Status

Study Period Privacy Engineering Framework (PEF)

Antonio Kung

PRIPARE

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

SEVENTH FRAMEWORK PROGRAMME

October 30th 2015

Outline

- Context and Summary
- Reminder Study Period Terms of Reference
- Overview of Contributions
- Sample Privacy Engineering Framework
- Further work

Context and Summary

- PRIPARE initiative to liaise with SO/IEC JTC1/ SC27/WG5 (October 2014 - Mexico)
- PRIPARE proposed a one year study period on Privacy Engineering Framework (May 2015 -Kuching)
  - Rapporteur Antonio Kung
  - Co-rapporteur Mathias Reins
- Intermediate report (October 2015 - Jaipur)
  - Contributions made by PRIPARE
  - Integrates NIST report and other contributions
- Objective until next meeting (May 2016 – Tampa)
  - Consolidating work
  - Integrating quality management, assurance, supplier viewpoints, …
  - Proposal for further work

Terms of Reference (1/2)

- Taken into account
  - ISO/IEC 29100, 29101, 29134, 27034
  - ISO/IEC 42010 (instead of 42001), 15288, 12207
  - CNIL methodology for privacy risk management
  - NIST Interagency Report on Privacy Engineering (draft forthcoming)
  - PRIPARE project methodology
  - OASIS Privacy Management Reference Model and Privacy by Design Documentation for Software Engineers
  - EDPS Internet Privacy Engineering Network
  - MITRE Privacy Engineering Framework
  - Centre for Information Policy Leadership research on Privacy Risk Management
- Establish a Study Period to review the emerging field of privacy engineering starting in May 2015 and

Terms of Reference (2/2)

- task the rapporteurs of the Study Period
  - to review privacy engineering terms, definitions, methodologies, frameworks, objectives, and principles to develop a high-level description of the privacy engineering process (taking into account the existing spectrum of models from traditional to agile models);
  - to review the relationship between privacy engineering and other privacy, security, and risk management standards, as appropriate;
  - to identify possible improvements to existing privacy impact assessment and management standards;
  - to potentially provide (a) New Work Item Proposal(s) and/or other input material to the Work Group, depending on the outcome of this assessment.
- A first call for contributions will be circulated after the May Meeting. The National Body contributions received in response to this call for contributions will be discussed at the ISO/IEC JTC 1/SC 27 Working Group 5 Meetings in October 2015.
- A second call for contributions will be circulated further to the October Meeting depending on the outcome of these discussions.

Overview of Contributions

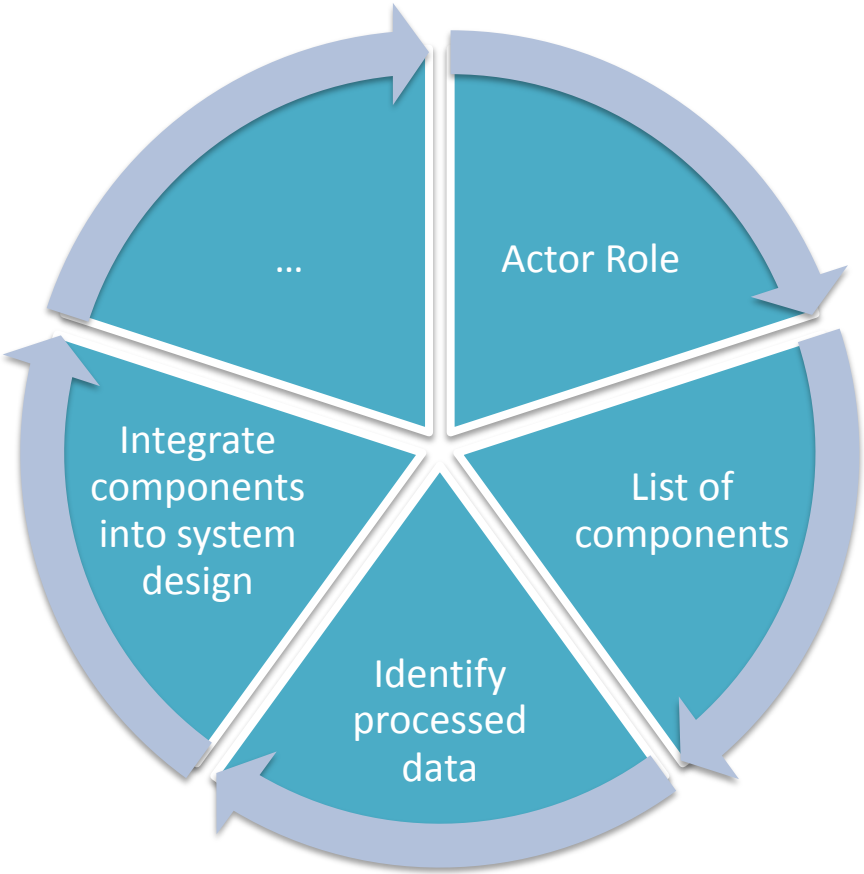
- Concerns/Recommendations
  - Clarify scope w.r.t to other standards e.g. 29134
  - Link with HL7 standards related to privacy
    - Privacy, Access and Security Services (PASS): Security Labeling Service, Release 1 (SLS)
    - Privacy, Access and Security Services (PASS): PASS ACS Access Control Functional Model, Obligation Service, Trust Framework
    - Patient Friendly Language for Consumer User Interfaces Implementation Guide (PFL),

Content

- Overall vision
  - Focus on a framework for practice
  - Take into account wealth of work on system and software engineering
    - ISO/IEC JCT1/SC7 systems and software engineering
    - Software engineering In particular reuse wealth of knowledge (www.swebok.org;http://www.computer.org/web/swebok/v3)

