PRIPARE

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

PRIPARE Discussion with NIST

Outline

- Introduction on PRIPARE
- What is privacy-by-design engineering?
  - Design
  - Risk analysis
- Standardisation: agreement on Concepts?
- Collaboration

PRIPARE

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

Introduction on PRIPARE

PRIPARE (prepareproject.eu)

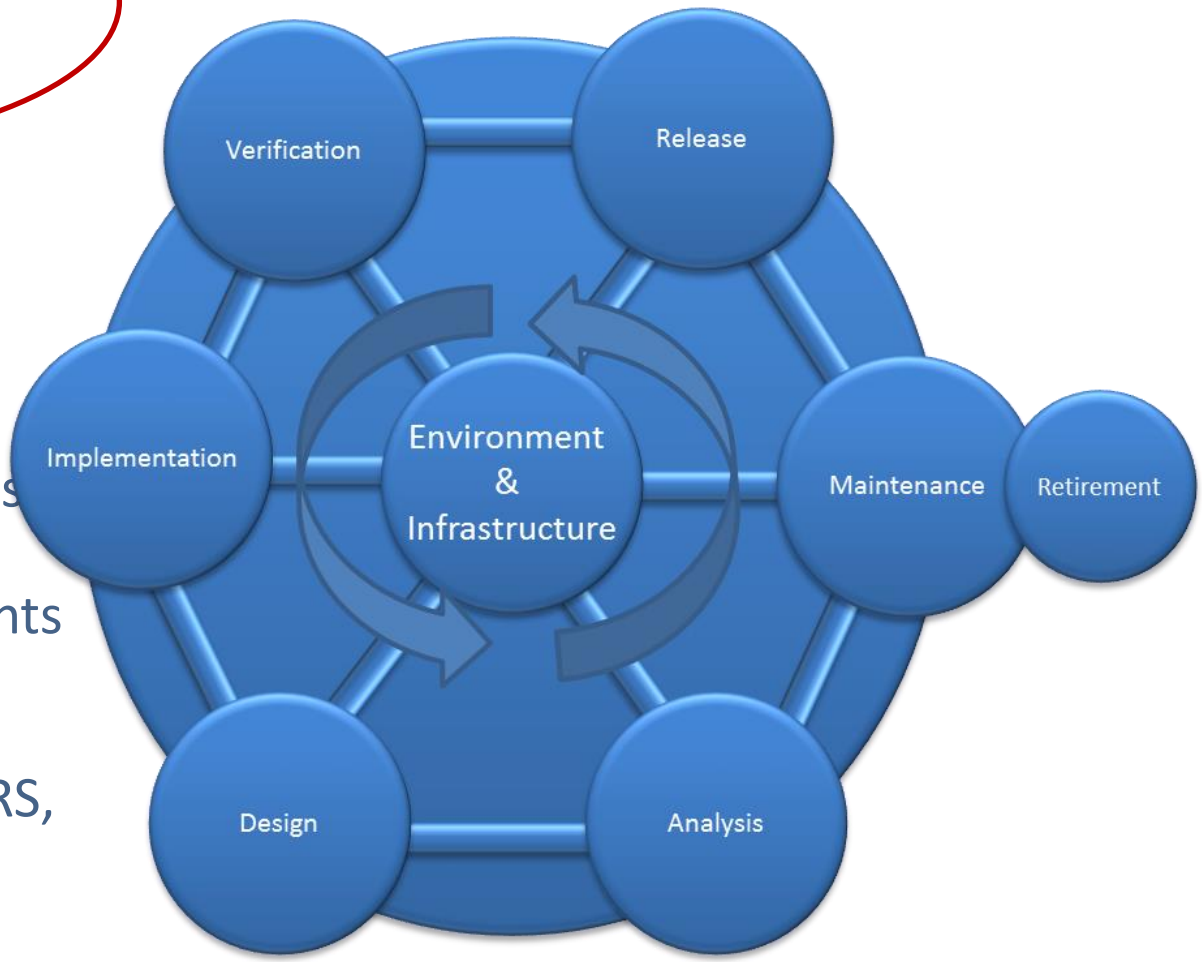
PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Support Action Mission:

