ADACOR Workshop
19th-21st April, 2016
Luxembourg

Tailoring information security to business requirements

# ISO standards on Privacy

21/04/2016

Dr. Carlo Harpes

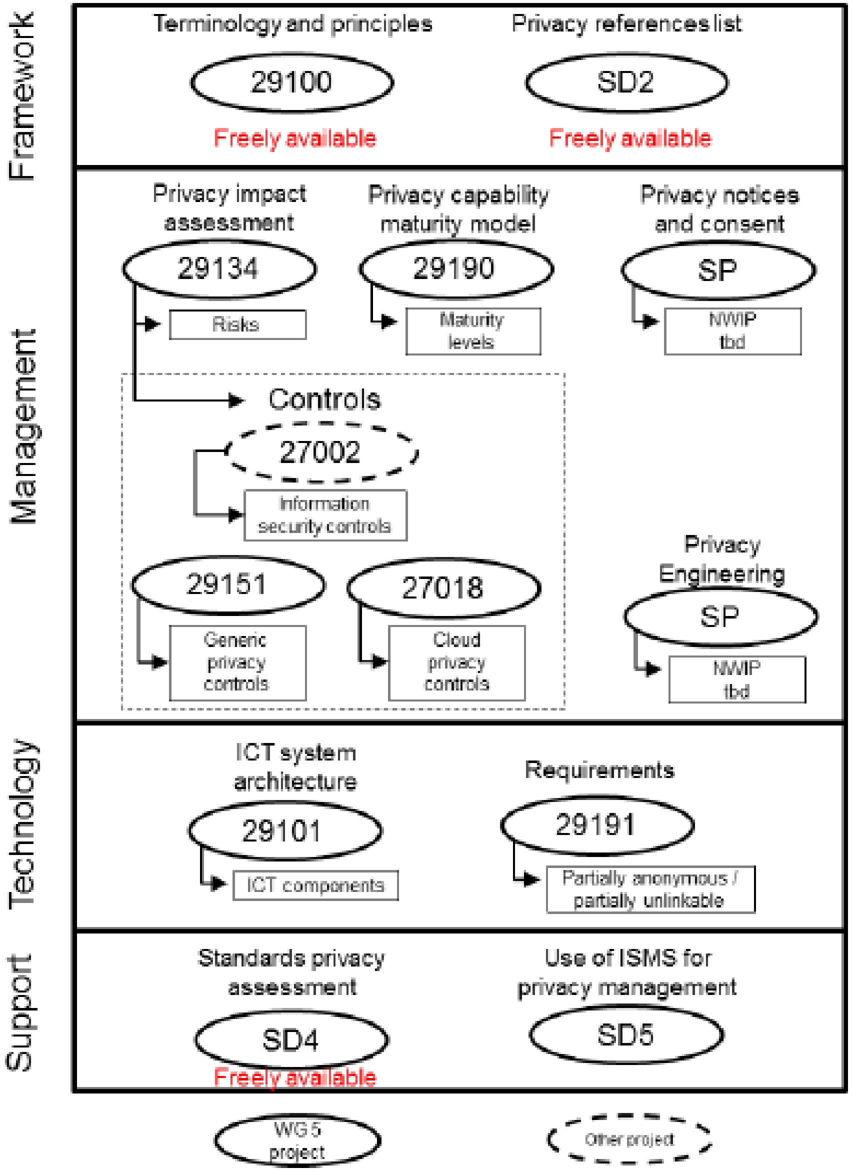
**itrust consulting s.à r.l.**
55, rue Gabriel Lippmann
L-6947 Niederanven

Tel: +352 2617 6212

Web: [www.itrust.lu](http://www.itrust.lu)

# Agenda

1. Current standards
2. 29100 Privacy framework
3. 29101 Privacy Architecture framework
4. Pre-DIS 29151 Code of practice for PII protection
5. Enhancement to ISO/IEC 27001 for privacy management
6. 29134 Privacy Impact Assessment Methodology - Guidelines



Framework

Terminology and principles: 29100 – Freely available

Privacy references list: SD2 – Freely available

Management

Privacy impact assessment: 29134 → Risks

Privacy capability maturity model: 29190 → Maturity levels

Privacy notices and consent: SP → NWIP tbd

Controls: 27002 → Information security controls; 29151 → Generic privacy controls; 27018 → Cloud privacy controls

Privacy Engineering: SP → NWIP tbd

Technology

ICT system architecture: 29101 → ICT components

Requirements: 29191 → Partially anonymous / partially unlinkable

Support

Standards privacy assessment: SD4 – Freely available

Use of ISMS for privacy management: SD5

WG 5 project

Other project

# 1. Current standards (Search “Privacy”)

ISO 22307:2008

Financial services -- Privacy impact assessment

ISO/IEC 29100:2011

Information technology -- Security techniques -- Privacy framework

ISO/IEC 29101:2013

Information technology -- Security techniques -- Privacy architecture framework

ISO/IEC 29176:2011

Information technology -- Mobile item identification and management -- Consumer privacy-protection protocol for Mobile RFID services

ISO/IEC 29187-1:2013

Information technology -- Identification of privacy protection requirements pertaining to learning, education and training (LET) -- Part 1: Framework and reference model

ISO/IEC 15944-8:2012

Information technology -- Business Operational View -- Part 8: Identification of privacy protection requirements as external constraints on business transactions

ISO/TR 12859:2009

Intelligent transport systems -- System architecture -- Privacy aspects in ITS standards and systems

