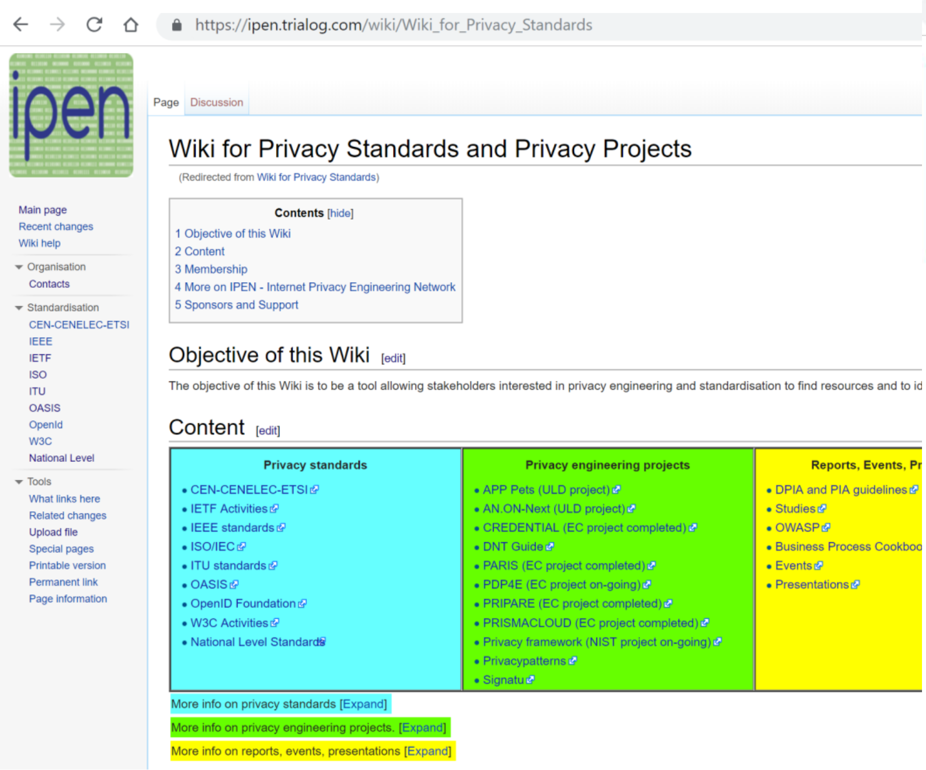
Standards for Privacy-by-design

Antonio Kung, CTO
25 rue du Général Foy, 75008 Paris
www.trialog.com

Introduction Speaker

- Engineering background
  - Coordinator PRIPARE (pripareproject.eu) 2013-2015
    - Methodological Tools to Implement Privacy and Foster Compliance with the GDPR
    - Liaison with ISO/IEC JTC1/SC27/WG5
    - Member of OASIS (Privacy Management Reference Model - PMRM)
- Active participation in privacy standards since PRIPARE
  - Consumer protection -- Privacy by design for consumer goods and services (ISO 31700 contributor)
  - Privacy engineering (ISO/IEC 27550 editor)
  - Big data – Security and privacy fabric (ISO/IEC 20547-4 contributor)
  - Privacy guidelines for smart cities (ISO/IEC 27570 editor)
  - Security and privacy guidelines for IoT (ISO/IEC 27030 co-editor)
  - User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences (ISO/IEC 27556 co-editor)
- Others
  - FG-DPM (D4.1 Framework of Security and Privacy in Data Processing Management)
  - European Innovation Platform – Smart Cities and Communities
    - Citizen approach to data: privacy-by-design

IPEN member (ipen.trialog.com)



https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards

Wiki for Privacy Standards and Privacy Projects

(Redirected from Wiki for Privacy Standards)

Objective of this Wiki [edit]

The objective of this Wiki is to be a tool allowing stakeholders interested in privacy engineering and standardisation to find resources and to id

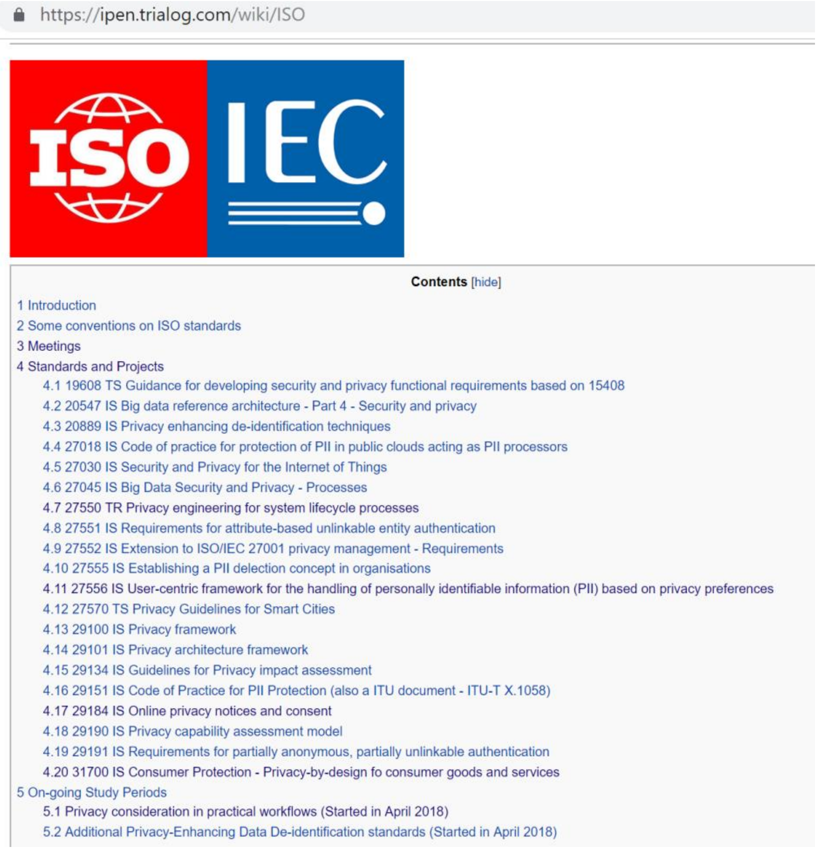
Content [edit]

Privacy standards	Privacy engineering projects	Reports, Events, Pr
• CEN-CENELEC-ETSI • IETF Activities • IEEE standards • ISO/IEC • ITU standards • OASIS • OpenID Foundation • W3C Activities • National Level Standards	• APP Pets (ULD project) • AN.ON-Next (ULD project) • CREDENTIAL (EC project completed) • DNT Guide • PARIS (EC project completed) • PDP4E (EC project on-going) • PRIPARE (EC project completed) • PRISMACLOUD (EC project completed) • Privacy framework (NIST project on-going) • Privacypatterns • Signatu	• DPIA and PIA guidelines • Studies • OWASP • Business Process Cookboo • Events • Presentations

More info on privacy standards [Expand]

More info on privacy engineering projects. [Expand]

More info on reports, events, presentations [Expand]