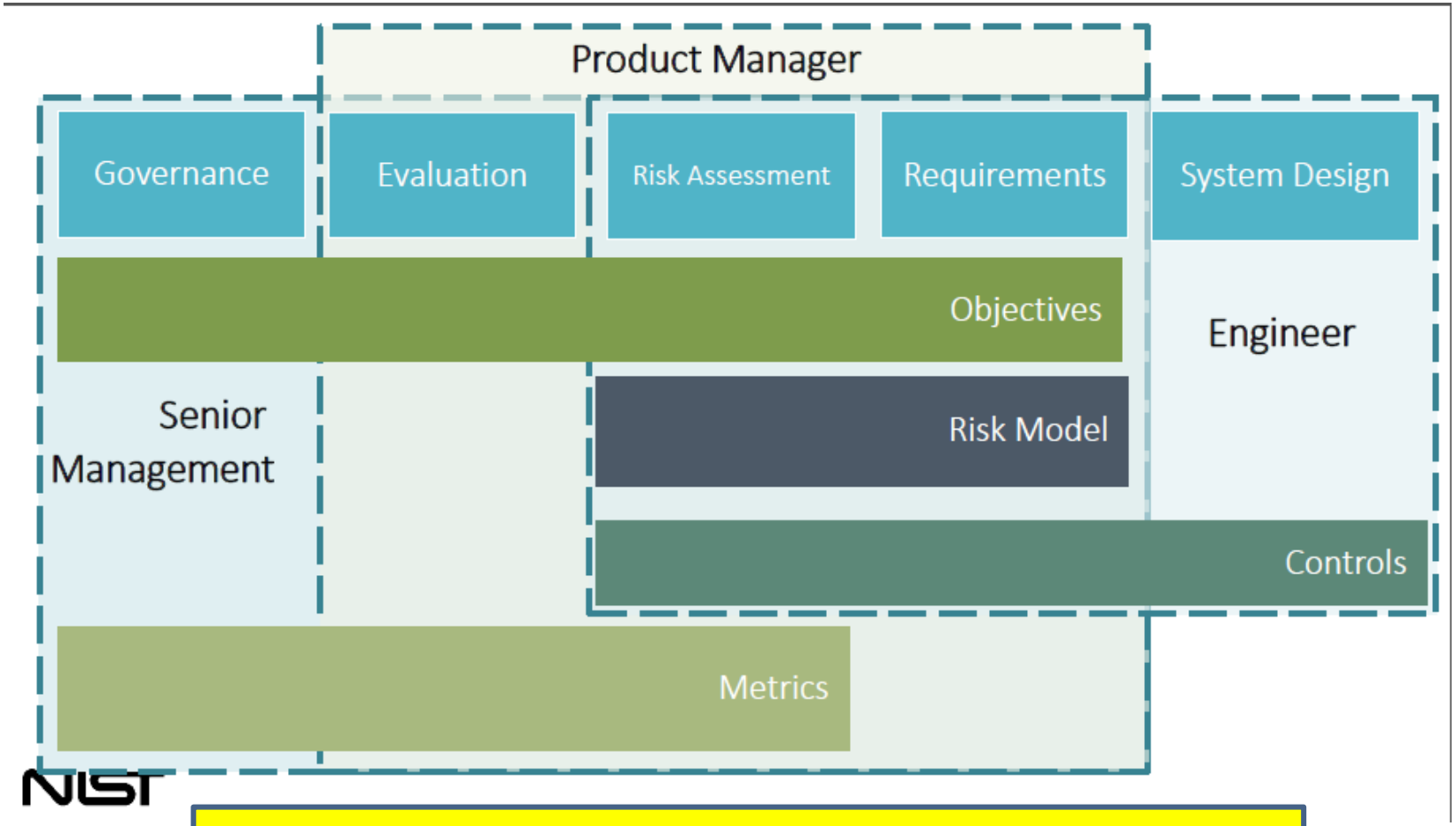
Content

- Defines important steps in engineering
- Example (material prepared for 29101 but not integrated)
  - Step One: Determine the actor roles of the PII handling ICT systems
  - Step Two: Compile the list of components required by each ICT system
  - Step Three: Identify processed data
  - Step Four: Integrate the components into ICT system design.



NIST Report

from Informal NIST PRIPARE Discussion 1/4



Contribution on privacy engineering framework

Positioning Privacy Engineering In Organisations

NIST Report
from Informal NIST PRIPARE Discussion 2/4

Draft Privacy Engineering Objectives

- Design characteristics or properties of the system
- Support policy
- Support control mapping

Predictability is the enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.

Manageability is providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure.

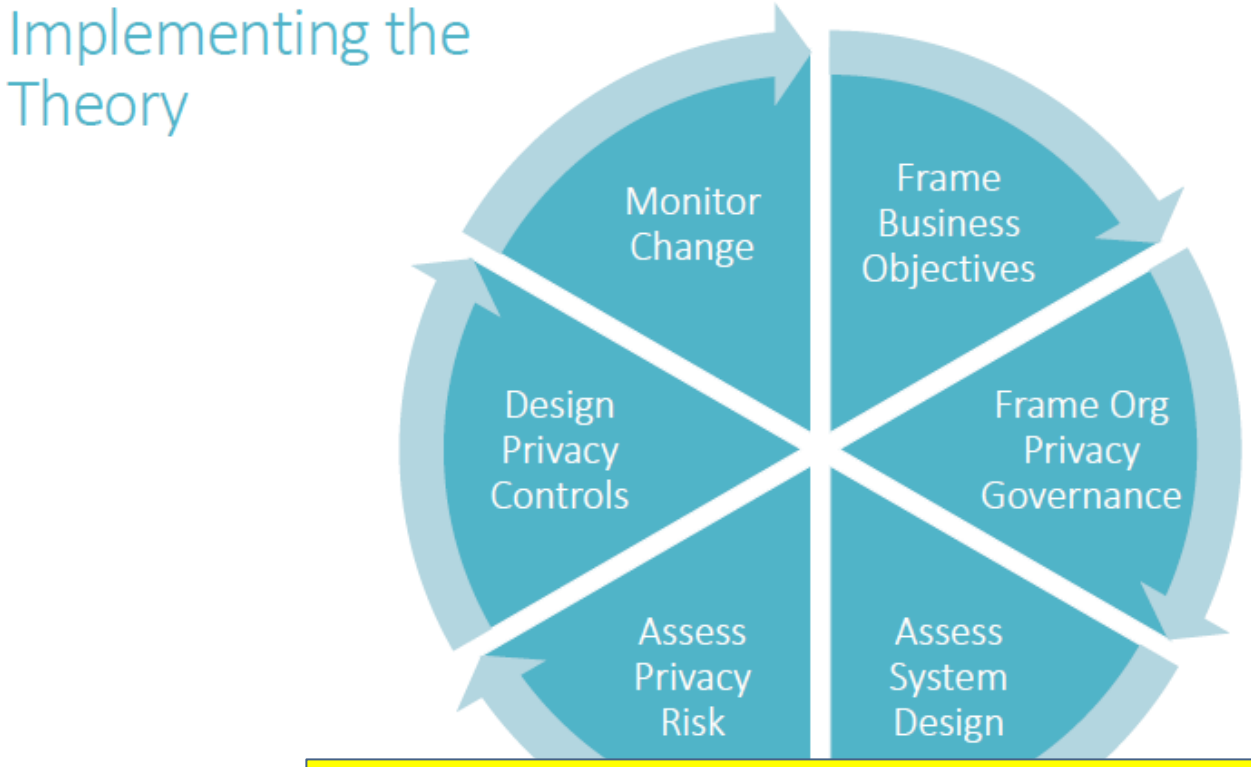
Disassociability is enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.