# 1. Current standards (Search "Privacy")

| | |
|---|---|
| ISO/TS 14441:2013 | Health informatics -- Security and privacy requirements of EHR systems for use in conformity assessment |
| ISO/IEC 29190:2015 | Information technology -- Security techniques -- Privacy capability assessment model |
| ISO/TR 17427-7:2015 | Intelligent transport systems -- Cooperative ITS -- Part 7: Privacy aspects |
| ISO/TS 14904:2002 | Road transport and traffic telematics -- Electronic fee collection (EFC) -- Interface specification for clearing between operators |
| ISO/TS 25237:2008 | Health informatics -- Pseudonymization |
| ISO/TS 27790:2009 | Health informatics -- Document registry framework |
| ISO/TS 21547:2010 | Health informatics -- Security requirements for archiving of electronic health records -- Principles |
| ISO/IEC TR 24763:2011 | Information technology -- Learning, education and training -- Conceptual Reference Model for Competency Information and Related Objects |
| ISO/IEC 18013-3:2009 | Information technology -- Personal identification -- ISO-compliant driving licence -- Part 3: Access control, authentication and integrity validation |
| ISO/IEC 19784-4:2011 | Information technology -- Biometric application programming interface -- Part 4: Biometric sensor function provider interface |
| ISO/IEC 19794-14:2013 | Information technology -- Biometric data interchange formats -- Part 14: DNA data |
| ISO/IEC TR 24729-4:2009 | Information technology -- Radio frequency identification for item management -- Implementation guidelines -- Part 4: Tag data security |
| ISO/TR 12296:2012 | Ergonomics -- Manual handling of people in the healthcare sector |

# 1. Current standards (Search “Privacy”)

| | |
|---|---|
| ISO 24534-1:2010 | Automatic vehicle and equipment identification -- Electronic registration identification (ERI) for vehicles -- Part 1: Architecture |
| ISO 24534-2:2010 | Automatic vehicle and equipment identification -- Electronic registration identification (ERI) for vehicles -- Part 2: Operational requirements |
| ISO 24534-4:2010 | Automatic vehicle and equipment identification -- Electronic registration identification (ERI) for vehicles -- Part 4: Secure communications using asymmetrical techniques |
| ISO/IEC 29341-13-10:2008 | Information technology -- UPnP Device Architecture -- Part 13-10: Device Security Device Control Protocol - Device Security Service |
| ISO/IEC TS 29140-2:2011 | Information technology for learning, education and training -- Nomadicity and mobile technologies -- Part 2: Learner information model for mobile learning |
| ISO/IEC 24745:2011 | Information technology -- Security techniques -- Biometric information protection |
| ISO 9564-1:2011 | Financial services -- Personal Identification Number (PIN) management and security -- Part 1: Basic principles and requirements for PINs in card-based systems |
| ISO 24534-5:2011 | Intelligent transport systems -- Automatic vehicle and equipment identification -- Electronic Registration Identification (ERI) for vehicles -- Part 5: Secure communications using symmetrical techniques |
| ISO/IEC 15944-1:2011 | Information technology -- Business Operational View -- Part 1: Operational aspects of Open-edi for implementation |

# 1. Current standards (Search “Privacy”)

itrust consulting

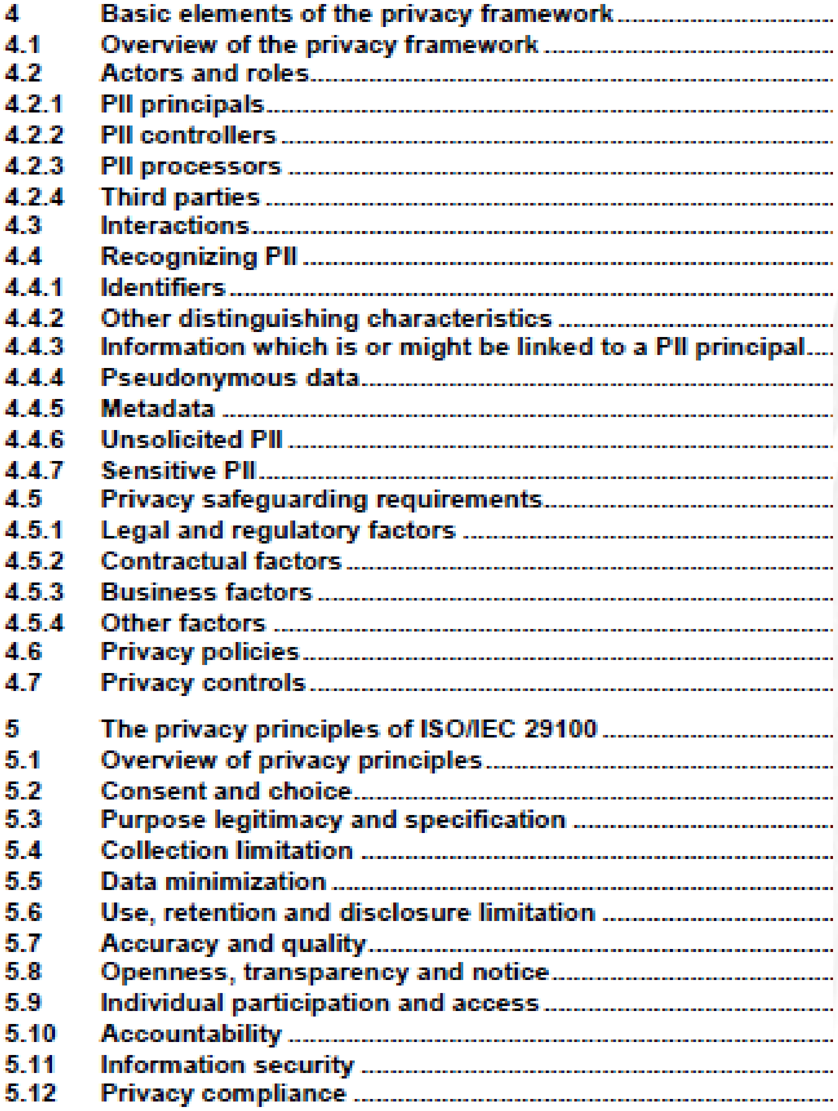
| | |
|---|---|
| ISO 16175-1:2010 | Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles |
| ISO/IEC 15944-10:2013 | Information technology -- Business Operational View -- Part 10: IT-enabled coded domains as semantic components in business transactions |
| ISO/TS 17427:2014 | Intelligent transport systems -- Cooperative systems -- Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems |
| ISO/IEC 27018:2014 | Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors |
| ISO/TS 28560-4:2014 | Information and documentation -- RFID in libraries -- Part 4: Encoding of data elements based on rules from ISO/IEC 15962 in an RFID tag with partitioned memory |
| ISO 28560-1:2014 | Information and documentation -- RFID in libraries -- Part 1: Data elements and general guidelines for implementation |
| ISO 13185-2:2015 | Intelligent transport systems -- Vehicle interface for provisioning and support of ITS services -- Part 2: Unified gateway protocol (UGP) requirements and specification for vehicle ITS station gateway (V-ITS-SG) interface |
| ISO/IEC TS 20013:2015 | Information technology for learning, education and training -- A reference framework of e-Portfolio information |
| ISO/IEC 19785-1:2015 | Information technology -- Common Biometric Exchange Formats Framework -- Part 1: Data element specification |