https://ipen.trialog.com/wiki/ISO

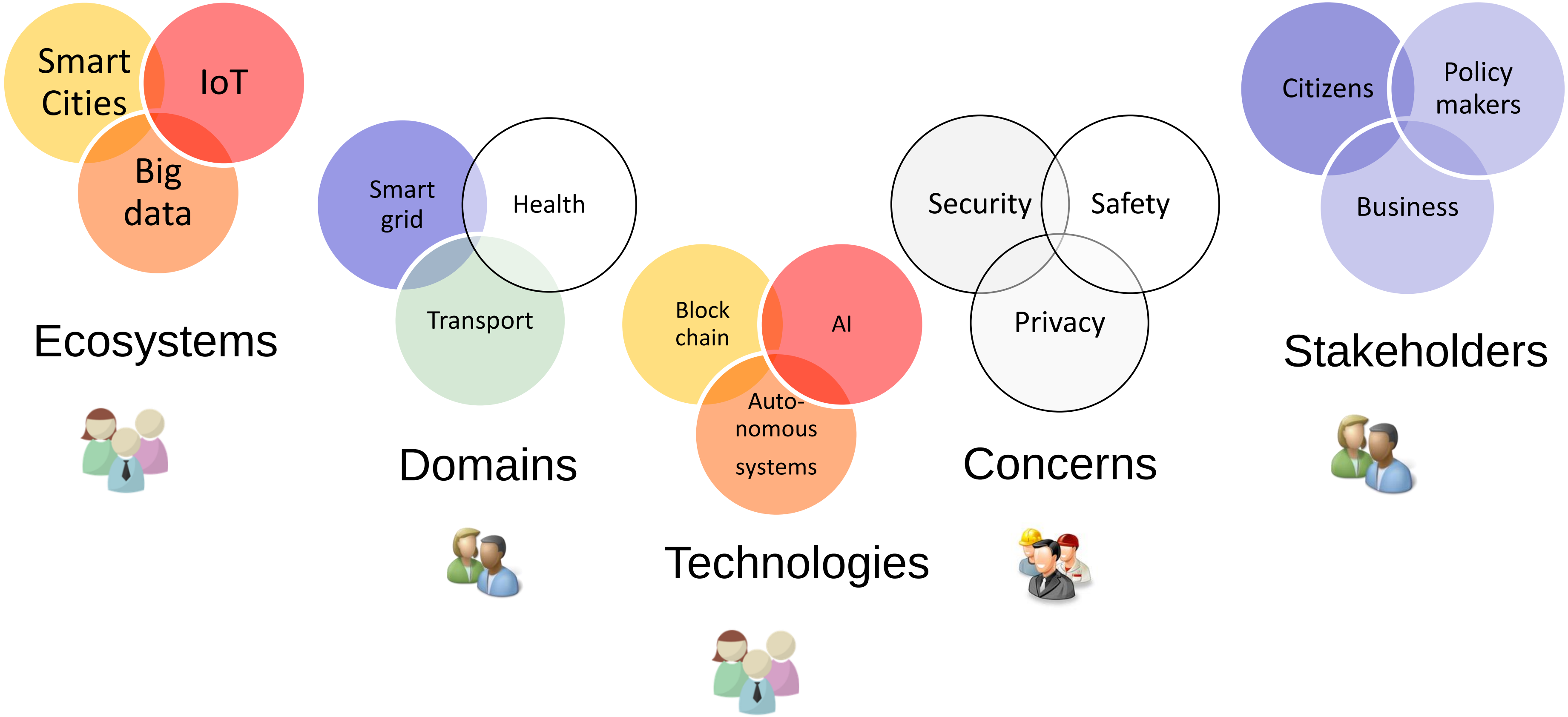
Outline

- Privacy from a policy maker viewpoint
- Overview of standards
  - 27550 Privacy engineering for system lifecycle processes
  - 27570 Privacy guidelines for smart cities
  - 27556 User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences
  - 31700 Consumer protection: privacy-by-design for consumer products and services