NIST

Contribution on privacy engineering framework
Privacy Engineering Objectives

8

NIST Report
from Informal NIST PRIPARE Discussion 3/4



Contribution on privacy risk framework

Methodology

Contribution on privacy engineering framework

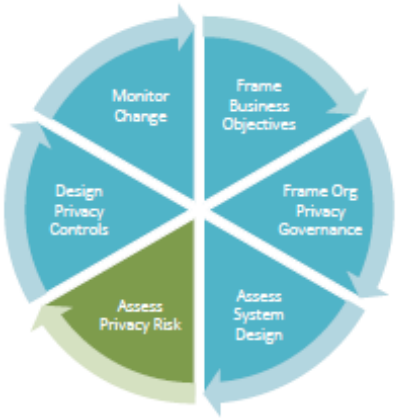
Important steps in system engineering

NIST Report
from Informal NIST PRIPARE Discussion 4/4

Contribution on privacy risk framework

Methodology

Assess Privacy Risk



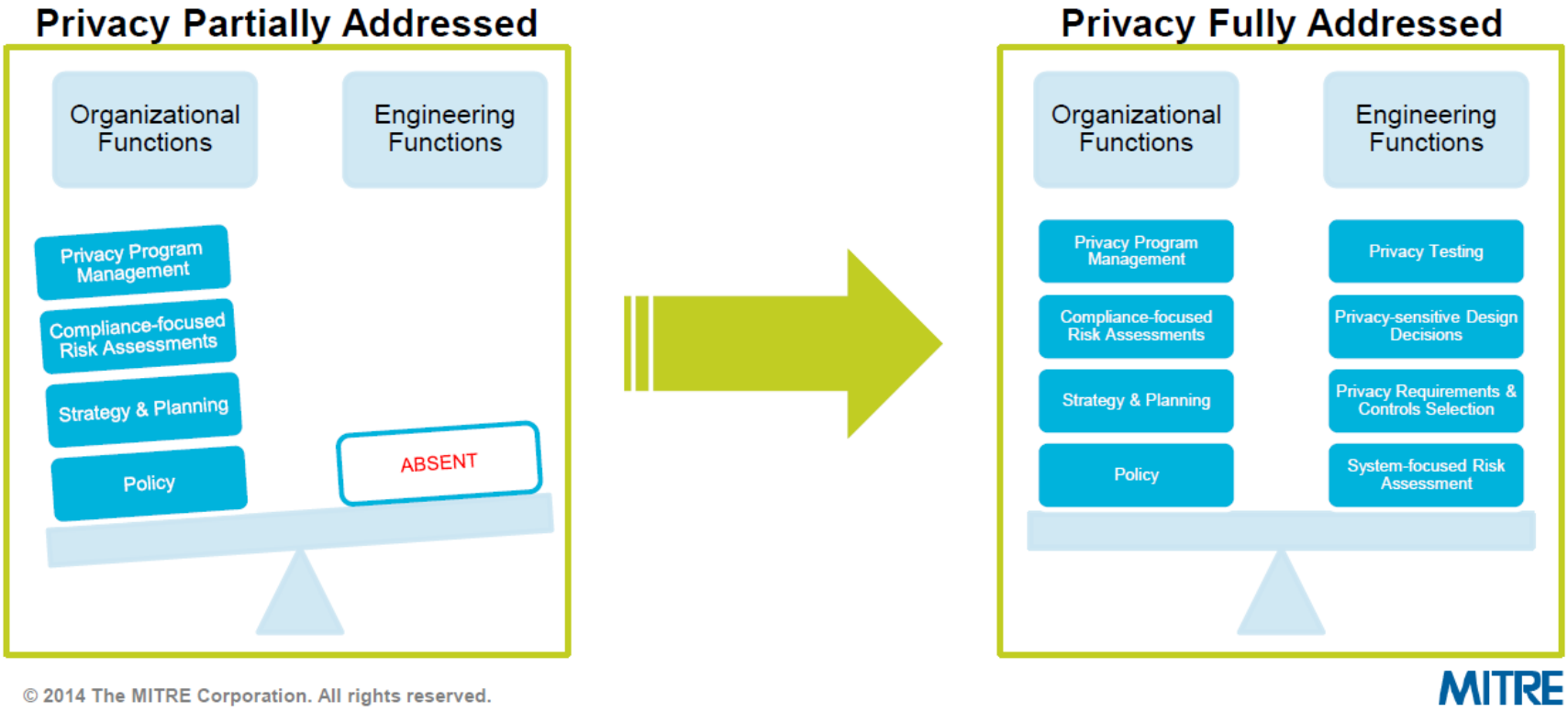
SAMPLE TABLE

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -Surveillance -Unanticipated Revelation	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	7
			Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.	2
	Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider?	-This summary issue will be associated with another data action.		NA
	How will percept organization's priva willingness to con			

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Business Impact Factors					Total Business Impact (per Potential Problem)
				Noncompliance Costs	Direct Business Costs	Reputational Costs	Internal Culture Costs	Other	
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -Surveillance -Unanticipated Revelation	Stigmatization	7	6	6	4		23
			Power Imbalance	7	6	8	4		25
	How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action?	-Induced disclosure -Surveillance	Loss of Trust	7	6	8	7		28