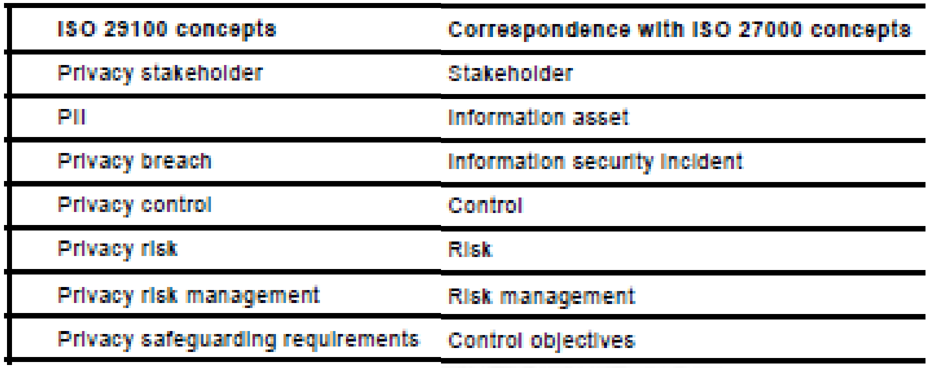
# 1. Current standards (Search “Privacy”)

| | |
|---|---|
| ISO/TS 17975:2015 | Health informatics -- Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information |
| ISO/TS 19299:2015 | Electronic fee collection -- Security framework |
| ISO/IEC TR 18121:2015 | Information technology -- Learning, education and training -- Virtual experiment framework |
| ISO/TS 13582:2015 | Health informatics -- Sharing of OID registry information |
| ISO 9564-4:2016 | Financial services -- Personal Identification Number (PIN) management and security -- Part 4: Requirements for PIN handling in eCommerce for Payment Transactions |
| ISO/IEC 11889-1:2015 | Information technology -- Trusted platform module library -- Part 1: Architecture |
| ISO 24534-3:2016 | Intelligent transport systems -- Automatic vehicle and equipment identification -- Electronic registration |

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## ToC





| ISO 29100 concepts | Correspondence with ISO 27000 concepts |
|---|---|
| Privacy stakeholder | Stakeholder |
| PII | Information asset |
| Privacy breach | Information security incident |
| Privacy control | Control |
| Privacy risk | Risk |
| Privacy risk management | Risk management |
| Privacy safeguarding requirements | Control objectives |

Free of charge !!!

## Terms

**anonymity**

characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly

**anonymization**

process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

**anonymized data**

data that has been produced as the output of a personally identifiable information anonymization process

**consent**

personally identifiable information (PII) principal’s freely given, specific and informed agreement to the processing of his or her PII

**identifiability**

condition which results in a personally identifiable information (PII) principal being identified, directly or indirectly, on the basis of a given set of PII

**identify**

establish the link between a personally identifiable information (PII) principal and PII or a set of PII

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## Terms

**identity**

set of attributes which make it possible to identify the personally identifiable information principal

**opt-in**

process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose

NOTE A different term that is often used with the privacy principle ‘consent and choice’ is “opt-out”. It describes a process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent, or oppose a specific type of processing. The use of an opt-out policy presumes that the PII controller has the right to process the PII in the intended way. This right can be implied by some action of the PII controller different from consent (e.g., an order in an online shop).

**personally identifiable information PII**

any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

NOTE To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## Terms

**PII controller**

privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

NOTE A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

**PII principal**

natural person to whom the personally identifiable information (PII) relates

NOTE Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.

**PII processor**

privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

**privacy breach**

situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements

**privacy controls**

measures that treat privacy risks by reducing their likelihood or their consequences

NOTE 1 Privacy controls include organizational, physical and technical measures, e.g., policies, procedures, guidelines, legal contracts, management practices or organizational structures.