- Define and Support practice of privacy-by-design
- Provide educational material … [to foster risk management culture]

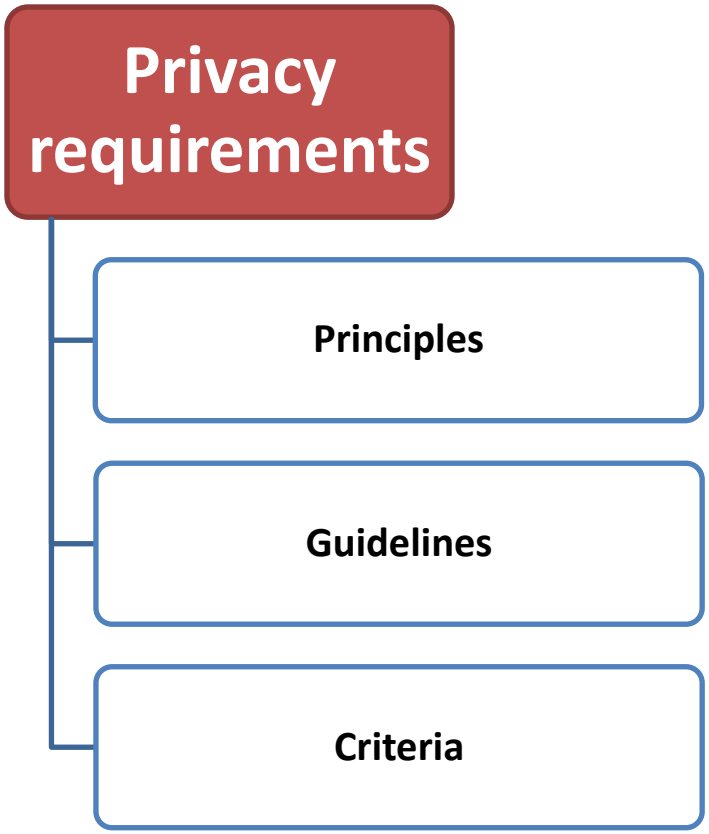
PRIPARE Methodology

- Need to cover entire life cycle
- More of a study on a global methodology
- Integrates
  - Privacy risk analysis (LINDDUN, CNIL)
  - Privacy requirements (UPM)
  - Design for privacy preservation (PEARS, Hoepman)
  - PIAs



PRIPARE Privacy Requirements

- This phase focuses on privacy requirement Operationalisation
  - map high-level, legal and user concerns into engineering requirements
- Three steps
  - Principles (the high level concerns)
  - Guidelines (specific goals)
  - Criteria(resulting engineering requirements)



Example

Principle	Guideline	Criteria
2. Data minimization and proportionality	G-2.1 Avoid and minimise use of personal data along whole lifecycle	C-2.1.1 When personal data is collected or retained, only allow those authorized and consented by the user
		C-2.1.2 Periodically evaluate that all the personal data is identified…
		C-2.1.3 When personal data is no longer needed, delete or anonymise it
		C-2.1.4…
	G-2.2 Minimise personal data used in pre-production systems	C-2.2.1 When doing testing, training and research: Apply procedures to minimise personal data
		C-2.2.2…