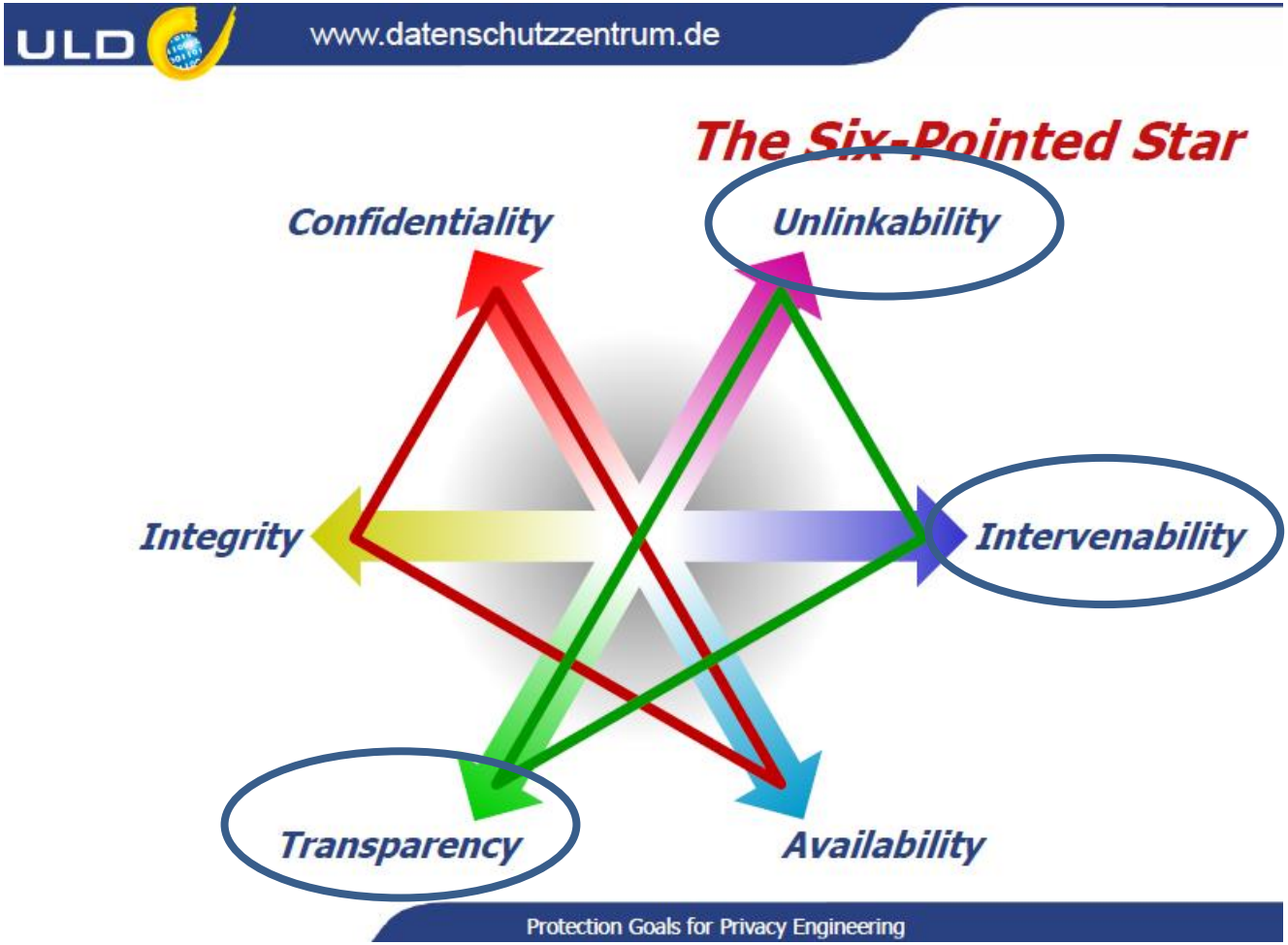
PRIPARE compilation 1/6

- MITRE



Contribution on privacy engineering framework
Rationale

PRIPARE compilation 2/6

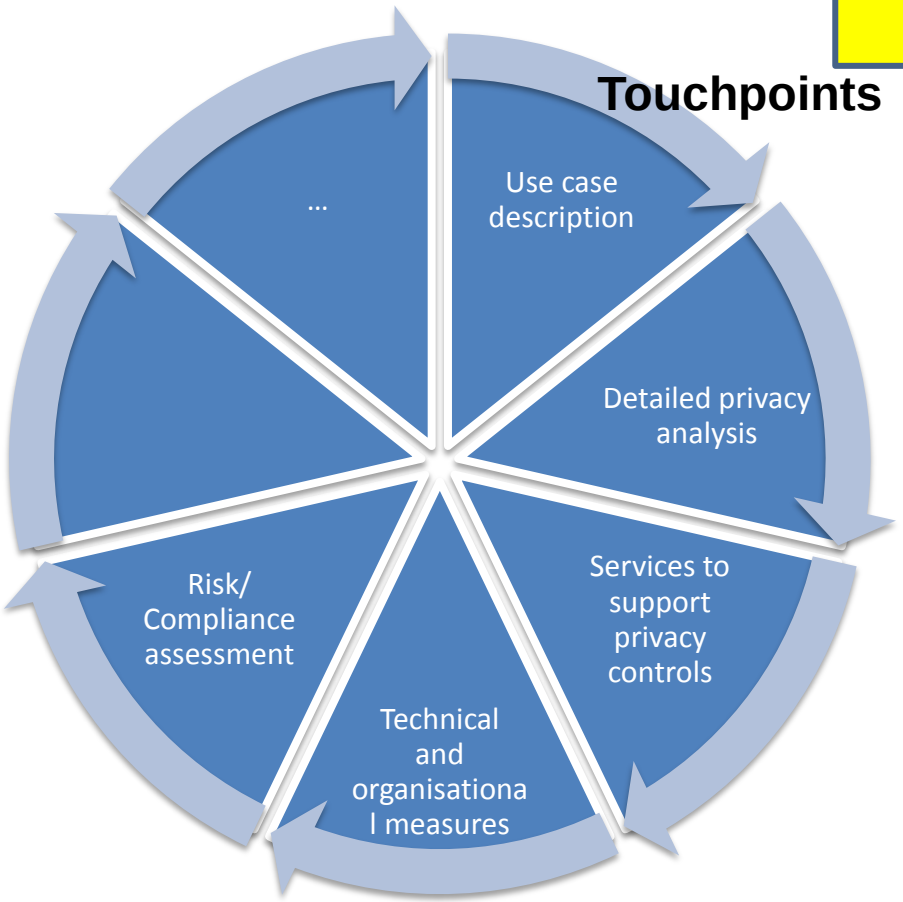


Contribution on privacy engineering framework
Privacy Protection Goals

PRIPARE compilation 3/6

- OASIS PMRM

Contribution on privacy engineering
Process for Operational Privacy control Requirements



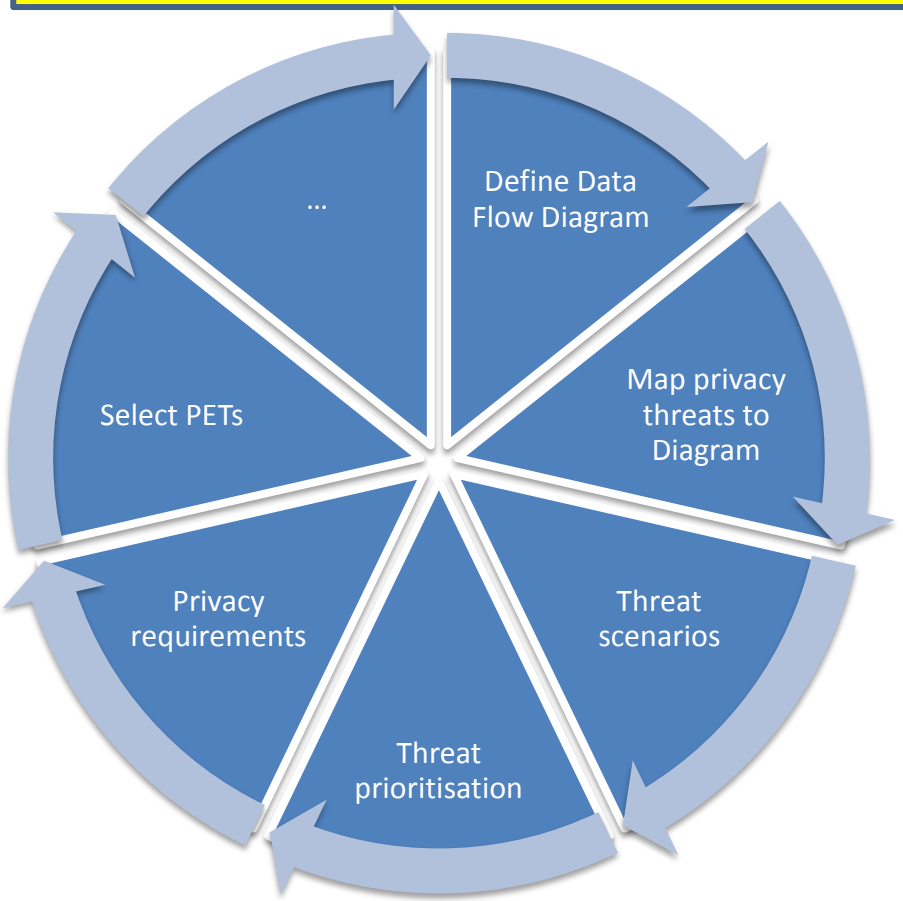
Service	Purpose
Agreement	Management of permissions and rules
Usage	Controlling personal data usage
Validation	Checking personal data
Certification	Checking stakeholders credentials
Enforcement	Monitor operations and react to exceptions
Security	Safeguard privacy information and operations
Interaction	Information presentation and communication
Access	Data subject access to their personal data
Accountability (proposal)	Log and audit management