NOTE 2 Control is also used as a synonym for safeguard or countermeasure.

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## Terms

**privacy enhancing technology PET**

privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system

NOTE 1 Examples of PETs include, but are not limited to, anonymization and pseudonymization tools that eliminate, reduce, mask, or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII.

NOTE 2 Masking is the process of obscuring elements of PII.

**privacy policy**

overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting

**privacy preferences**

specific choices made by a personally identifiable information (PII) principal about how his or her PII should be processed for a particular purpose

**privacy principles**

set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## Terms

**privacy risk**

effect of uncertainty on privacy

NOTE 1 Risk is defined as the “effect of uncertainty on objectives” in ISO Guide 73 and ISO 31000.

NOTE 2 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

**privacy risk assessment**

overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII)

NOTE This process is also known as a privacy impact assessment.

**privacy safeguarding requirements**

set of requirements an organization has to take into account when processing personally identifiable information (PII) with respect to the privacy protection of PII

**privacy stakeholder**

natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing

**processing of PII**

operation or set of operations performed upon personally identifiable information (PII)

NOTE Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## Terms

**pseudonymization**

process applied to personally identifiable information (PII) which replaces identifying information with an alias

NOTE 1 Pseudonymization can be performed either by PII principals themselves or by PII controllers, … can be used by PII principals to consistently use a resource or service without disclosing their identity to this resource or service (or between services), while still being held accountable for that use.

NOTE 2 Pseudonymization does not rule out the possibility that there might be (a restricted set of) privacy stakeholders other than the PII controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it.

**secondary use**

processing of personally identifiable information (PII) in conditions which differ from the initial ones NOTE Conditions that differ from the initial ones could involve, for example, a new purpose for processing PII, a new recipient of the PII, etc.

**sensitive PII**

category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the

**PII principal**

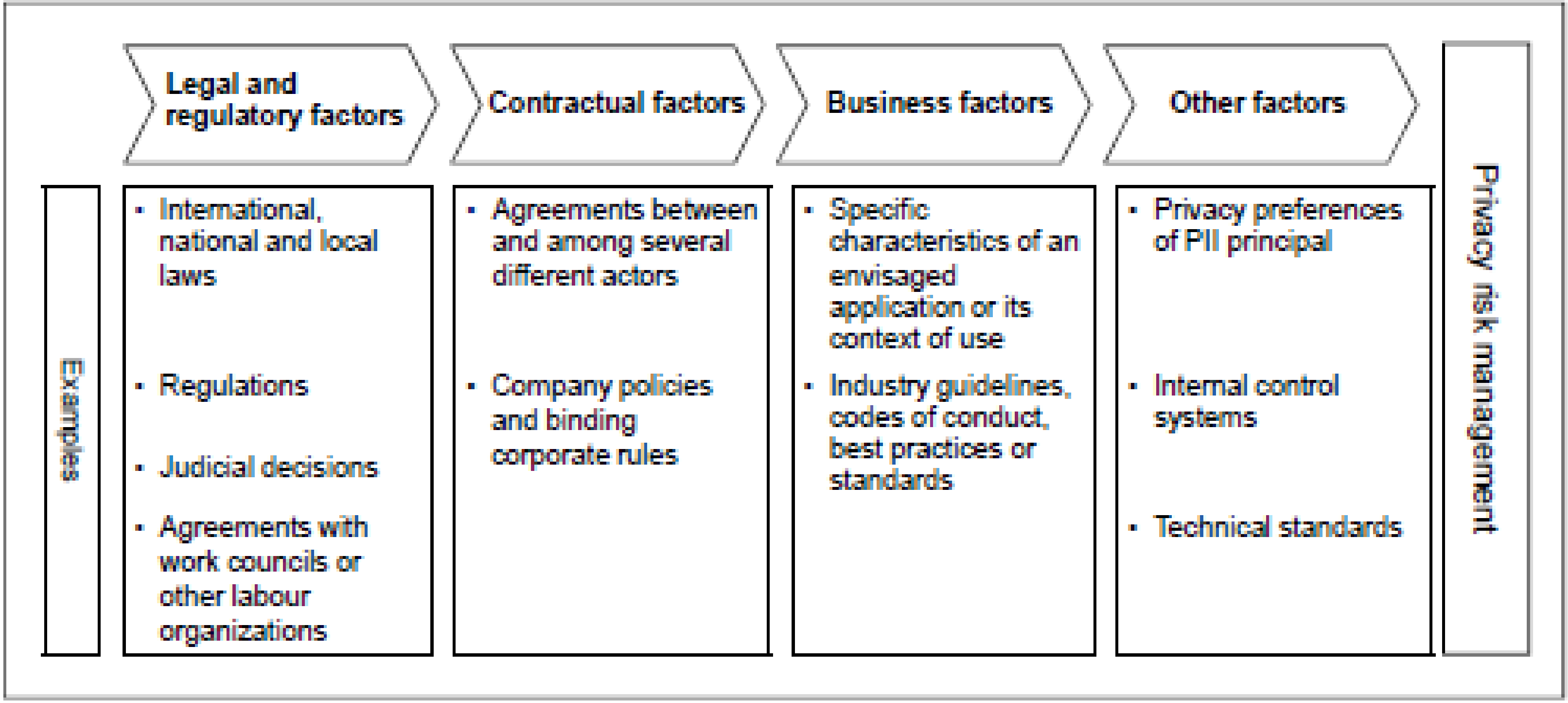
NOTE In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.