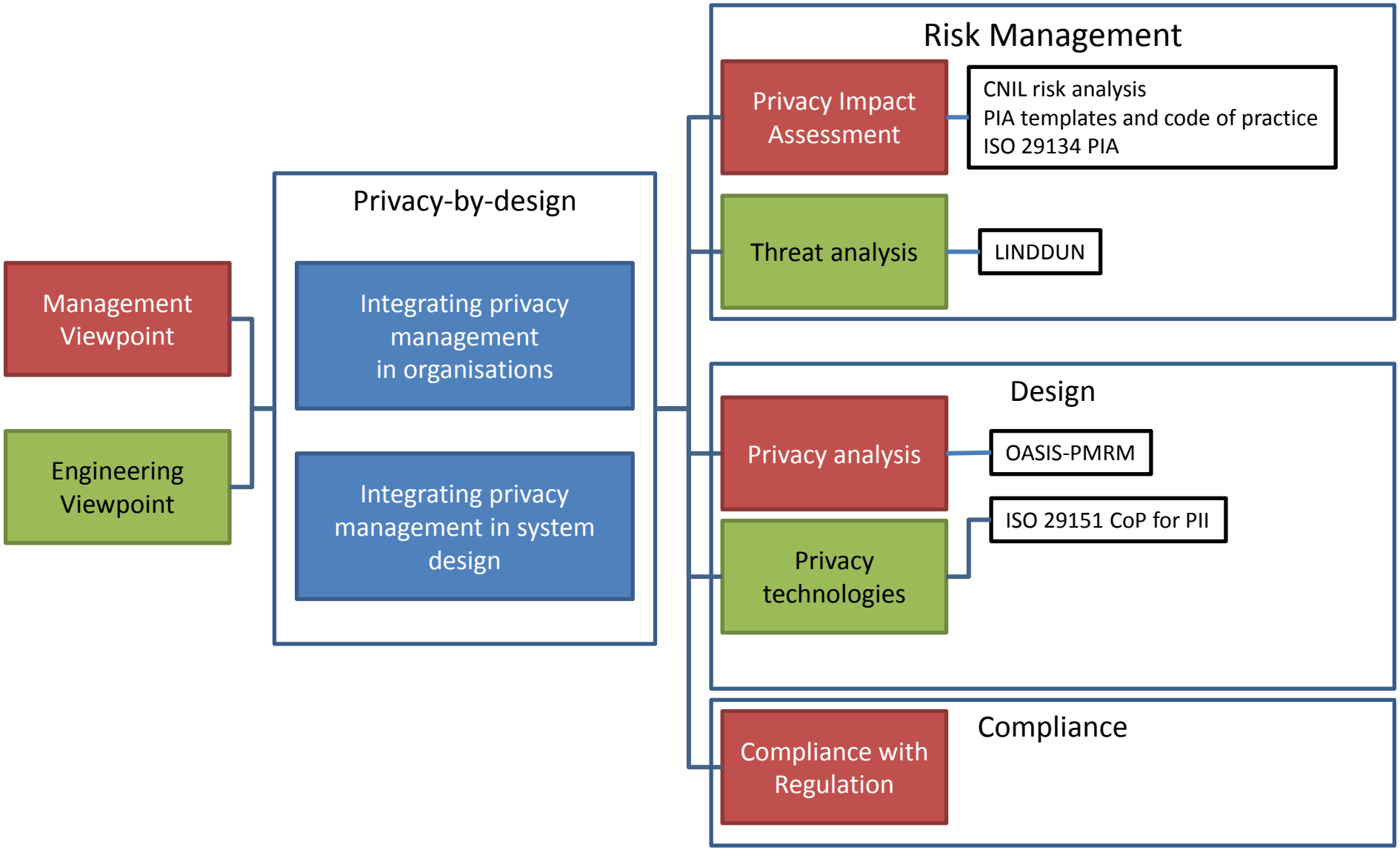
PRIPARE

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

What is Privacy-by-design Engineering?

(presented to the European Commission on June 11th, 2015)