PRIPARE compilation 3/6

- LINDDUN

Property	Threat
Unlinkability	**L**inkability
Anonymity	**I**dentifiability
Plausible deniability	**N**on-repudiation
Undetectability and unobservability	**D**etectability
Confidentiality	**D**isclosure of information
Content awareness	**U**nawareness
Policy and consent compliance	**N**on compliance

Contribution on privacy engineering
Threat-based methodology



PRIPARE compilation 4/6

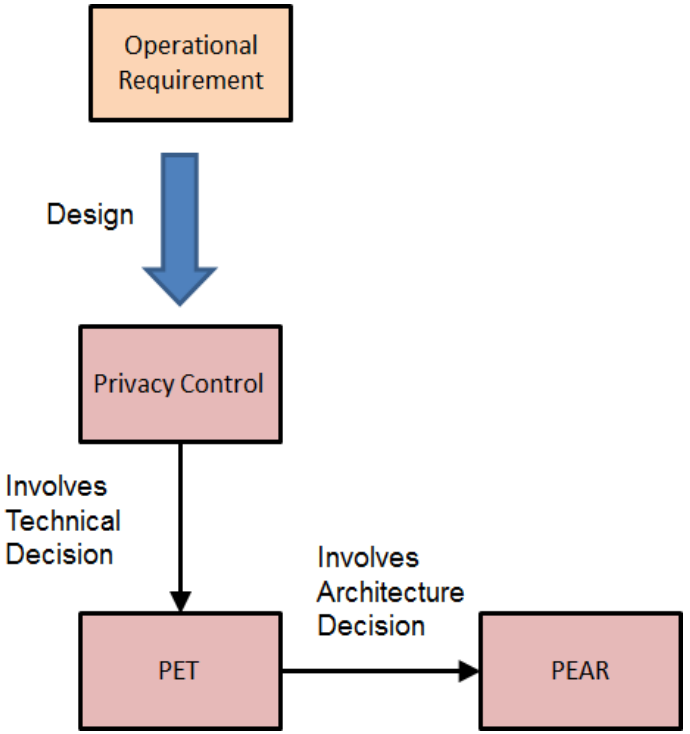
- Hoepman design strategy

Data oriented strategies	**1 Minimization**	**Amount of processed personal data restricted to the minimal amount possible**
	2 Hide	Personal data, and their interrelationships, hidden from plain view
	3 Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible
	4 Aggregate	Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful
Process oriented strategies	5 Inform	Transparency
	6 Control	Data subjects provided agency over the processing of their personal data
	7 Enforce	Privacy policy compatible with legal requirements to be enforced
	8 Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements

Contribution on privacy engineering framework
Principles for design of privacy controls

PRIPARE compilation 5/6

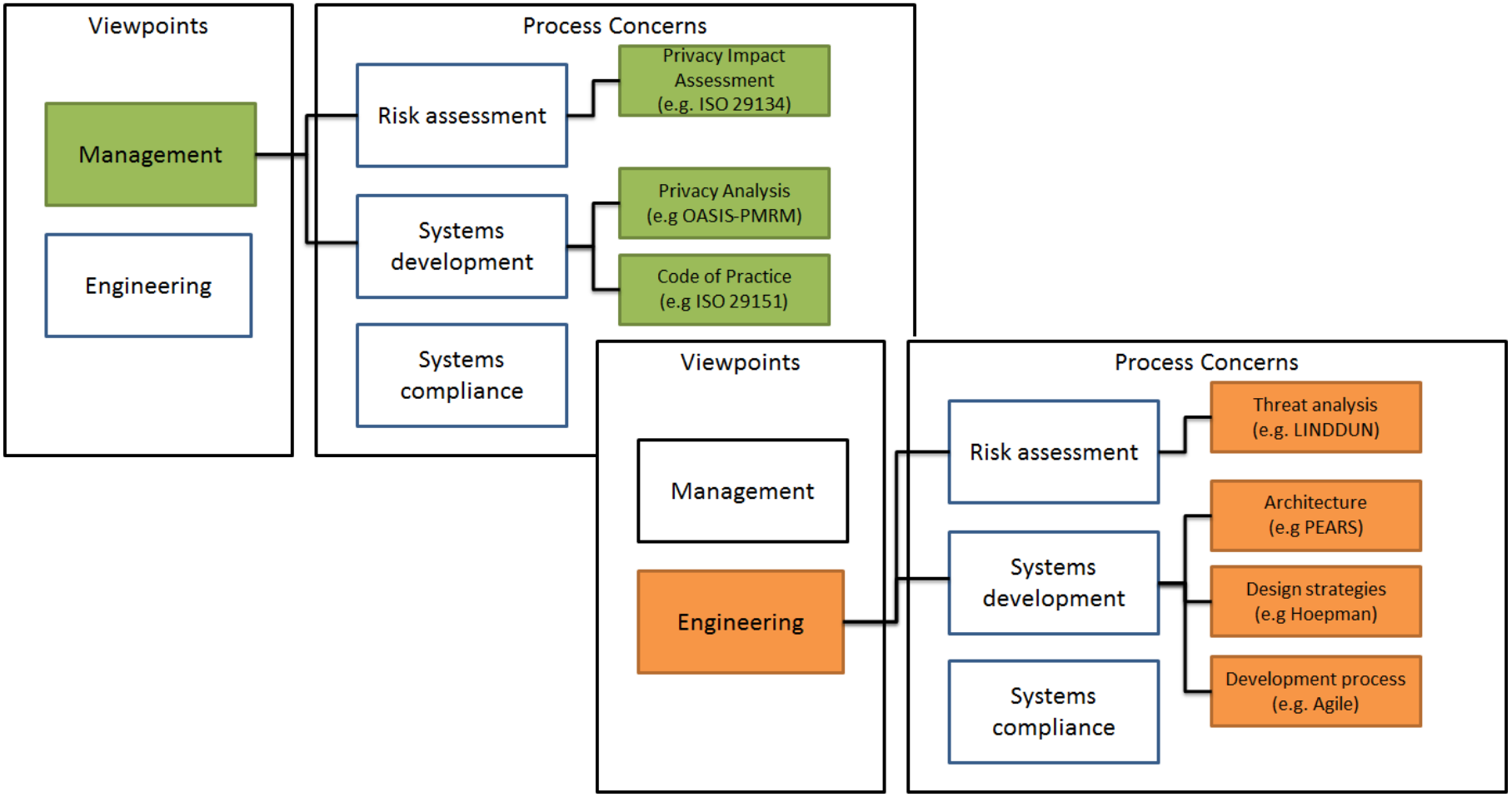
- Privacy Enhancing architectures



Contribution on privacy engineering framework

Designing PETS involve Architecture Decisions

PRIPARE compilation 6/6



Contribution on privacy engineering framework
Positioning Privacy Engineering In Organisations

Strawman PEF
(Privacy Engineering Framework)