**third party** privacy stakeholder other than the PII principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## Privacy risks

### Factors influencing privacy risk management



| | Legal and regulatory factors | Contractual factors | Business factors | Other factors |
|---|---|---|---|---|
| Examples | - International, national and local laws<br>- Regulations<br>- Judicial decisions<br>- Agreements with work councils or other labour organizations | - Agreements between and among several different actors<br>- Company policies and binding corporate rules | - Specific characteristics of an envisaged application or its context of use<br>- Industry guidelines, codes of conduct, best practices or standards | - Privacy preferences of PII principal<br>- Internal control systems<br>- Technical standards |

Privacy risk management

# ISO/IEC 29100:2011 Security techniques — Privacy framework

## Privacy Principles

1. **Consent and choice**
2. **Purpose legitimacy and specification**
3. **Collection limitation**
4. **Data minimization**
5. **Use, retention and disclosure limitation**
6. **Accuracy and quality**
7. **Openness, transparency and notice**
8. **Individual participation and access**
9. **Accountability**
10. **Information security**
11. **Privacy compliance**

# ISO/IEC 29100:2011 Security techniques — Privacy framework

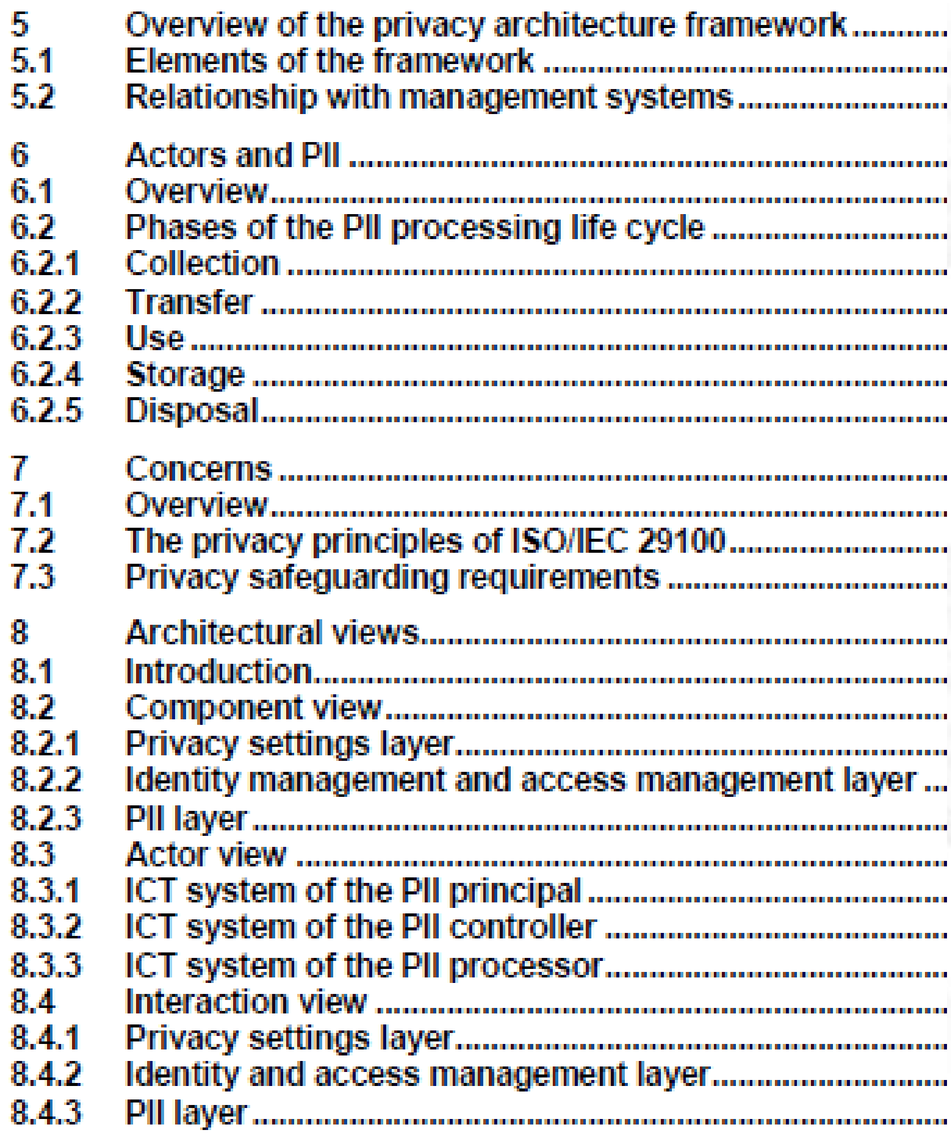
## Privacy Principles

### Information security

- protecting PII under its authority with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle;
- choosing PII processors that provide sufficient guarantees with regard to organizational, physical and technical controls for the processing of PII and ensuring compliance with these controls;
- basing these controls on applicable legal requirements, security standards, the results of systematic security risk assessments as described in ISO 31000, and the results of a cost/benefit analysis;
- implementing controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held;
- limiting access to PII to those individuals who require such access to perform their duties, and limit the access those individuals have to only that PII which they require access to in order to perform their duties;
- resolving risks and vulnerabilities that are discovered through privacy risk assessments and audit processes; and
- subjecting the controls to periodic review and reassessment in an ongoing security risk management process.