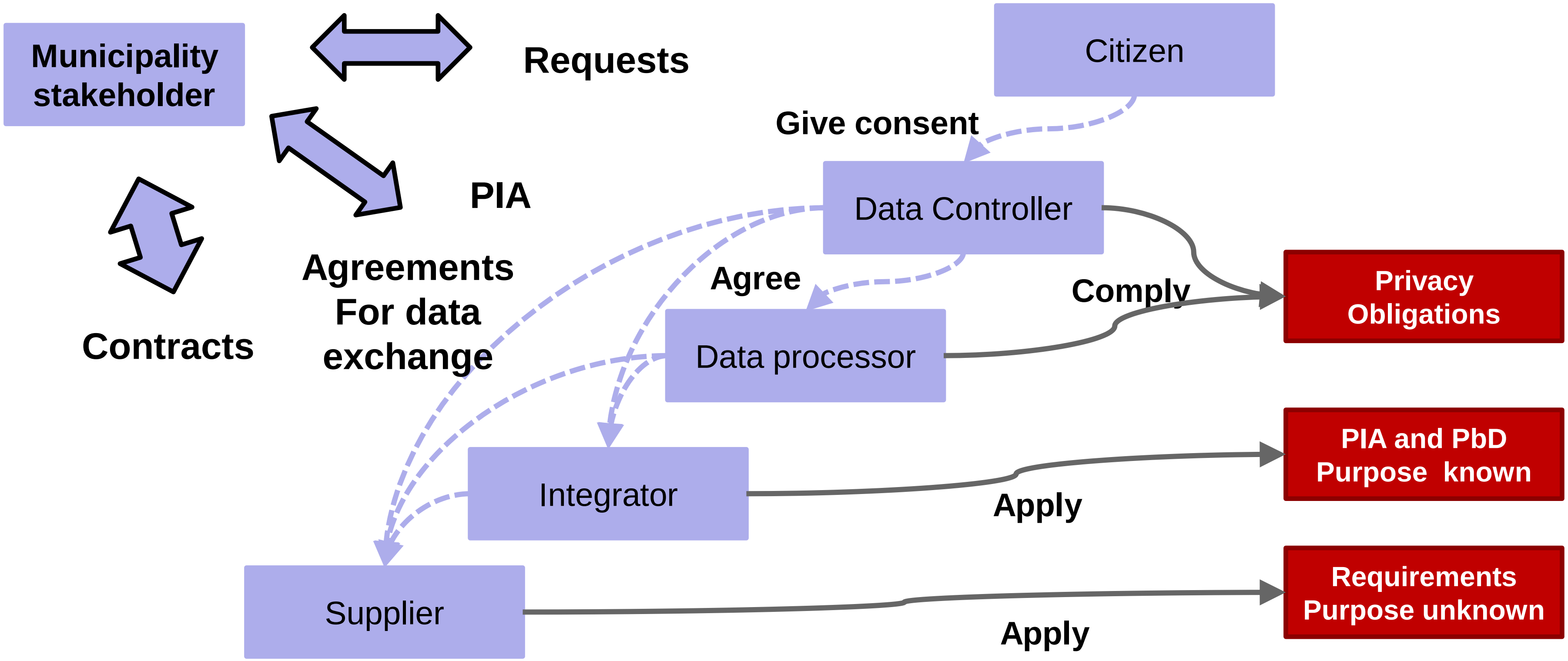
Privacy from a Policy Maker Viewpoint

Example of smart cities

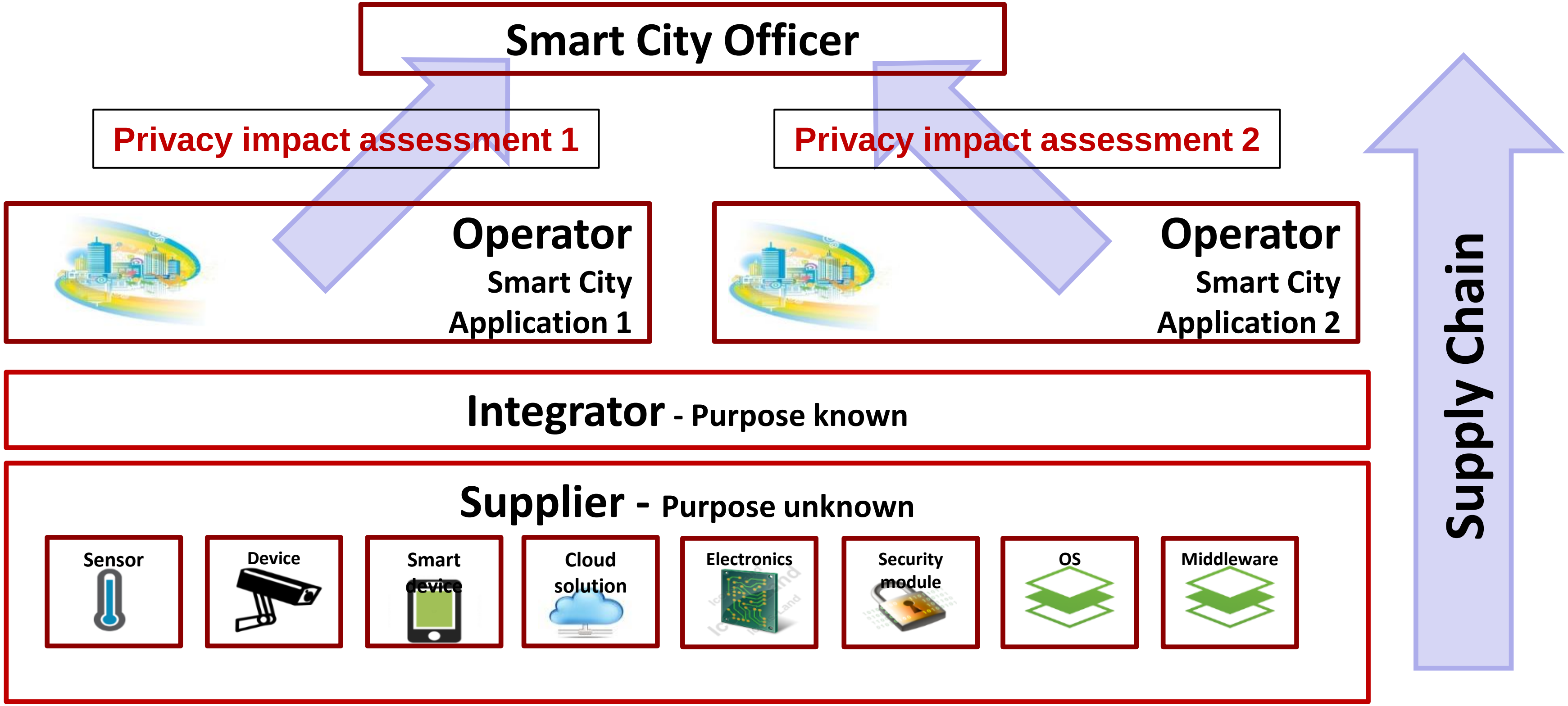
They deal with complex ecosystems



They manage privacy for these ecosystems



Including a supply chain vision



Smart City Officer

Privacy impact assessment 1

Privacy impact assessment 2

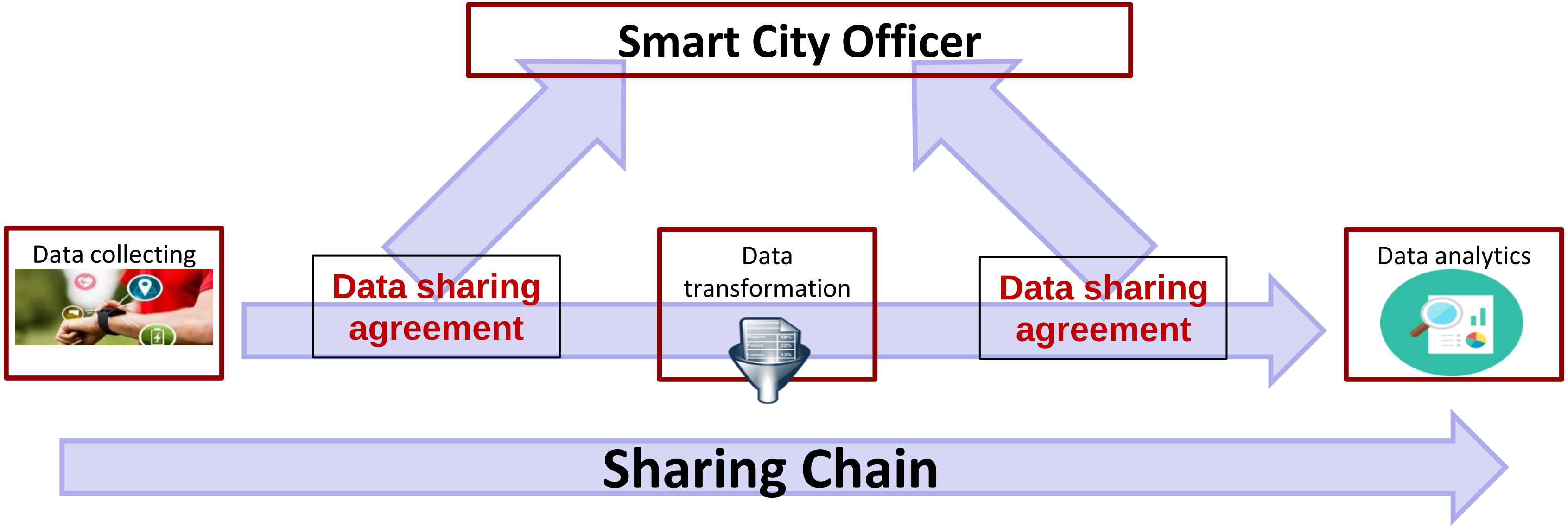
Operator
Smart City
Application 1

Operator
Smart City
Application 2

Integrator - Purpose known

Supplier - Purpose unknown

Including a sharing chain vision



Smart City Officer

Data collecting

Data sharing agreement

Data transformation

Data sharing agreement

Data analytics

Sharing Chain

Several Types of Concerns

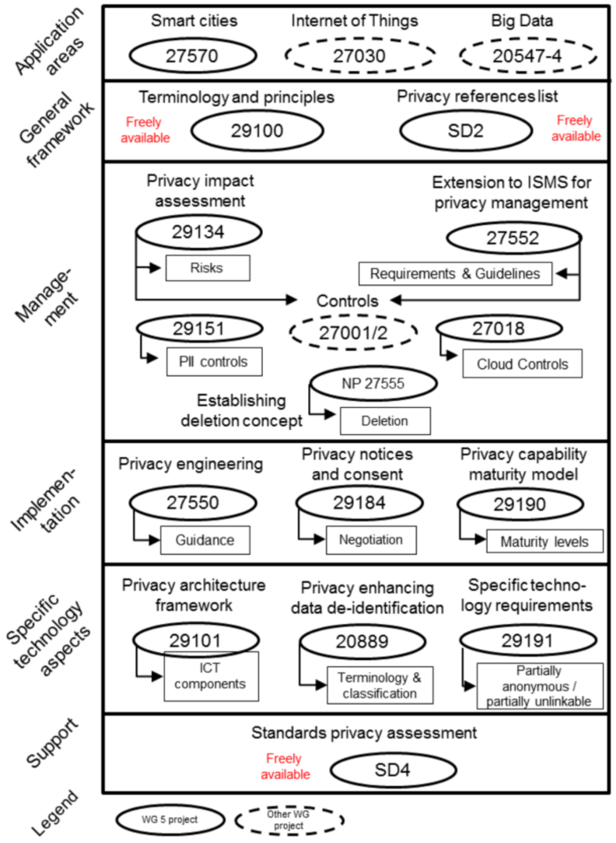
<table>
<tr><th colspan="2">Stakeholder</th><th>Legal Compliance Concern</th><th>Management Concern</th><th>System Lifecycle Concern</th></tr>
<tr><td rowspan="4">Demand side
↓
Supply side</td><td>Policy maker</td><td colspan="3"><b>Compliance Check / Follow standards
Transparency</b></td></tr>
<tr><td><b>Operator</b>
Data Controller</td><td rowspan="2">Regulation
<b>e.g. GPDR in Europe, Privacy act in Japan</b></td><td rowspan="2">Privacy Impact Assessment
<b>PIA</b>
Sharing Agreement</td><td rowspan="2">Privacy-by-Design
<b>PbD</b></td></tr>
<tr><td><b>Operator</b>
Data processor</td></tr>
<tr><td><b>Supplier</b></td><td colspan="3"><b>Operators Requirements</b></td></tr>
</table>

Overview of Standards

Several Viewpoints

SC27/WG5 Privacy Viewpoint

- Standing document
  - https://www.din.de/blob/259644/c1e0abcb551e7926a4452cf10fec53a5/sc27wg5-sd1-data.pdf
- Categories of privacy standards
  - Application area
  - General framework
  - Management
  - Implementation
  - Technology



Application areas

Smart cities 27570 — Internet of Things 27030 — Big Data 20547-4

General framework

Terminology and principles: Freely available 29100 — Privacy references list: SD2 Freely available

Manage-ment

Privacy impact assessment 29134 → Risks

Extension to ISMS for privacy management 27552 → Requirements & Guidelines

Controls

29151 → PII controls — 27001/2 — 27018 → Cloud Controls

Establishing deletion concept: NP 27555 → Deletion

Implemen-tation

Privacy engineering 27550 → Guidance — Privacy notices and consent 29184 → Negotiation — Privacy capability maturity model 29190 → Maturity levels

Specific technology aspects

Privacy architecture framework 29101 → ICT components — Privacy enhancing data de-identification 20889 → Terminology & classification — Specific techno-logy requirements 29191 → Partially anonymous / partially unlinkable