Privacy-by-design



PRIPARE

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

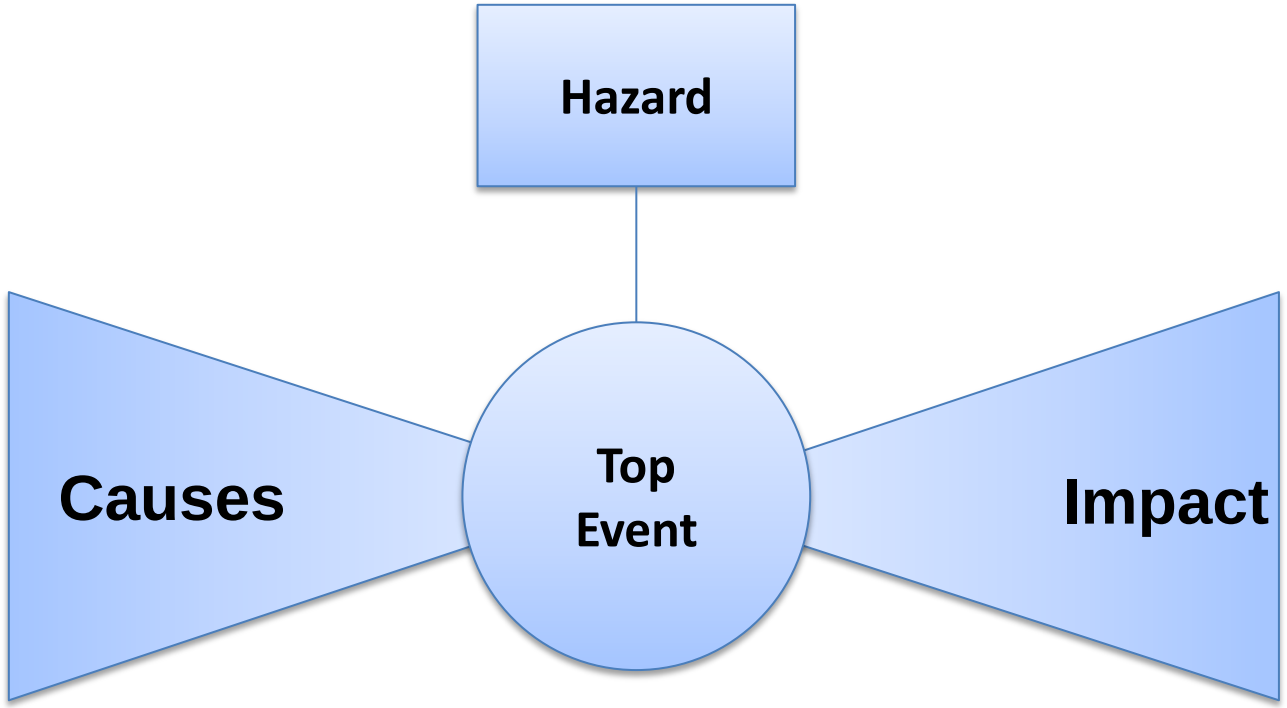
Risk Management?

Issues Related to Threat Analysis

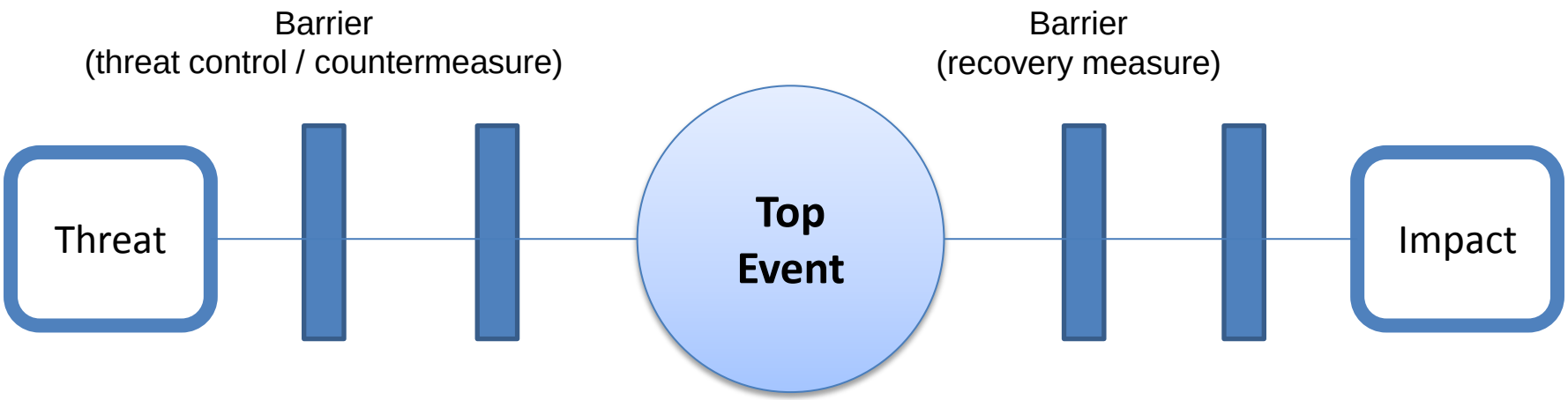
- Threat to the person vs Threat to the organisation
  - Person
    - All the data of a person are revealed
    - But only one customer is lost
  - Organisation
    - Limited data for each person is reveal
    - But trust is lost and organisation goes bankrupt
- Security threats vs Organisation/Process threats
  - Organisation/Process threats
    - Trust issue (e.g. too many persons have access to data)
    - Transparency issue (e.g. not enough mechanisms for transparency in integrated)
    - Accountability issue (e.g. liability issues are not well spelled out in the design)
- Small Threats vs Big Threats?
- Focus on counter measures VS recovery measures