Integrates in PRIPARE proposal other contributions

PRIPARE

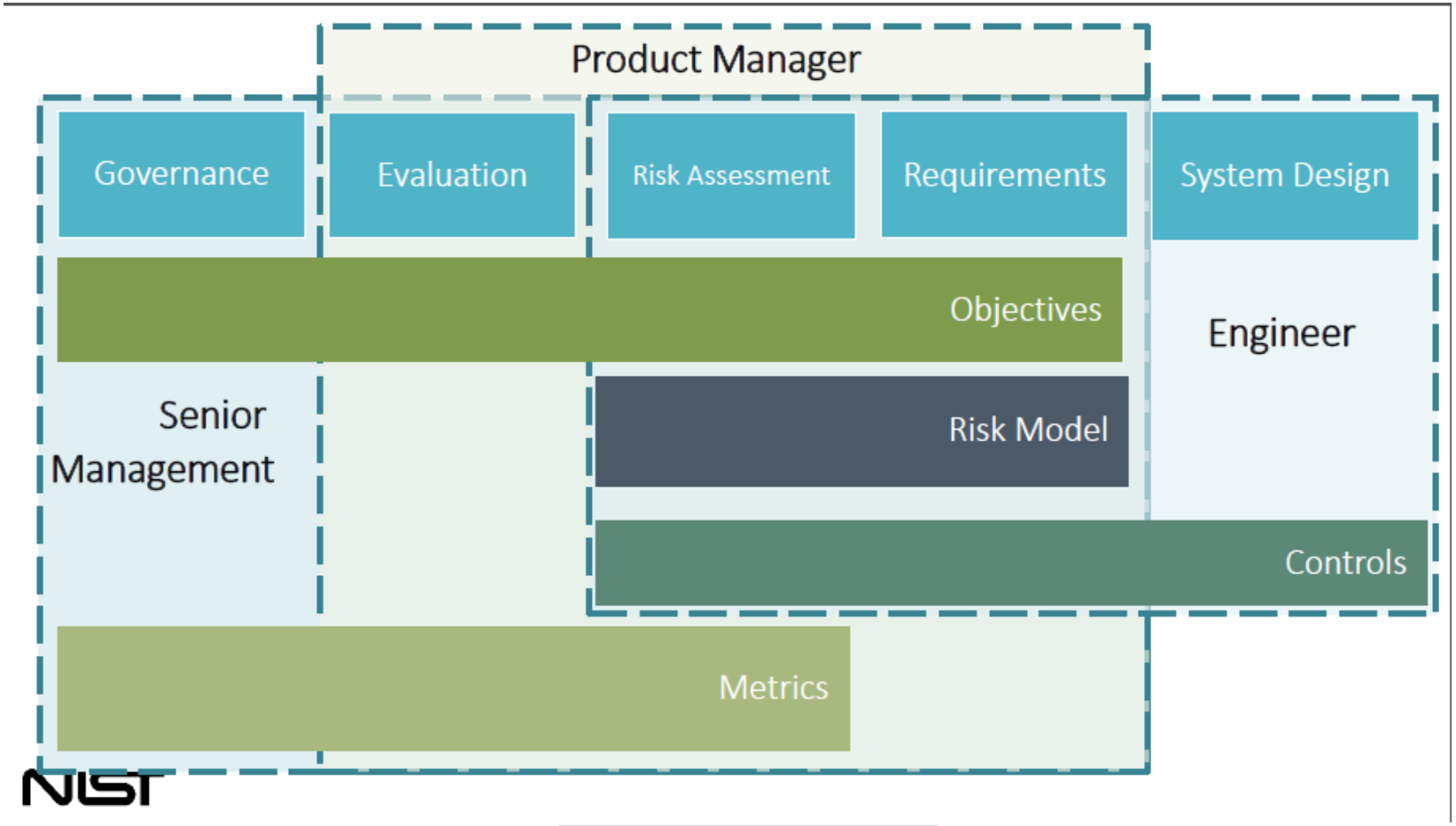
PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

SEVENTH FRAMEWORK PROGRAMME

Strawman PEF: Structure Inspired by 29100

- Introduction/Positioning
- Basic concepts
  - Privacy engineering and Privacy-by-design
  - Privacy engineering objectives
  - Privacy protection goals
  - Organisation support
  - Lifecycle support
    - Privacy Analysis : from privacy principles to privacy control requirements
    - Privacy Design: from privacy control requirements to privacy controls
- Privacy engineering principles

Strawman PEF: Introduction/Positioning



Focus on Practice

Strawman PEF: Basic Concepts

- Privacy engineering
  - A systematic, risk-driven process that operationalizes the Privacy-by-Design philosophical framework within IT systems. Privacy concerns are subsequently integrated into systems as part of the systems engineering process
- Privacy-by-design
  - Institutionalisation of the concepts of privacy and security in organisations and integration of these concepts in the engineering of systems

Example of definitions / Not Final!

Strawman PEF: Basic Concepts

- Privacy Engineering Objectives
  - Design characteristics or properties of the system
  - Support policy
  - Support control mapping

Predictability is the enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.

Manageability is providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure.

Disassociability is enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.