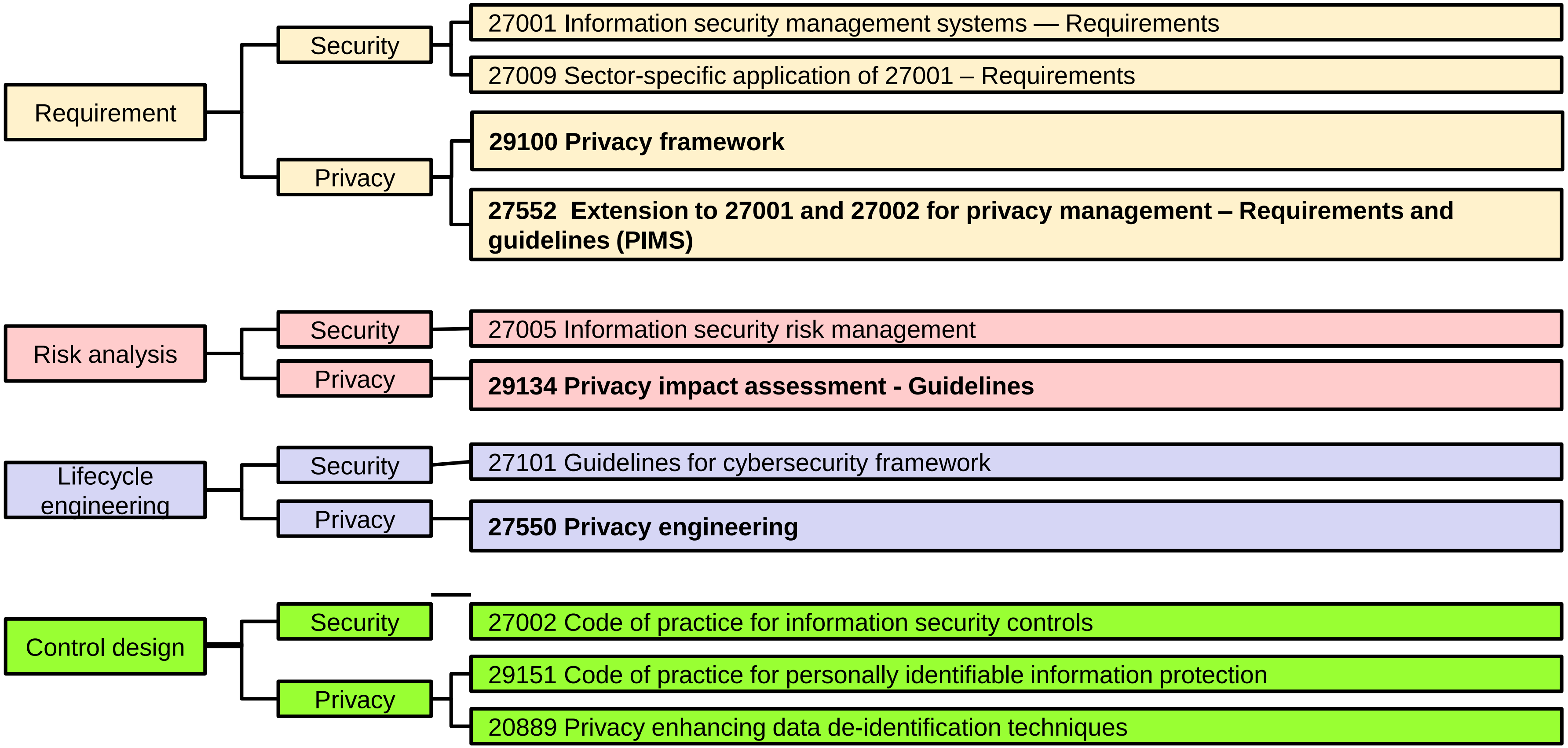
Support

Standards privacy assessment: Freely available SD4

Legend

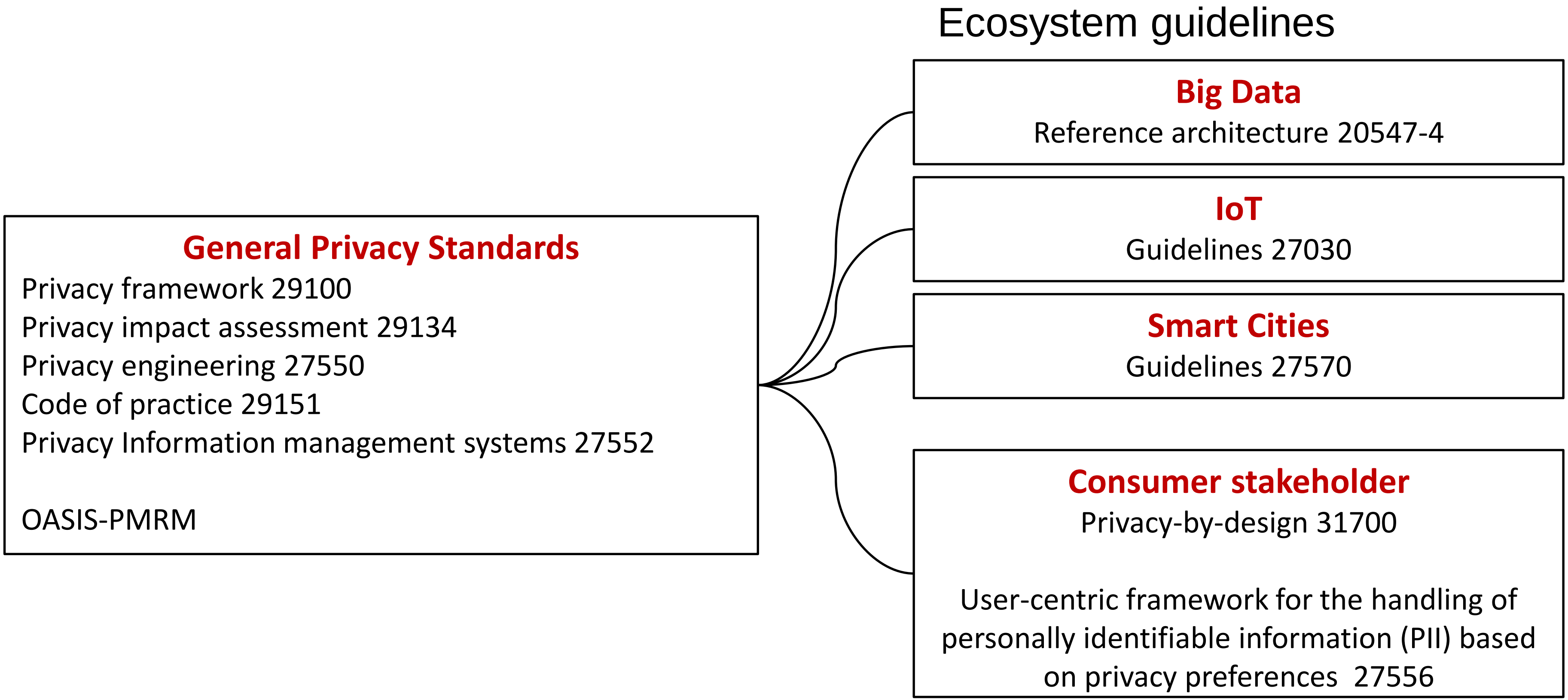
WG 5 project — Other WG project

Security and Privacy Viewpoint



- Requirement
  - Security
    - 27001 Information security management systems — Requirements
    - 27009 Sector-specific application of 27001 – Requirements
  - Privacy
    - **29100 Privacy framework**
    - **27552 Extension to 27001 and 27002 for privacy management – Requirements and guidelines (PIMS)**
- Risk analysis
  - Security
    - 27005 Information security risk management
  - Privacy
    - **29134 Privacy impact assessment - Guidelines**
- Lifecycle engineering
  - Security
    - 27101 Guidelines for cybersecurity framework
  - Privacy
    - **27550 Privacy engineering**
- Control design
  - Security
    - 27002 Code of practice for information security controls
  - Privacy
    - 29151 Code of practice for personally identifiable information protection
    - 20889 Privacy enhancing data de-identification techniques

Ecosystem Viewpoint



Ecosystem guidelines

General Privacy Standards

Privacy framework 29100
Privacy impact assessment 29134
Privacy engineering 27550
Code of practice 29151
Privacy Information management systems 27552