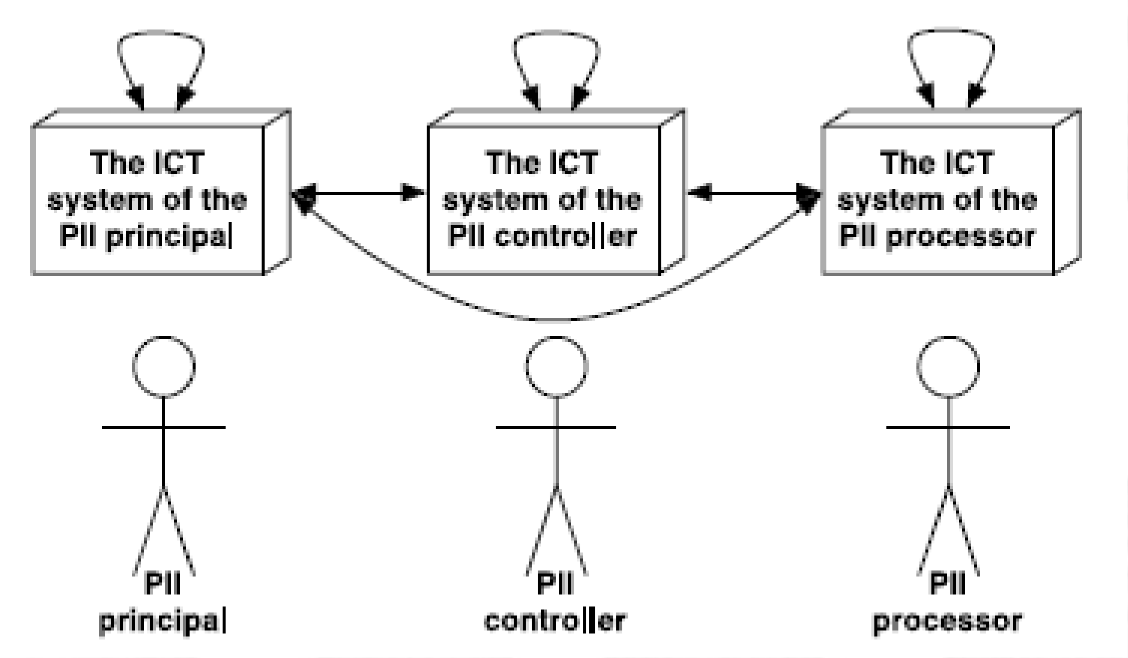
# ISO/IEC 29101:2013 — Privacy Architecture framework

## ToC



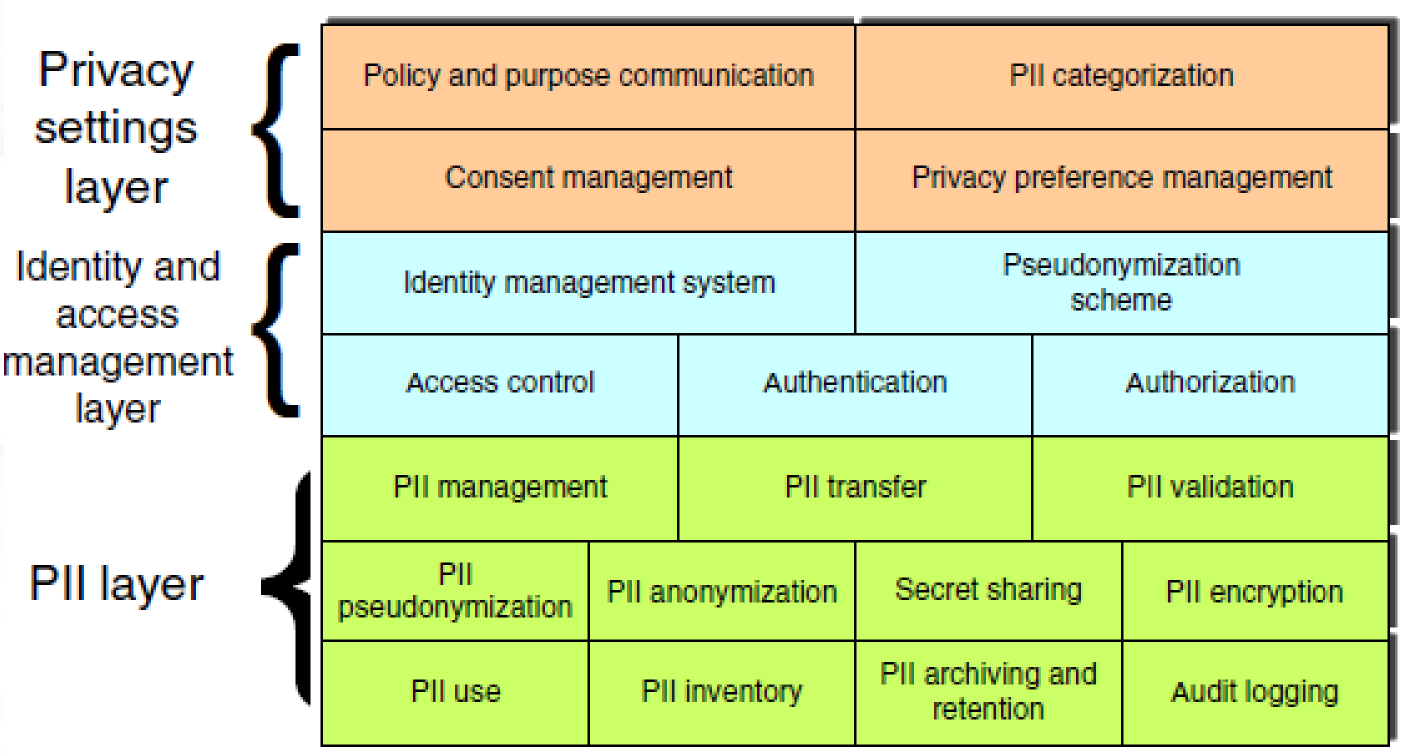
# ISO/IEC 29101:2013 — Privacy Architecture framework