NIST

8

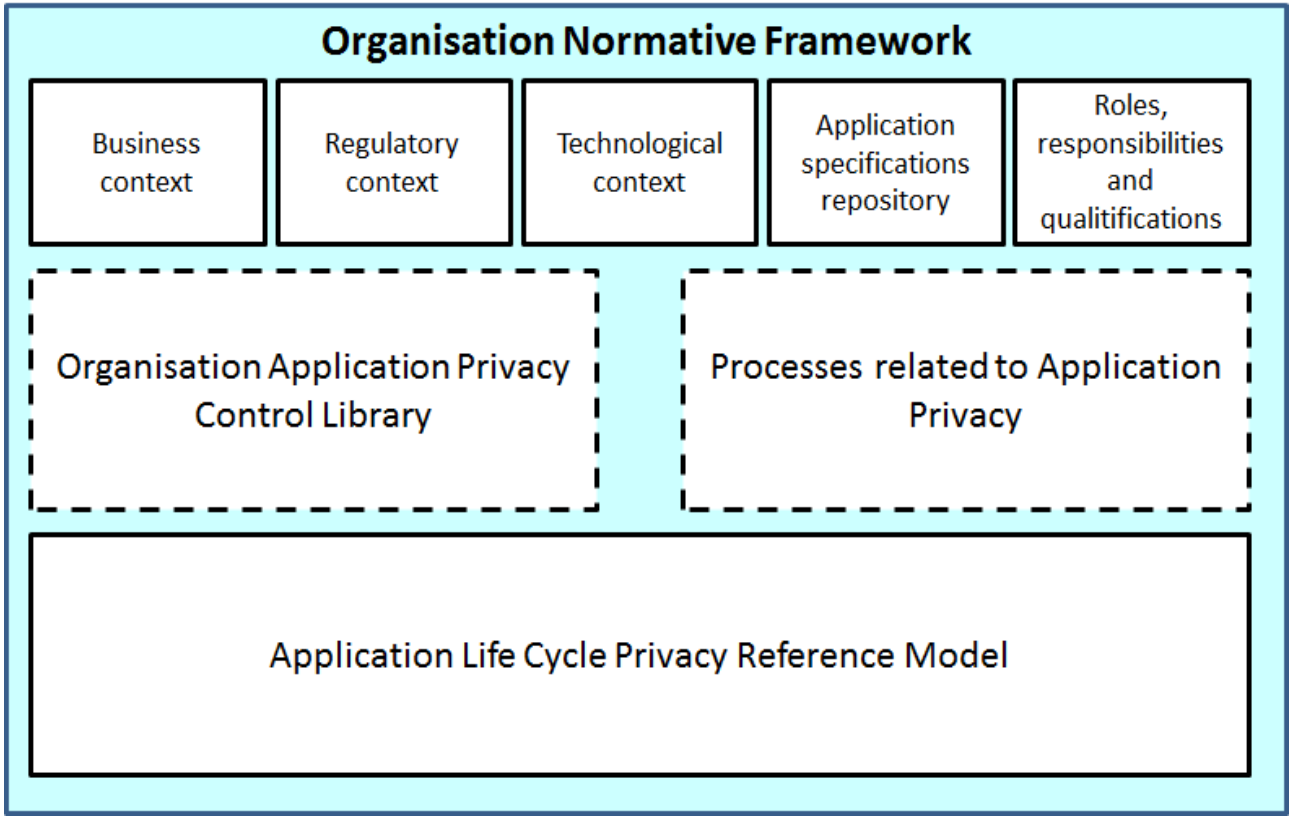
Strawman PEF: Basic Concepts

- Privacy Protection Objectives
  - Complements security protection goals (confidentiality, integrity, availability)

Unlinkability	Ensures that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended.
Transparency	Ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed.
Intervenability	Ensures that data subjects, operators and supervisory authorities can intervene in all privacy-relevant data processing.

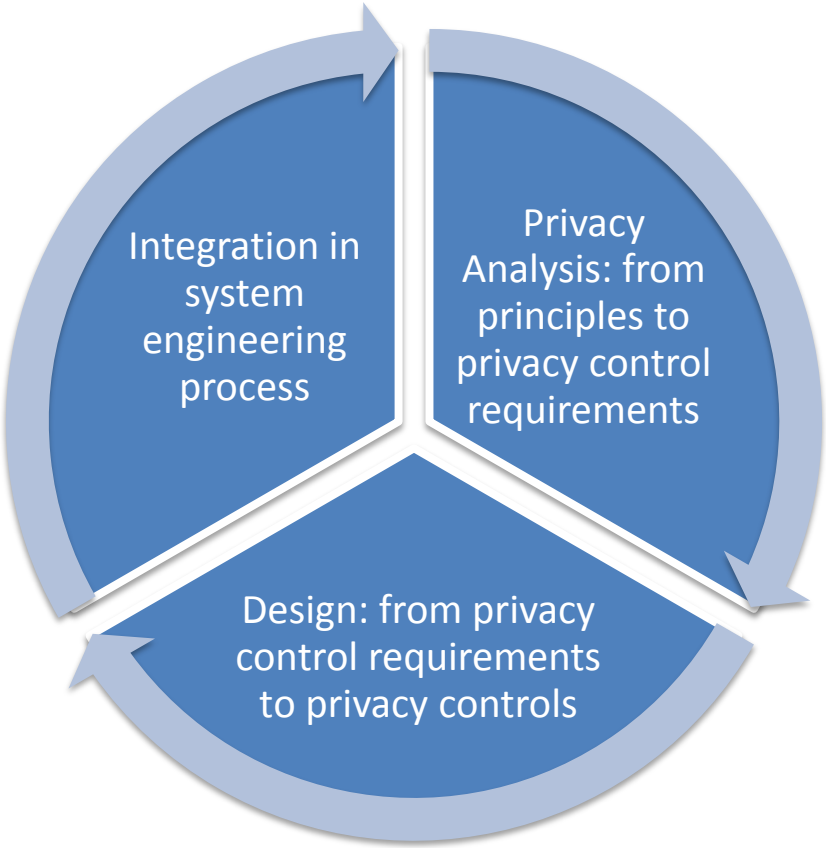
Strawman PEF: Basic Concepts

- Organisation support
  - inspired from ISO 27034, adapted to privacy



Strawman PEF: Basic Concepts

- Lifecycle support
  - Stick to principle level to support different methodologies and software engineering approaches



Strawman PEF: Basic Concepts

- Lifecycle support: privacy analysis
  - From privacy principles to privacy control requirements
    - Step 1: Definition of scope of use case (inventory of services, applications, privacy principles, list of threats)
    - Step 2: Detailed use case analysis (stakeholders, data flows and touch points)
    - Step 3: Identify operational requirements (by carrying out a threat analysis and a goal oriented analysis)
    - Step 4: Associate privacy functional services
  - Organisation support
    - List of principles and associated catalog of guidelines and criteria
    - Categories of threats and associated catalog
    - Categories of privacy functional services and associated catalog

Strawman PEF: Basic Concepts

- Lifecycle support: privacy design
  - From privacy control requirements to privacy controls design
    - Step 1: Identification of privacy control (PETS) using privacy design strategies
    - Step 2: if needed identification of architecture decisions (PEARs)
    - Step 3: if needed evaluate architecture
    - Step 4: Identification of privacy patterns
    - Step 5: Evaluation of privacy control effectiveness (e.g. privacy quantification)
    - Step 6: Evaluation of compliance
  - Organisation support
    - List of design strategies and associated catalog of patterns and controls