OASIS-PMRM

Big Data

Reference architecture 20547-4

IoT

Guidelines 27030

Smart Cities

Guidelines 27570

Consumer stakeholder

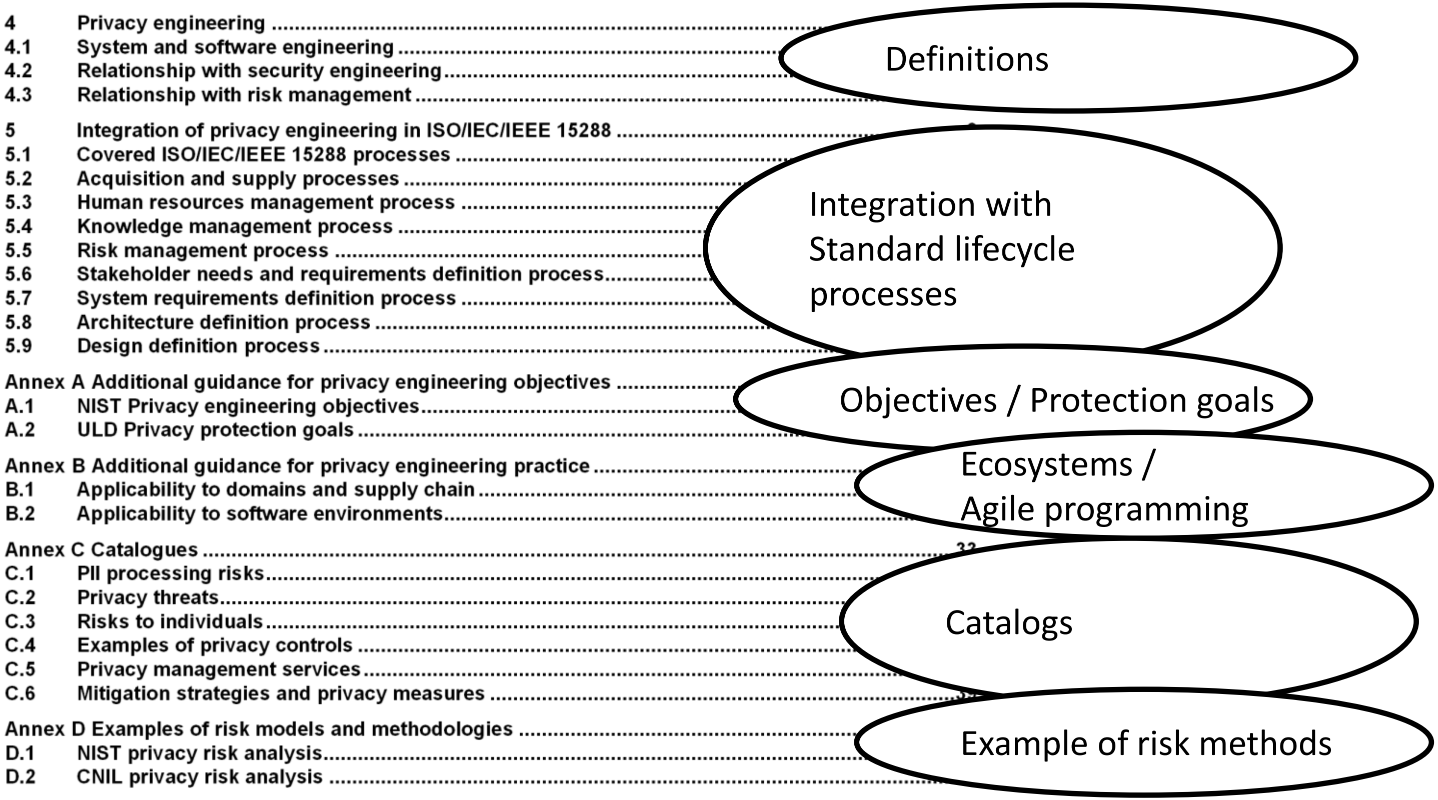
Privacy-by-design 31700

User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences 27556

ISO/IEC 27550

Privacy Engineering for system lifecycle process

Structure



Definitions

Integration with
Standard lifecycle
processes

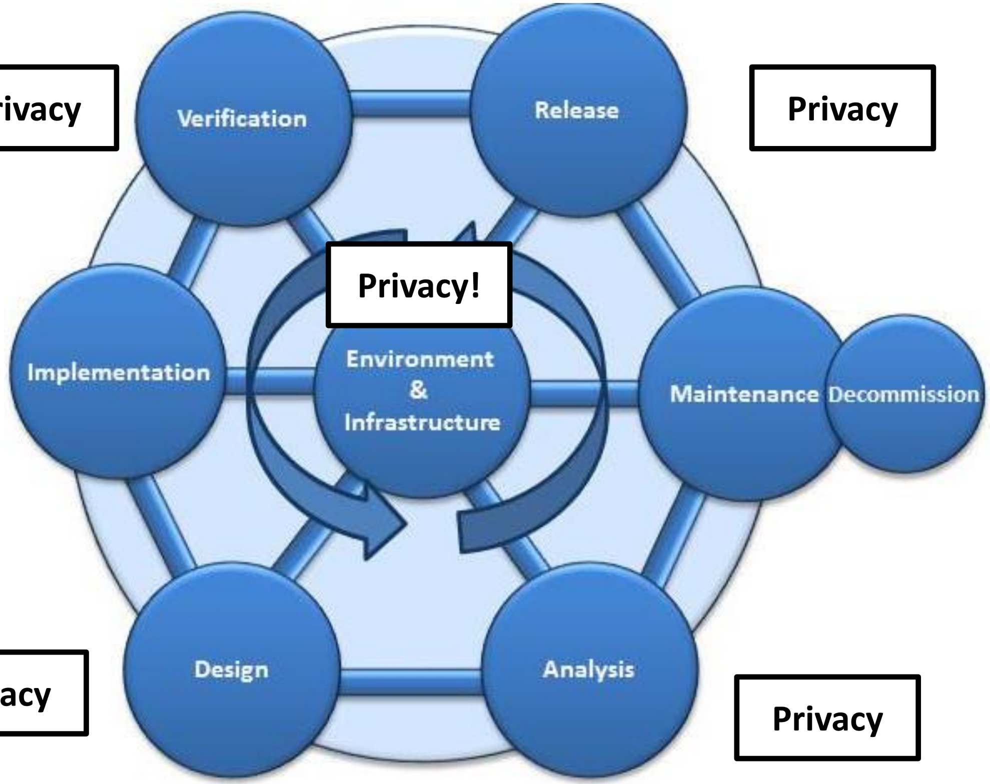
Objectives / Protection goals

Ecosystems /
Agile programming

Catalogs

Example of risk methods

Privacy Engineering: Integrating privacy concerns



Privacy

Privacy

Privacy!

Privacy

Privacy

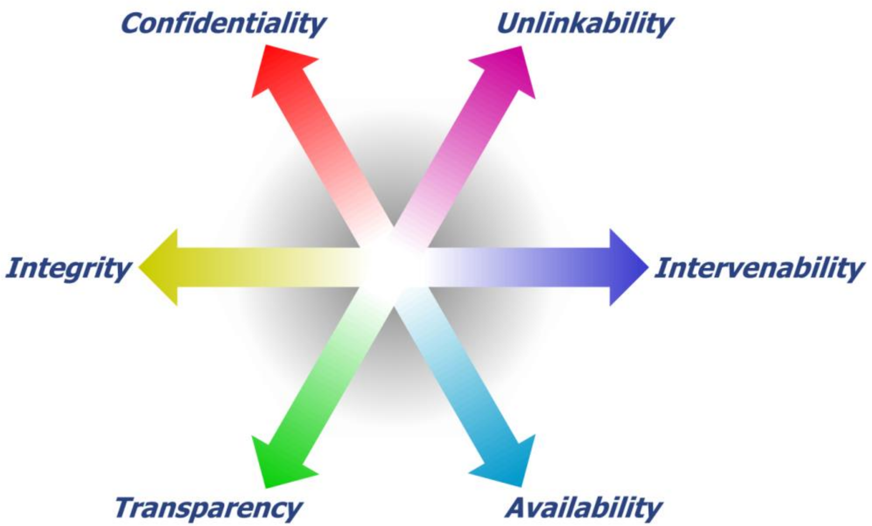
Privacy

Privacy

Beyond CIA

- Confidentiality
- Integrity
- Availability

- Unlinkability
- Intervenability
- Transparency

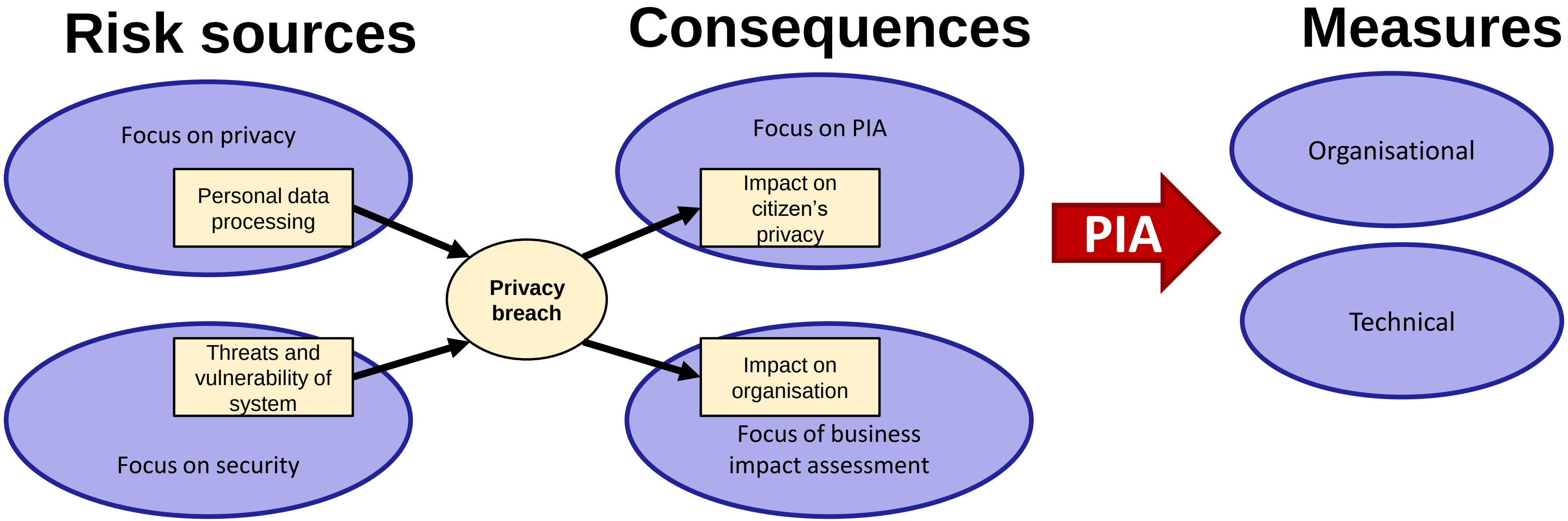


From ULD: ieee-security.org/TC/SPW2015/IWPE/2.pdf

ISO 15288 System Life Cycle Processes

- Agreement
  - Acquisition
  - Supply
- Organisational project-enabling
  - Life cycle model management
  - Infrastructure management
  - Portfolio management
  - Human resource management
  - Quality management
  - Knowledge management
- Technical management
  - Project planning
  - Project assessment and control
  - Decision management
  - Risk management
  - Configuration management
  - Information management
  - Measurement
  - Quality assurance
- Technical
  - Business or mission analysis
  - Stakeholder needs and requirements definition
  - System requirements definition
  - Architecture definition
  - Design definition
  - System analysis
  - Implementation
  - Integration
  - Verification
  - Transition
  - Validation
  - Operation
  - Maintenance
  - Disposal