## Actors


The ICT system of the PII principal
The ICT system of the PII controller
The ICT system of the PII processor
PII principal
PII controller
PII processor

# ISO/IEC 29101:2013 — Privacy Architecture framework

## The architecture of the ICT system of the PII principal



Privacy settings layer

- Policy and purpose communication | PII categorization
- Consent management | Privacy preference management

Identity and access management layer

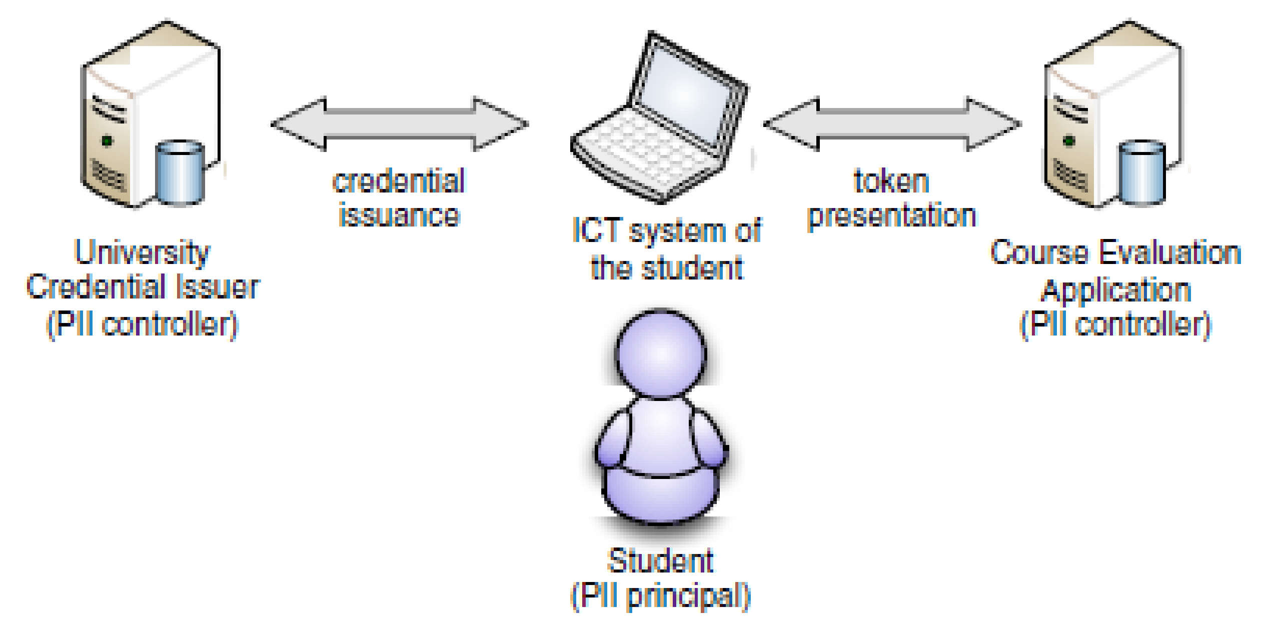
- Identity management system | Pseudonymization scheme
- Access control | Authentication | Authorization

PII layer

- PII management | PII transfer | PII validation
- PII pseudonymization | PII anonymization | Secret sharing | PII encryption
- PII use | PII inventory | PII archiving and retention | Audit logging

# ISO/IEC 29101:2013 — Privacy Architecture framework

## A privacy-friendly, pseudonymous system for identity and access control management


credential issuance
University Credential Issuer (PII controller)
ICT system of the student
token presentation
Course Evaluation Application (PII controller)
Student (PII principal)

# Pre-DIS 29151 Code of practice for PII protection

## Scope and Normative references

### Scope

- establishes control objectives, controls and guidelines for 4 implementing controls, to meet the requirements identified by a risk and impact assessment related to the 5 protection of Personally Identifiable Information (PII).
- applicable to all types and sizes of organizations acting as 10 PII controllers

### Normative references

1. 27000 ISMS - Overview
2. 27002 Code of practice for information security controls
3. 29100 Privacy framework

### Terms

1. **chief privacy officer**
   senior management individual who is in charge of the protection of PII in an organization
2. **de-identification**
   technique for manipulation of data semantics with the goal of obscuring the identities of data subjects

# Additional objectives and controls

## A.1 General policies for the use and protection of PII

To provide management direction and support for PII protection in accordance with business requirements and relevant laws and regulations.

Organizations involved in the processing of PII should establish a policy for the use and protection of PII.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.2 Consent and choice

### A.2.1 Consent

Objective: To make PII principals active participants in the decision-making process regarding the processing of their PII, except as otherwise limited by legislation and regulation, through the exercise of meaningful, informed and freely given consent.

Organizations should provide the means necessary for PII principals to exercise meaningful, informed, unambiguous, and freely given consent except where the PII principal cannot freely refuse consent or where applicable law specifically allows the processing of PII without the principal's consent.

### A.2.2 Choice

Objective: To present to PII principals, where appropriate and feasible, the choice not to allow the processing of their PII, refuse or withdraw consent, or oppose a specific type of processing, and explain to PII principal the implications of granting or refusing consent.

Organizations should provide PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice with respect to the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the PII principal's consent.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.3 Purpose legitimacy and specification

### A.3.1 Purpose legitimacy

Objective: To ensure that the purpose(s) for processing of PII complies with applicable laws and relies on a permissible legal ground.