Use Bow-Tie?

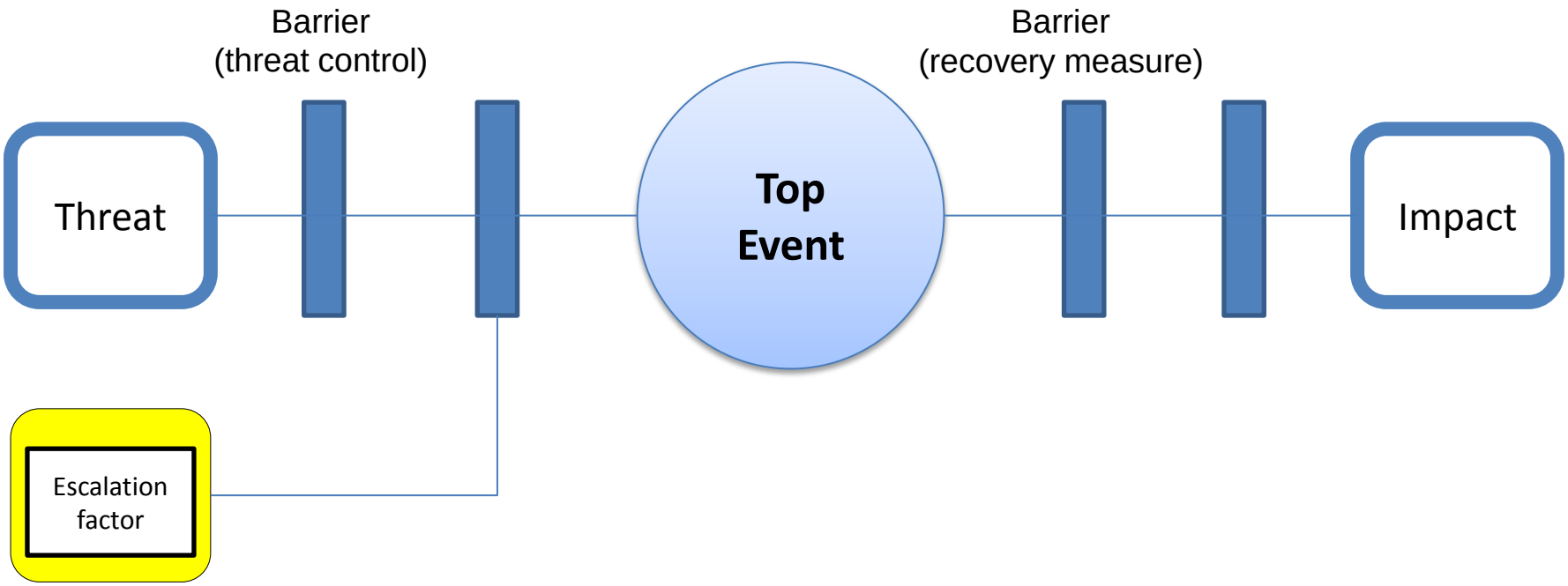
- Focuses on both countermeasures and recovery measures
- Focuses on top events (aka feared event)