Privacy Impact Assessment (PIA)

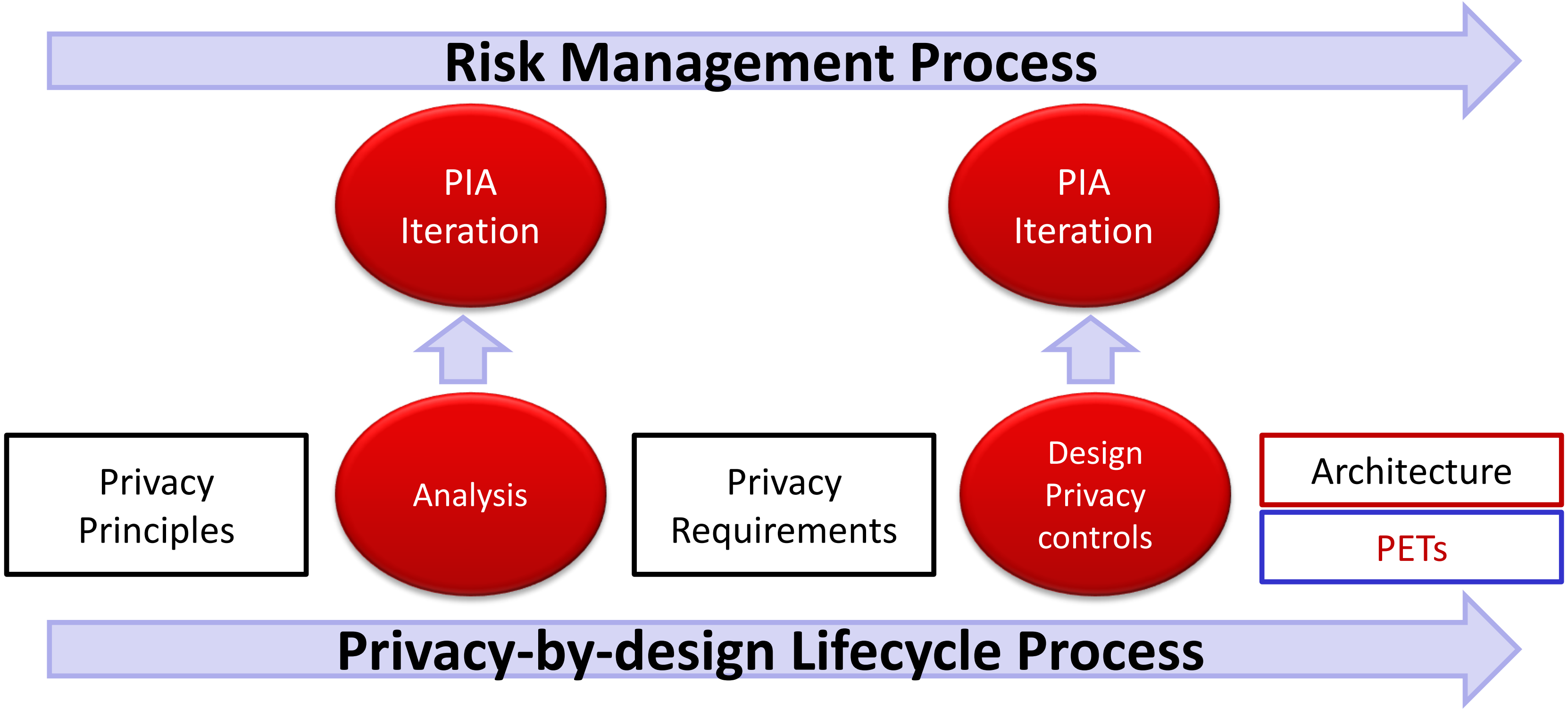


Risk sources

Consequences

Measures

Privacy-by-design



Risk Management Process

PIA Iteration

PIA Iteration

Privacy Principles

Analysis

Privacy Requirements

Design Privacy controls

Architecture

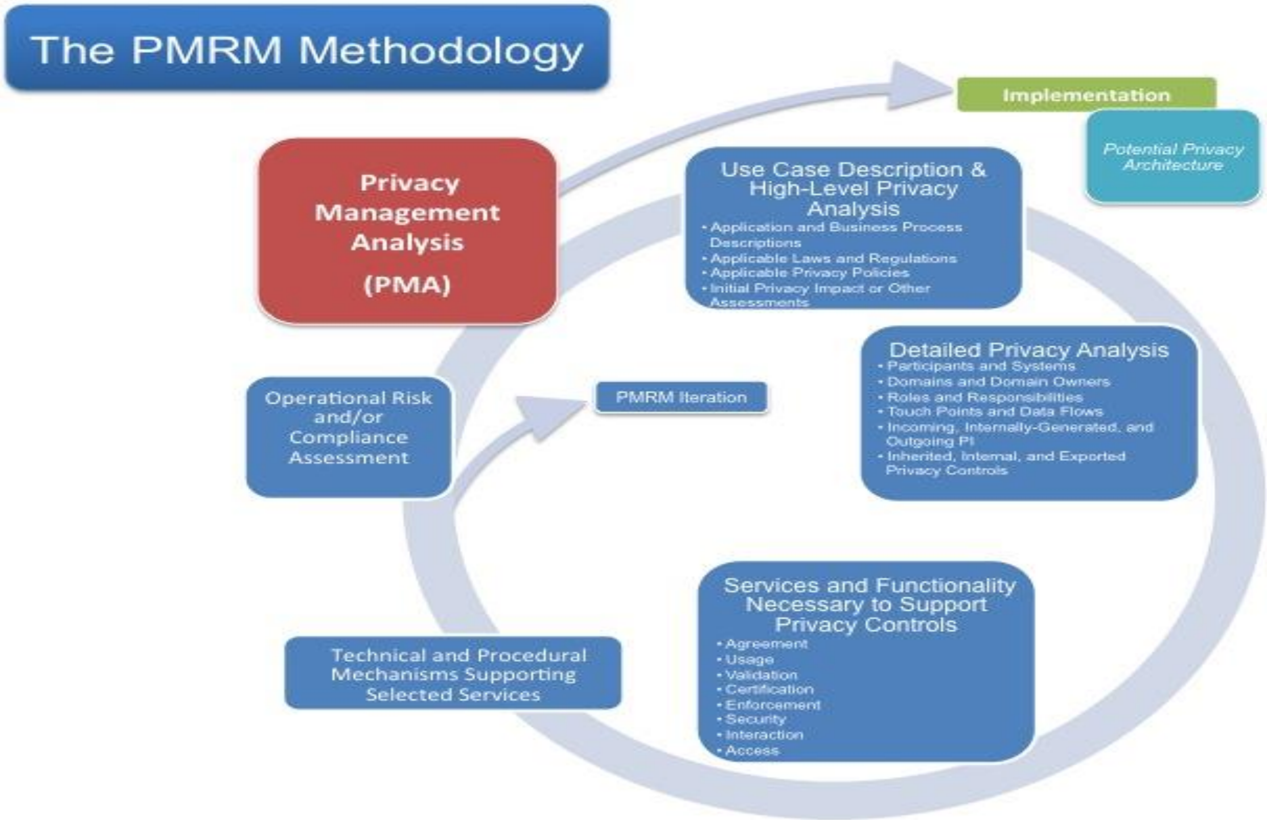
PETs

Privacy-by-design Lifecycle Process

From Principles to Services: OASIS-PMRM

Service		Purpose
Core policy services	Agreement	Manage and negotiate permissions and rules
	Usage	Control PII use
Privacy assurance services	Validation	Ensures PII quality
	Credential certification	Ensure appropriate management of credentials
	Enforcement	Monitor proper operation, respond to exception conditions and report on demand evidence of compliance where required for accountability
	Security	Safeguard privacy information and operations
Presentation and lifecycle services	Interaction	Information presentation and communication
	Access	View and propose changes to stored PII

OASIS PMRM Methodology



The PMRM Methodology

Implementation

Potential Privacy Architecture

Privacy Management Analysis (PMA)

Use Case Description & High-Level Privacy Analysis
- Application and Business Process Descriptions
- Applicable Laws and Regulations
- Applicable Privacy Policies
- Initial Privacy Impact or Other Assessments

Detailed Privacy Analysis
- Participants and Systems
- Domains and Domain Owners
- Roles and Responsibilities
- Touch Points and Data Flows
- Incoming, Internally-Generated, and Outgoing PI
- Inherited, Internal, and Exported Privacy Controls

Services and Functionality Necessary to Support Privacy Controls
- Agreement
- Usage
- Validation
- Certification
- Enforcement
- Security
- Interaction
- Access

