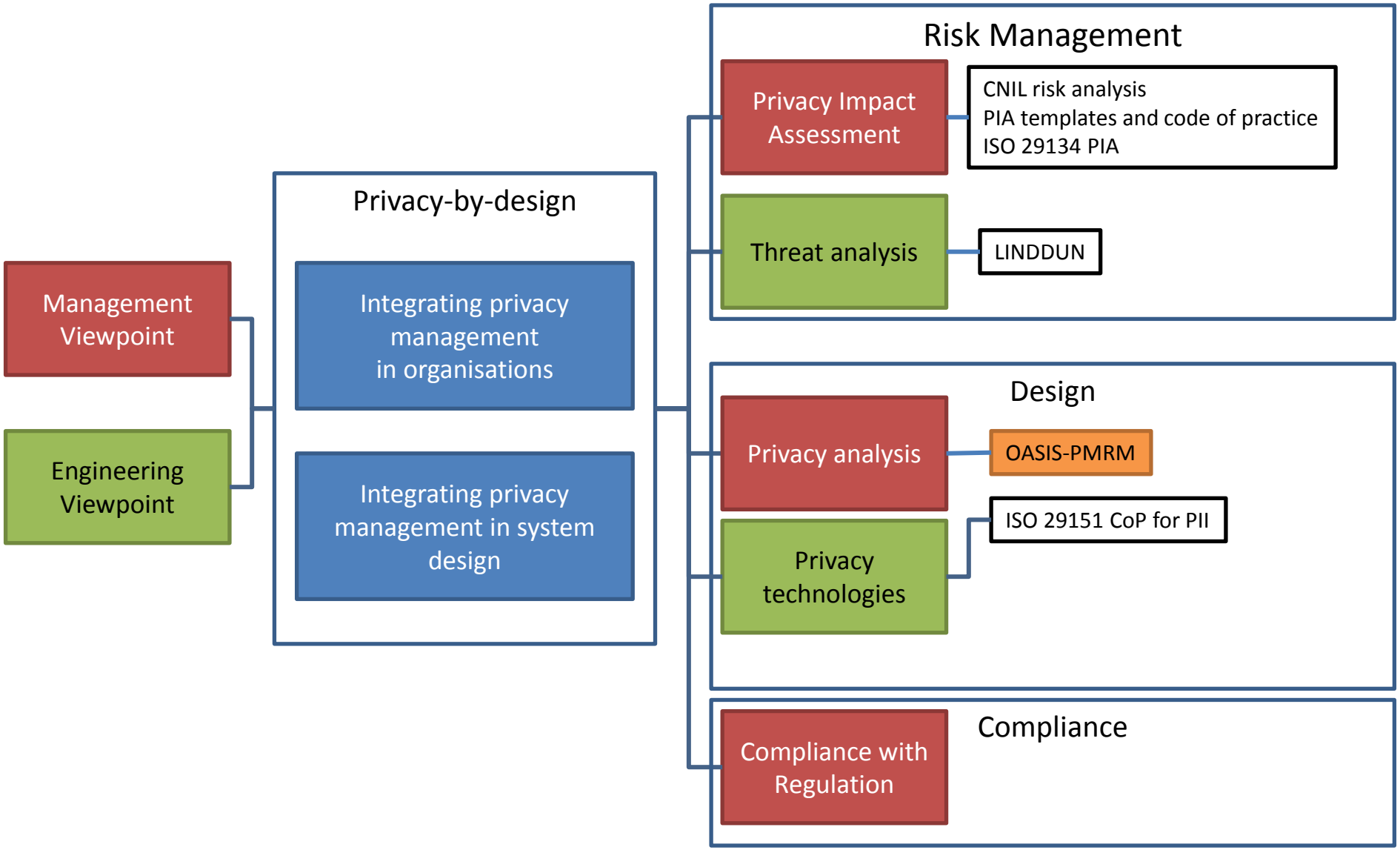
Current PbD Tools



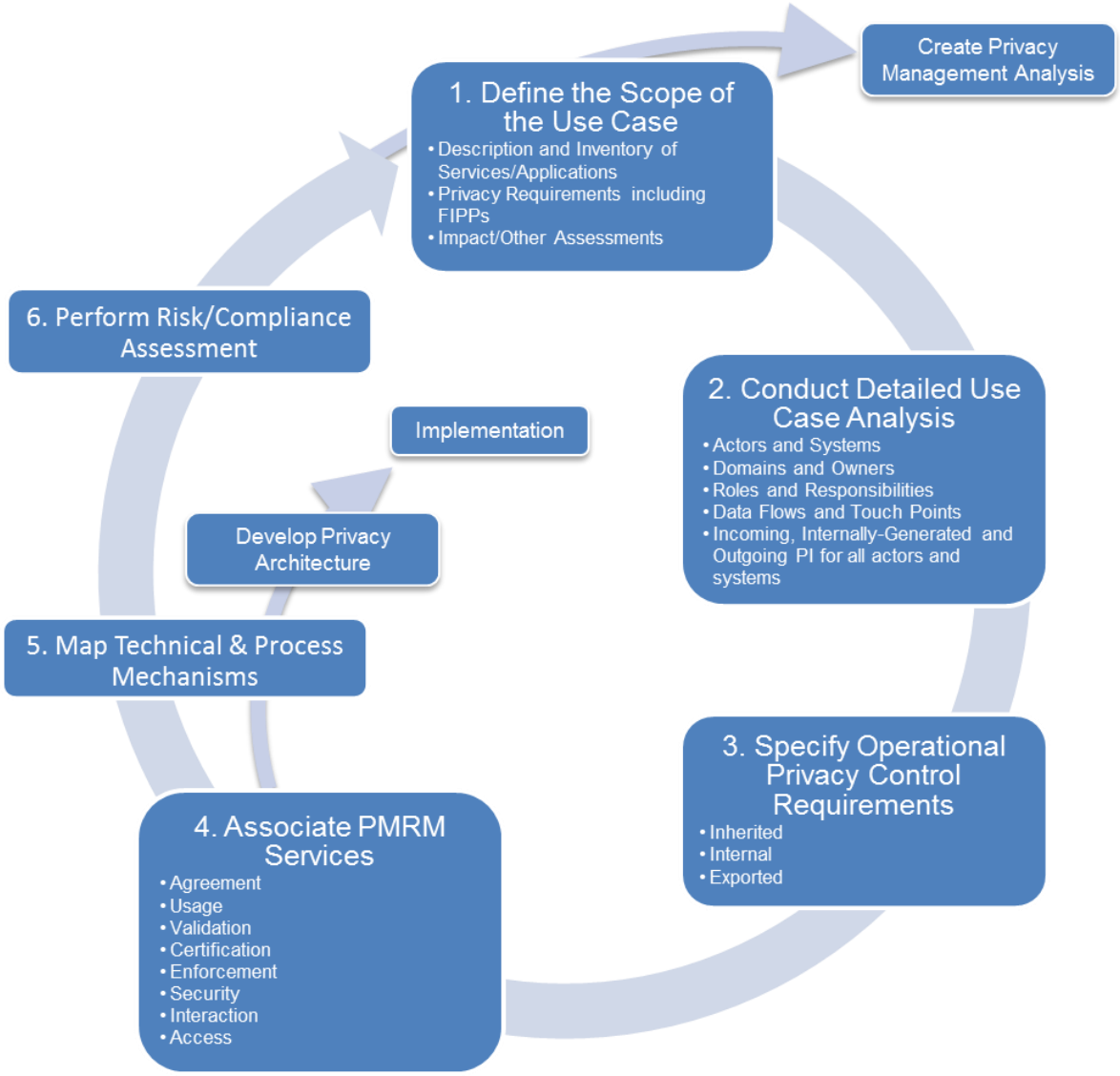
Privacy Risks: LINDDUN cheat sheet

Type	Property	Description	Threat
Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.	**L**inkability
	Anonymity	Hiding the link between an identity and an action or a piece of information	**I**dentifiability
	Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict	**N**on-repudiation
	Undetectability and unobservability	Hiding the user's actvities	**D**etectability
Security	Confidentiality	Hiding the data content or controlled release of data content	**D**isclosure of information
Soft Privacy	Content awareness	User's consciousness regarding his own data	**U**nawareness
	Policy and consent compliance	Data controller to inform the data subject about the system's privacy policy, or allow the data subject to specify consents in compliance with legislation	**N**on compliance