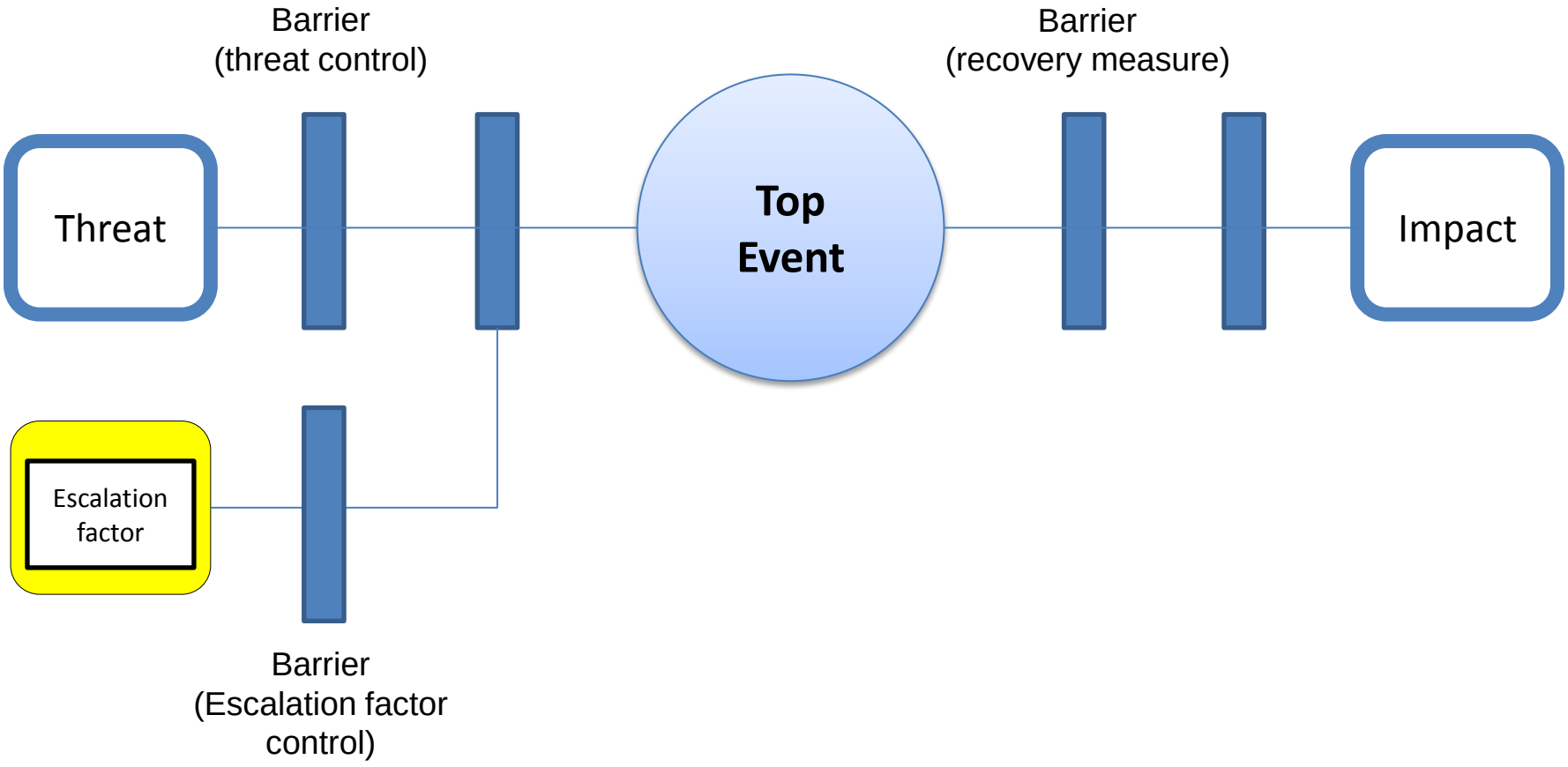
… from Threats to Impacts, with Barriers