Technical and Procedural Mechanisms Supporting Selected Services

Operational Risk and/or Compliance Assessment

PMRM Iteration

From security properties to security threats: STRIDE

Property	Description	Threat
Authentication	The identity of users is established (or you’re willing to accept anonymous users).	Spoofing
Integrity	Data and system resources are only changed in appropriate ways by appropriate people.	Tampering
Nonrepudiation	Users can’t perform an action and later deny performing it.	Repudiation
Confidentiality	Data is only available to the people intended to access it.	Information disclosure
Availability	Systems are ready when needed and perform acceptably.	Denial Of Service
Authorization	Users are explicitly allowed or denied access to resources.	Elevation of privilege

From privacy properties to privacy threats: LINDDUN

https://distrinet.cs.kuleuven.be/software/linddun/catalog.php

Type	Property	Description	Threat
Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.	Linkability
	Anonymity	Hiding the link between an identity and an action or a piece of information	Identifiability
	Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict	Non-repudiation
	Undetectability and unobservability	Hiding the user's actvities	Detectability
Security	Confidentiality	Hiding the data content or controlled release of data content	Disclosure of information
Soft Privacy	Content awareness	User's consciousness regarding his own data	Unawareness
	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	Non compliance

Design Strategy (J.H.Hoepman)

https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

Design strategy		Description	Privacy control examples
Data oriented strategies	Minimize	Limit as much as possible the processing of PII	Selection before collection, Anonymization
	Separate	Distribute or isolate personal data as much as possible, to prevent correlation	Logical or physical separation, Peer-to-peer arrangement, Endpoint processing
	Abstract	Limit as much as possible the detail in which personal data is processed, while still being useful	Aggregation over time (used in smart grids), Dynamic location granularity (used in location based services), k-anonymity
	Hide	Prevent PII to become public or known.	Encryption, Mixing, Perturbation (e.g. differential privacy, statistical disclosure control), Unlinking (e.g. through pseudonymisation), Attribute based credentials
Process oriented strategies	Inform	Inform PII principals about the processing of PII	Privacy icons, Layered privacy policies, Data breach notification
	Control	Provide PII principals control about the processing of their PII.	Privacy dashboard, Consent (including withdrawal)
	Enforce	Commit to PII processing in a privacy friendly way, and enforce this	Sticky policies and privacy rights management, Privacy management system, Commitment of resources, Assignment of responsibilities
	Demonstrate	Demonstrate that PII is processed in a privacy friendly way.	Logging and auditing, Privacy impact assessment, Design decisions documentation

List of security measures 1/2)

References

- ISO/IEC 27001 - Information security management systems – Requirements
- ISO/IEC 27002 - Code of practice for information security controls

Category	Sub-categories
Information security policies	□ Management direction.
Organization of information security	□ Internal organisation □ Mobile devices and teleworking
Human resource security	□ Prior to employment □ During employment □ Termination and change of employment
Asset management	□ Responsibility for assets □ Information classification
Access control	□ Business requirements of access control □ User access management □ User responsibilities □ System and application access control □ Media handling
Cryptography	□ Cryptographic controls
Physical and environmental security	□ Secure areas □ Equipment

List of security measures (2/2)

Category	Sub-categories
Operation security	□ Operational procedures and responsibilities □ Protection from malware □ Backup □ Logging and monitoring □ Control of operational software □ Technical vulnerability management □ Information systems audit considerations
Communication security	□ Network security management □ Information transfer
System acquisition, development and maintenance	□ Security requirements of information system □ Security in development and support processes □ Test data
Suppliers relationships	□ Information security in supplier relationships □ Supplier service delivery managment
Information security incident management	□ Management of information security incidents and improvements
Information security aspects of business continuity management	□ Information security continuity □ Redundancies
Compliance	□ Compliance with legal and contractual requirements □ Information security reviews

The Merit of Agreed Structures

ISO 27001 Categories of controls	
Information security policies	Management direction.
Human resource security	During employment
Access control	System and application access control
Cryptography	Cryptographic controls
Operation security	Operational procedures and responsibilities
	Logging and monitoring
	Control of operational software
	Technical vulnerability management
Communication security	Information transfer
System acquisition, development and maintenance	Security in development and support processes
Information security incident management	Management of information security incidents and improvements
Information security aspects of business continuity management	Information security continuity
Compliance	Compliance with legal and contractual requirements
	Information security reviews

The structure of 27002, 29151, 27552 is the same.
Simplifies reading, use
Shows same mindset and same culture

They are associated with 27005 and 27009

List of privacy measures (1/2) Data controller

References

- ISO/IEC 27552 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management - Requirements and guidelines
- ISO/IEC 29151 - Code of practice for personally identifiable information protection

Conditions for collection and processing	Identify and document purpose
	Identify lawful basis
	Determine when and how consent is to be obtained
	Obtain and record consent
	Privacy impact assessment
	Contracts with PII processors
	Records related to processing PII
Rights of PII principals	Determining PII principals rights and enabling exercise
	Determining information for PII principals
	Providing information for PII principals
	Provide mechanism to modify of withdraw consent
	Provide mechanism to object to processing
	Sharing the exercising of PII princ
	Correction or erasure
	Providing copy of PII processed
	Request management
	Automated decision taking
Privacy-by-design and by-default	Limit collection
	Limit processing
	Define and document PII minization and de-identification objectives
	Comply with data minimization and de-identification use
	PII de-identification and deletion
	Temporary files
	Retention
	Disposal
	Collection procedures
	PII transmission controls
PII sharing, transfer and disclosure	Identify basis for PII transfer
	Countries and organisations to which PII might be transferred
	Records of transfer of PII
	Records of PII disclosure to third parties
	Joint controller

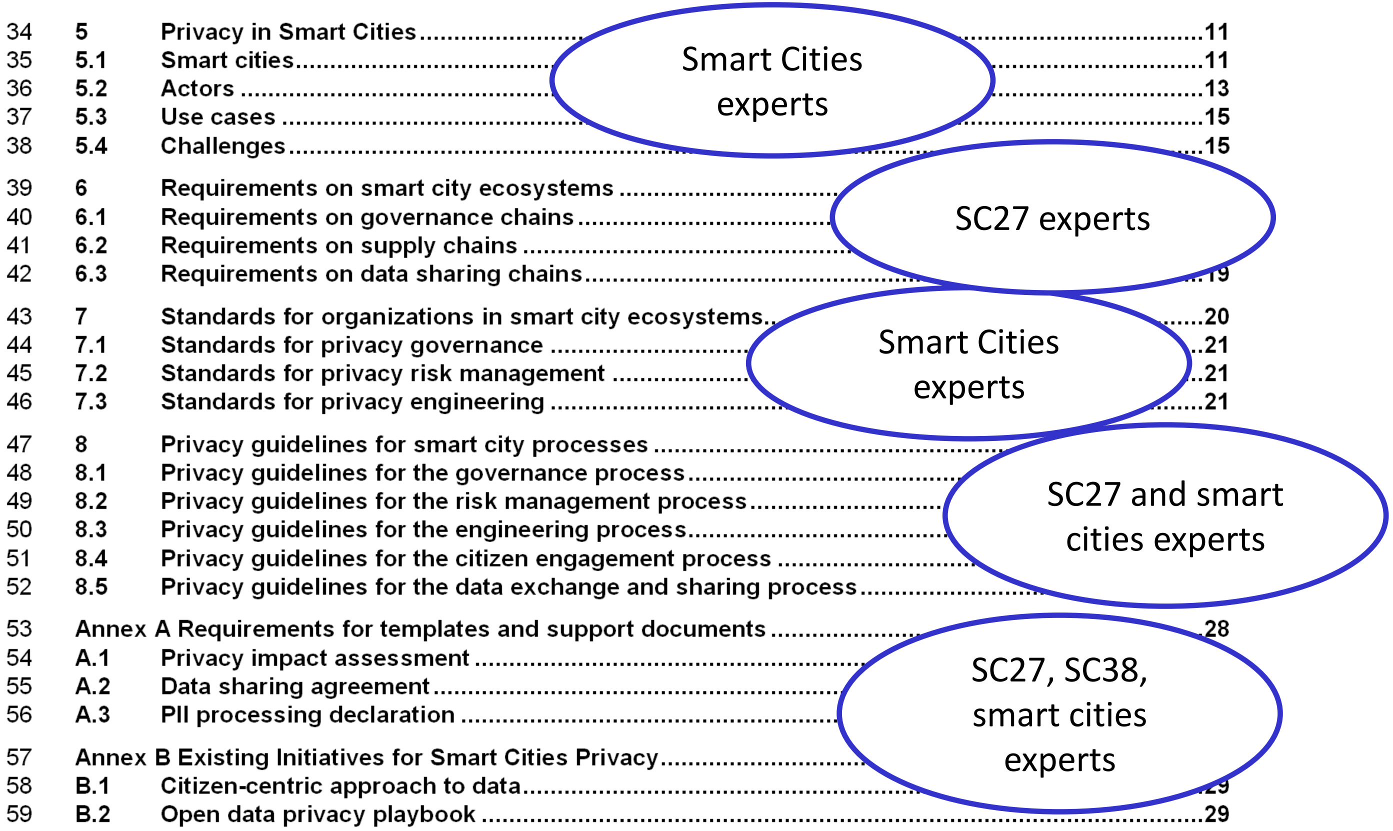
List of privacy measures (2/2) Data processor