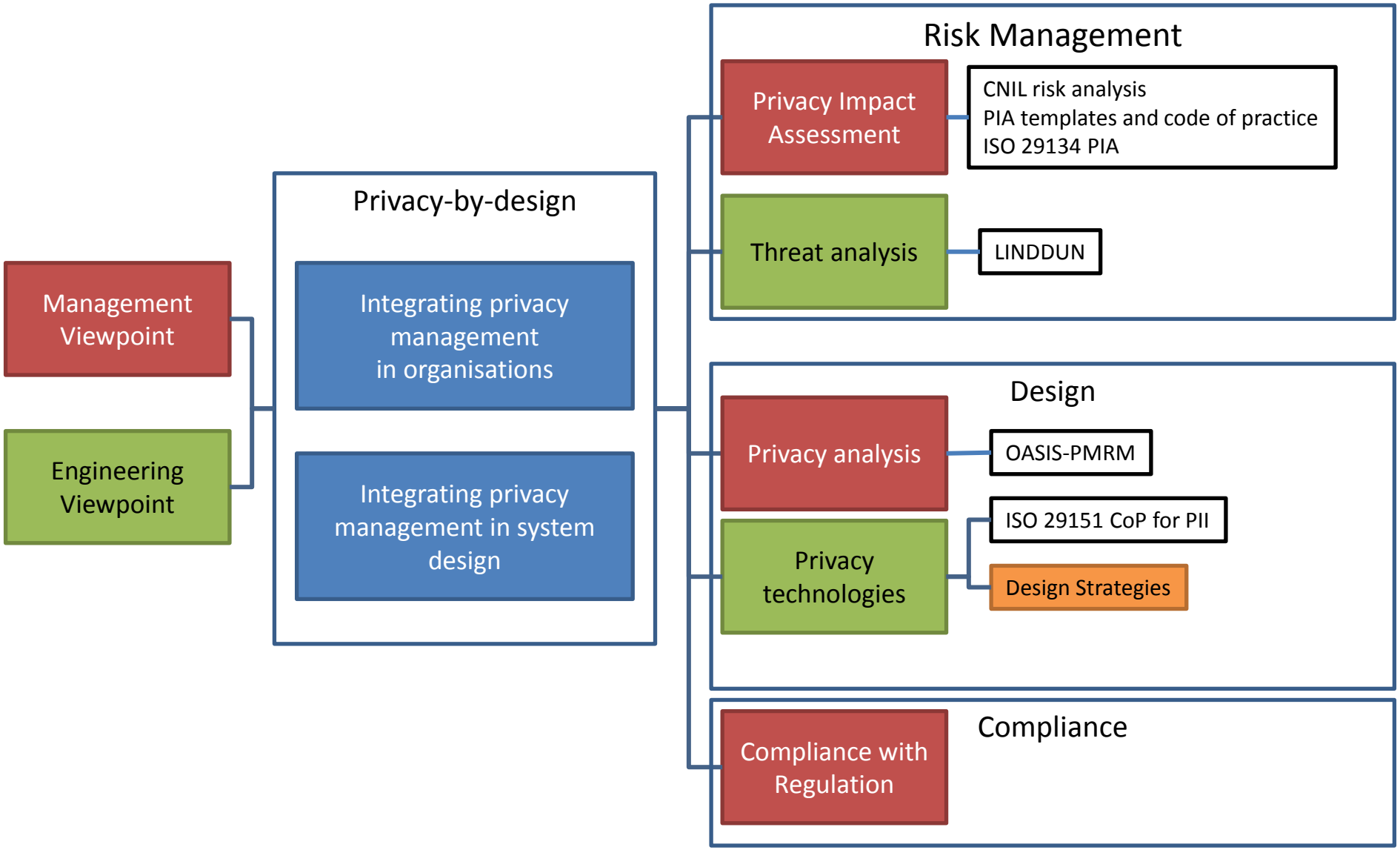
Current PbD Tools



OASIS PMRM


Create Privacy Management Analysis
1. Define the Scope of the Use Case
• Description and Inventory of Services/Applications
• Privacy Requirements including FIPPs
• Impact/Other Assessments
2. Conduct Detailed Use Case Analysis
• Actors and Systems
• Domains and Owners
• Roles and Responsibilities
• Data Flows and Touch Points
• Incoming, Internally-Generated and Outgoing PI for all actors and systems
3. Specify Operational Privacy Control Requirements
• Inherited
• Internal
• Exported
4. Associate PMRM Services
• Agreement
• Usage
• Validation
• Certification
• Enforcement
• Security
• Interaction
• Access
5. Map Technical & Process Mechanisms
Develop Privacy Architecture
Implementation
6. Perform Risk/Compliance Assessment

Current PbD Tools



Japp Henk Hoepman. Privacy design strategies .

ICT Systems Security and Privacy Protection - 29th IFIP TC 11 Int.Conf, SEC 2014, Marrakech, Morocco

also in ENISA Report Privacy and Data Protection by Design – from policy to engineering - Dec 2014

Strategy		Patterns Examples
1 Minimize	Amount of processed personal data restricted to the minimal amount possible	• select before you collect • anonymisation / pseudonyms
2 Hide	Personal data, and their interrelationships, hidden from plain view	• Storage and transit encryption of data • mix networks • hide traffic patterns • attribute based credentials • anonymisation / pseudonyms
3 Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible	• Not known
4 Aggregate	Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful	• aggregation over time (used in smart metering) • dynamic location granularity (used in location based services) • k-anonymity • differential privacy
5 Inform	Transparency	• platform for privacy preferrences • Data breach notification
6 Control	Data subjects provided agency over the processing of their personal data	• User centric identity management • End-to-end encryption support control
7 Enforce	Privacy policy compatible with legal requirements to be enforced	• Access control • Sticky policies and privacy rights management
8 Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements	• privacy management systems • use of logging and auditing

Gaps (to be discussed again)

		Standard	Purpose	Main feature	Opinion
Risk focus	CNIL risk analysis	Practice	Privacy breach analysis	Consistent with security risk analysis	**Lack** **(1) Integration of features** **(2) Addressing system vs subsystems**
	LINDDUN	Research		Categories of threats	
	ISO 29134	Yes	Privacy impact analysis		
	PIA template	Practice			
Goal focus	OASIS PMRM	Yes	Privacy analysis	Categories of services	
	PEARS	Research	Design for privacy	Architecture Modified by privacy	
	Design strategies	Research		Principles	
	ISO 29151	Yes		Categories of privacy measures	