Strawman PEF: Privacy Engineering Principles

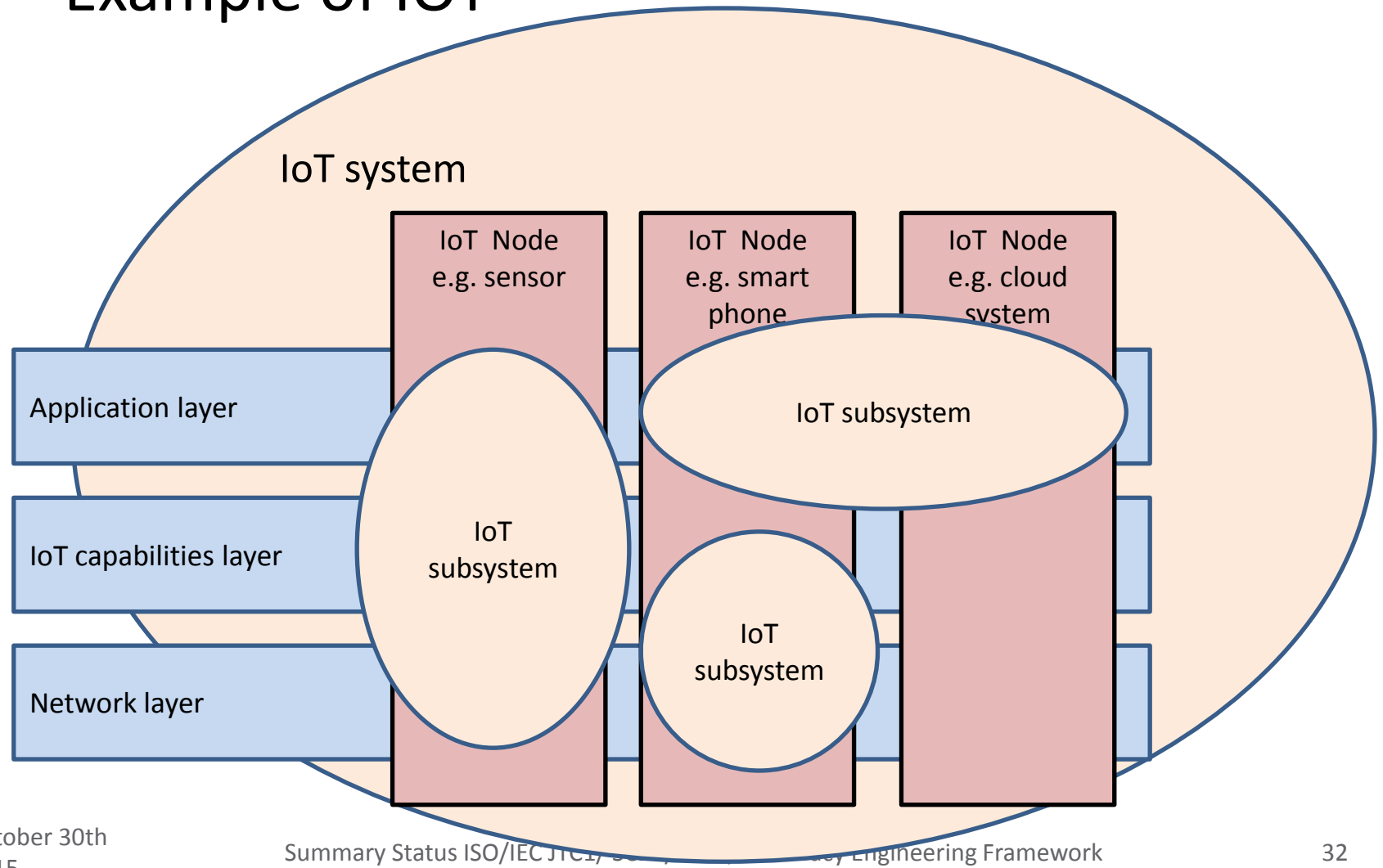
Privacy Engineering Principles	
(1) Integration of risk management	
(2) Integration of compliance	
(3) Engineering objectives	Dissociability
	Predictability
	Manageability
(4) Privacy protection goals	Unlinkability
	Transparency
	Intervenability
	…
(5) Design strategies	Data oriented Design strategies
	Process oriented Design strategies
(6) Lifecycle Support for privacy engineering	
(7) Organisation Support for privacy engineering	

Taking into account references

Privacy Engineering Principles – ISO 29100	
(1) Integration of risk management – ISO29134 / CNIL / NIST	
(2) Integration of compliance	
(3) Engineering objectives	Dissociability
	Predictability
	Manageability
(4) Privacy protection goals	Unlinkability
	Transparency
	Intervenability
(5) Design strategies	Data oriented Design strategies
	Process oriented Design strategies
(6) Lifecycle Support for privacy engineering – ISO 29101, ISO29151, OASIS PMRM – ISO15288, ISO12207, ISO42010	
(7) Organisation Support for privacy engineering – ISO27034	

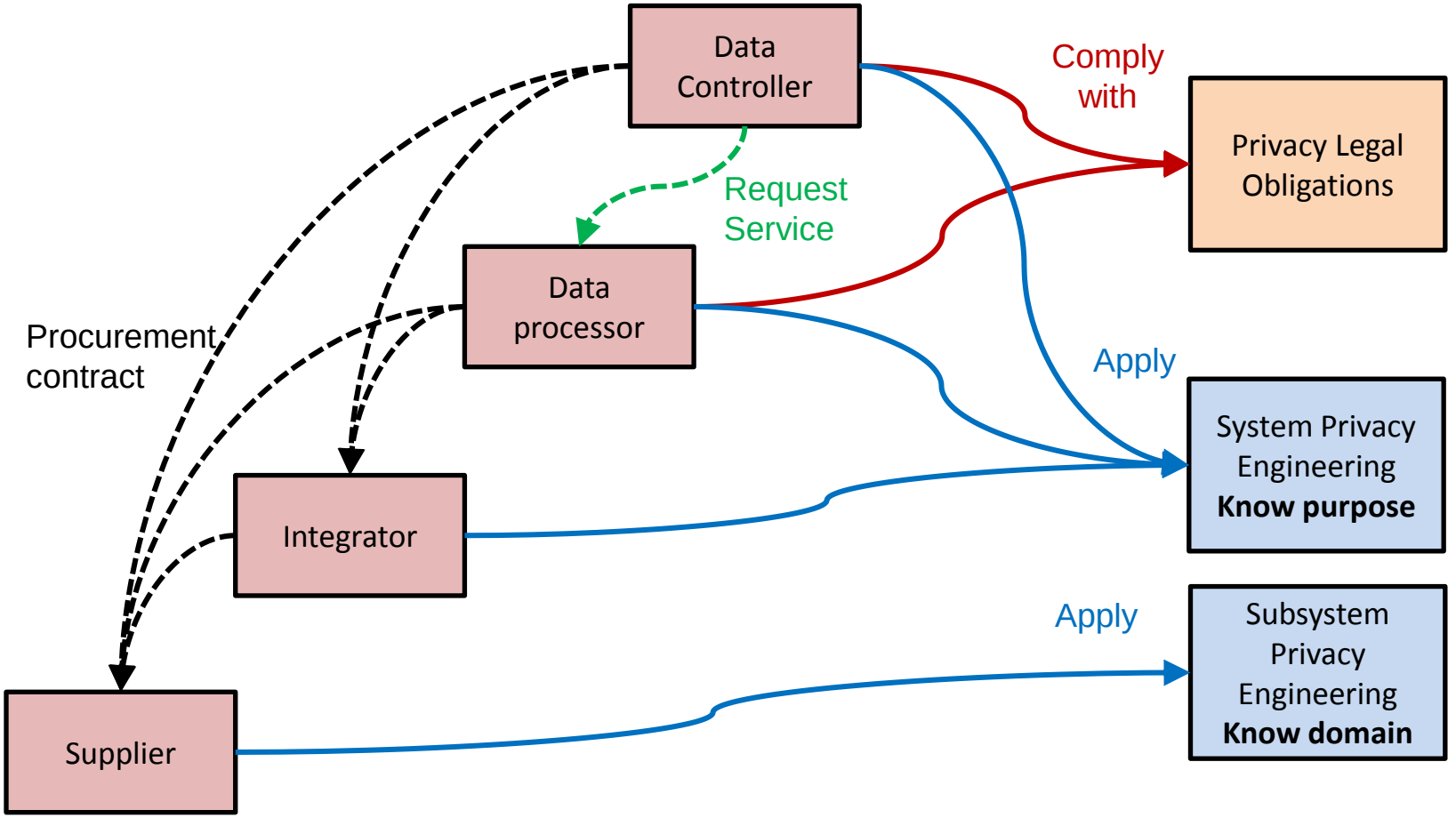
Further work: Supplier role

- Example of IOT



Further work: Supplier role

- IoT Value Chain (Privacy Viewpoint)



Further work

- Refinement of current work in the domain of
  - requirements, architecture, roles and practices
  - Quality management
  - Assurance
- Suppliers' viewpoint
- Cultural influence / Different legal domains
- Lifecycle support e.g. methodologies, existing standards, etc.
- Any other relevant aspect of WG5 (e.g. SP on privacy notice)

Thanks

PRIPARE

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

SEVENTH FRAMEWORK PROGRAMME