Conditions for collection and processing	Cooperation agreement
	Organization’s purposes
	Marketing and advertising use
	Infringing instruction
	PII controller obligations
	Records related to processing PII
Rights of PII principals	Obligations to PII principals
Privacy-by-design and by-default	Temporary files
	Return transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for transfert of PII
	Countries and organisations to which PII might be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

ISO 27570

Privacy guidelines for smart cities

Call for Contribution on 2nd WD (Feb 24th 2019)



Smart Cities experts

SC27 experts

Smart Cities experts

SC27 and smart cities experts

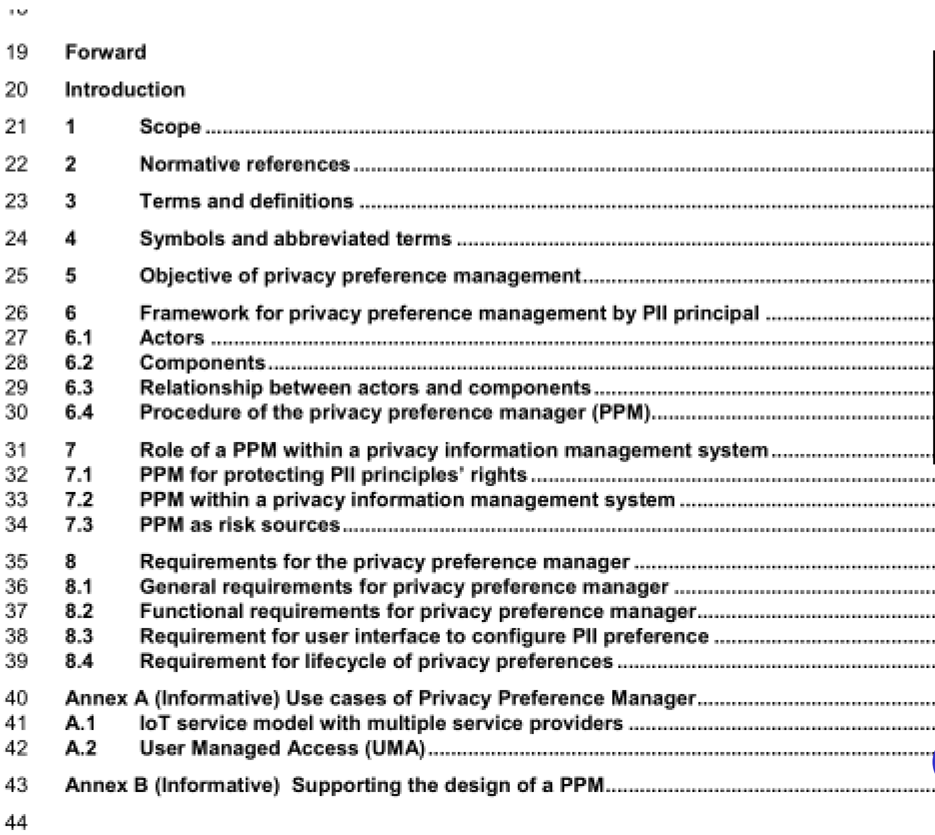
SC27, SC38, smart cities experts

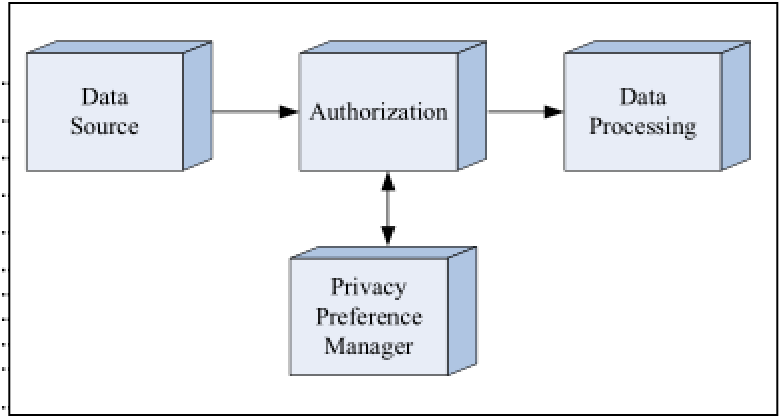
ISO 27556

User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences

a.k.a. Privacy Preference Management (PPM)

ISO/IEC 27556





Relationship with PIMS (27552)

TRiALOG

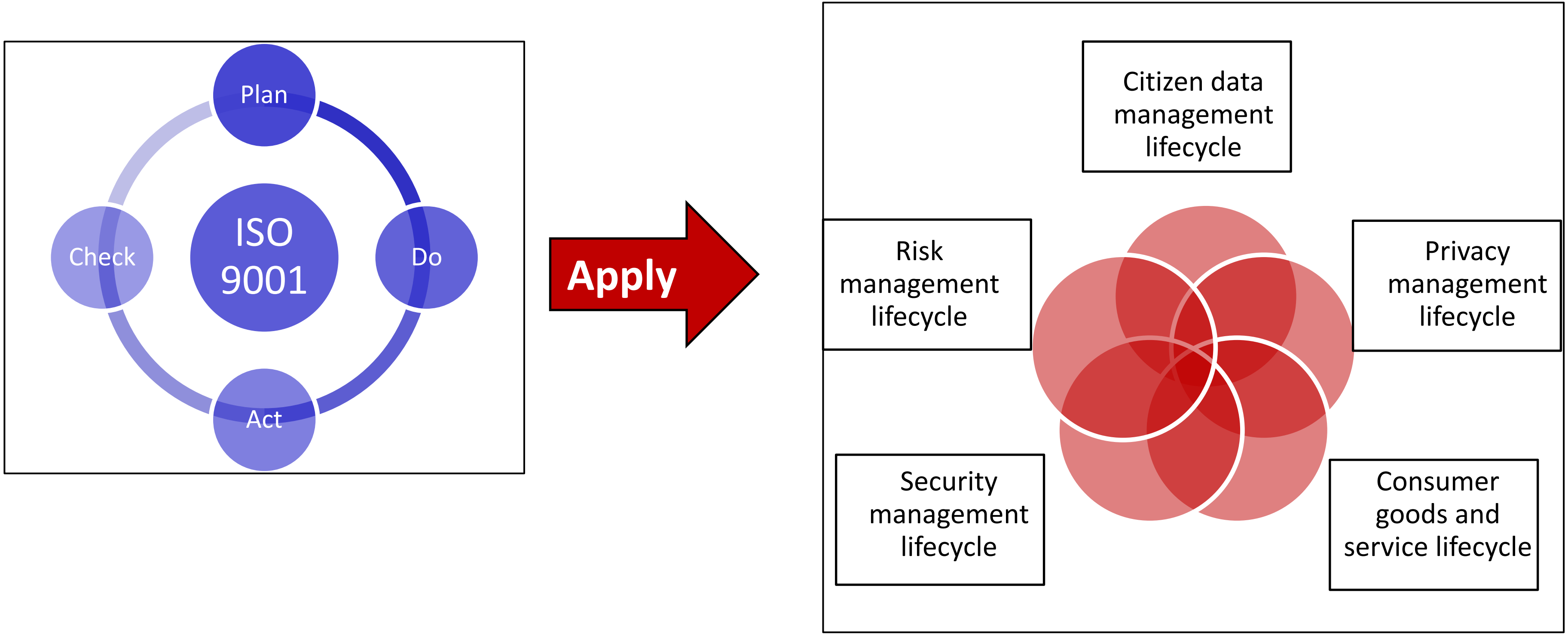
ISO 31700

Privacy-by-design for consumer goods and services

Scope

- Specification of the **design process** to provide consumer goods and services that meet
  - consumers' domestic processing privacy needs as well as
  - the personal privacy requirements of Data Protection.
- In order to **protect consumer privacy** the functional scope includes
  - security in order to prevent unauthorized access to data as fundamental to consumer privacy, and
  - consumer privacy control with respect to access to a person's data and their authorized use for specific purposes.
- The **process is to be based** on
  - the **ISO 9001** continuous quality improvement process and **ISO 10377** product safety by design guidance, as well as
  - incorporating privacy design **JTC1 security and privacy good practices**, in a manner suitable for consumer goods and services.

31700 will be influenced by lifecycles



Plan

Do

Act

Check

ISO 9001

Apply

Citizen data management lifecycle

Risk management lifecycle

Privacy management lifecycle

Security management lifecycle

Consumer goods and service lifecycle

www.trialog.com

Questions?