… Escalation Factors



… Barriers for Escalation Factors

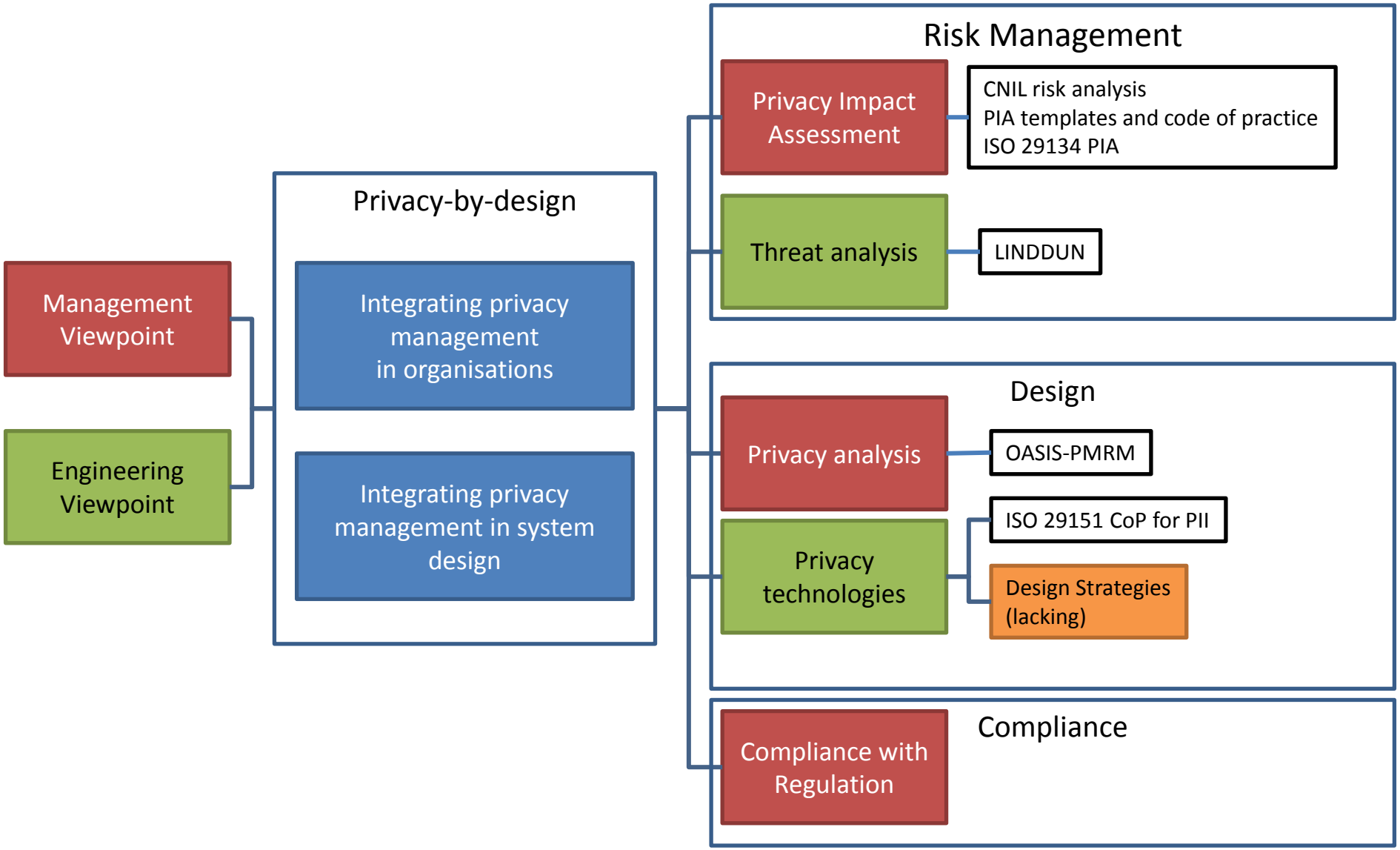


PRIPARE

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

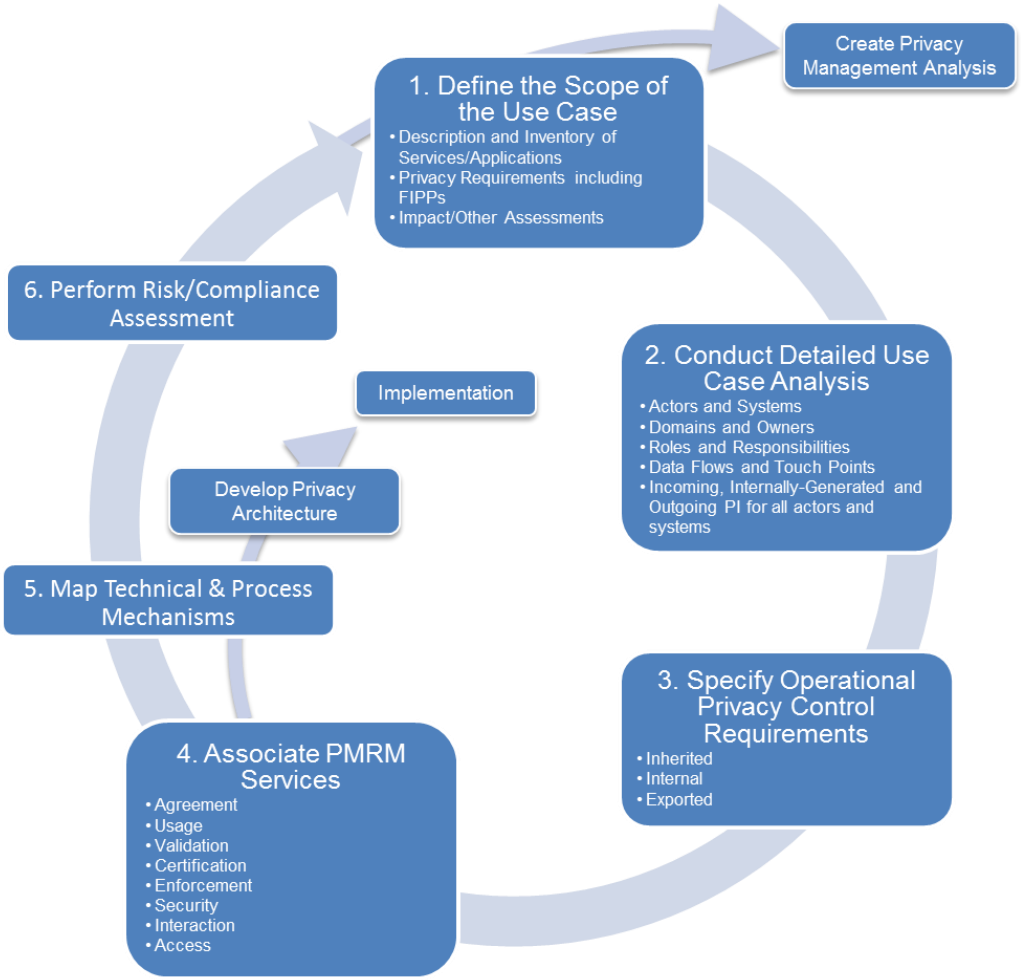
Design Management?

Current PbD Tools



OASIS PMRM

- Draft Standard
- Iterative
- Use case based
- Defines services
- Takes into account touch points



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

PRIPARE

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

Standardisation: Need for agreement on Concepts

Privacy Engineering?

- MITRE
  - A systematic, risk-driven process that operationalizes the Privacy by Design philosophical framework within IT systems …Privacy is integrated into systems as part of the systems engineering process
  - We like it
- Cavoukian
  - Discipline of understanding how to include privacy as a non-functional requirement in systems engineering
  - We prefer
    - Discipline of engineering systems integrating privacy as a non-functional requirement
- NIST
  - collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within information systems
  - We prefer
    - collection of methods to support the engineering of systems that mitigate risks to individuals arising from the processing of their personal information within information systems

NIST 8062 Privacy Engineering Objectives

- Vs Unlinkability/Transparency/Intervenability?

NIST Privacy Engineering Objectives	**Predictability**	**Enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system**
	Manageability	Providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure
	Disassociability	Enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.

Privacy Principles?

- E.g. ISO29100
- Relationship with privacy engineering objectives?

Consent and choice
Purpose legitimacy and specification
Collection limitation
Data minimization
Use, retention and disclosure limitation
Accuracy and quality
Openness, transparency and notice
Individual participation and access
Accountability
Information security
Privacy compliance

PRIPARE

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

Collaboration

ISO Study period on privacy engineering

- Contributions by August 15.
- We can provide a version to NIST by early August
- Sharing contributions?