Organizations should implement appropriate measures to ensure that t PII processing complies with applicable law and relies on a permissible legal ground.

### A.3.2 Purpose specification

Objective: To specify the purposes for which PII are collected not later than at the time of PII collection and limit the subsequent use to the fulfilment of original purposes.

Organizations should communicate to the PII principal from whom they are going to collect PII, the purpose(s) for which that PII is being collected and the purpose(s) for which the PII will be processed. Such communication should take place at or before the PII is collected and before the PII is processed for any purpose(s) not previously communicated to the PII principal.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.4 Collection limitation

#### A.4.1 Collection limitation

Objective: To limit the collection of PII to that which is within the boundaries of applicable law and strictly necessary for the specified purpose(s).

Organizations should implement appropriate measures to limit the collection of the type and amount of PII to the minimum elements for the purposes described in the notice (See A.8.1) and to that which is within the bounds of applicable laws and regulations.

### A.5 Data minimization

#### A.5.1 Minimization

Objective: To minimize the PII which is processed to what is strictly necessary for the legitimate interests pursued by the PII controller and to limit the disclosure of PII to a minimum number of privacy stakeholders.

Organizations should implement appropriate measures to minimize the amount of PII being processed to that which is strictly necessary for the legitimate interests of the PII controller (e.g., an organization may seek to increase or extend its business operations in a manner which legitimately increases the amount of PII it processes and stores).

# Additional objectives and controls

## A.6 Use, retention and disclosure limitation

Objective: To limit the use and disclosure of PII for specific, explicit and legitimate purposes and retain PII no longer than necessary to fulfil the stated purposes or to abide with applicable laws.

Organizations should implement appropriate measures to limit the processing of PII for legitimate and intended purposes and to retain PII only as long as necessary to fulfil the stated purposes or to abide with applicable laws.

### A.6.2 Secure erasure of temporary files

To provide technical measures for temporary files to be deleted within the specific period.

Temporary files and documents that may contain PII should be disposed of within a specified, documented period.

### A.6.3 PII disclosure notification

To ensure the PII processor notifies the PII controller of any legally binding request for disclosure of PII.

The contract between the PII controller and the PII processor should require the PI processor to notify the PII controller, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by law enforcement or other authority, unless such a disclosure is otherwise prohibited by law.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.6 Use, retention and disclosure limitation

…

### A.6.4 Recording of PII disclosures

Objective: To ensure that disclosures of PII to third parties are recorded.

Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom, at what time and for what purpose.

### A.6.5 Disclosure of sub-contracted PII processing

Objective: To ensure that PII processors disclose any use of sub-contractors to PII controller.

The use of sub-contractors by the PII processor to process PII should be disclosed to the PII controller prior to any such use.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.7 Accuracy and quality

#### A.7.1 Data quality

Objective: To ensure that the PII processed is accurate, complete, up-to-date, adequate and relevant for the purpose of use.

Organizations should implement appropriate measures to ensure that PII collected from a PII principal, either directly or indirectly, is of appropriate quality. 3

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.8 Openness, transparency and notice

### A.8.1 Privacy notice

Objective: To ensure that privacy notices contain the appropriate level of details, are written in plain language, and are easily accessible.

Organizations should implement appropriate measures to provide PII principals with appropriate notice of the purposes of the PII processing.

### A.8.2 Openness and transparency

Objective: To provide PII principals with clear and easily accessible information about the PII controller’s policies, procedures and practices with respect to the handling of PII.

Organizations should implement appropriate measures to provide PII principals with appropriate information about their PII processing policies, procedures and practices with respect to the handling of PII.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.9 PII principal participation and access

### A.9.1 PII principal access

Objective: To give PII principals the ability to access and review their PII and to challenge its accuracy and completeness.

Appropriate measures should be implemented by organizations to provide PII principals with the ability to have access to their PII, and to obtain rectification of the PII and/or deletion of the PII.

### A.9.2 Redress and participation

Objective: To provide any amendment, correction or removal to PII processors and third parties to whom personal data had been disclosed

Unless prohibited by relevant legislation or regulation, organizations should implement appropriate measures to provide PII principals with the ability to correct, amend or delete PII maintained by organizations. Organization should also establish a mechanism by which any corrections, amendments or deletions are notified to PII processors and as far as possible, to third parties to whom PII had been disclosed.

### A.9.3 Complaint management

Objective: To set up efficient internal complaint handling and redress procedures for use by PII principals.

Organizations should implement appropriate measures to efficiently handle complaints received from PII principals

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.10 Accountability

**A.10.1 Governance**

Objective: To establish efficient governance for PII processing.

Organizations should implement appropriate measures to establish efficient governance related to PII processing.

**A.10.2 Privacy risk assessment**

Objective: To establish a privacy risk assessment process and to perform a privacy risk assessment as necessary.

If an organization is processing PII, then the organizations should establish the processes necessary to conduct a privacy risk assessment.

**A.10.3 Privacy requirement for contractors and PII processors**

Objective: To ensure, through contractual or other means such as mandatory internal policies, that the third party recipient provide at least equivalent levels of PII protection.

Organizations should implement appropriate measures to ensure contractors and PII processors have implemented adequate levels of PII protection.

…

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

**A.10 Accountability (cont.)**

…

**A.10.4 Privacy monitoring and auditing**

Objective: To monitor and audit PII protection controls and the effectiveness of internal PII protection policy.

Organizations should implement appropriate measures to periodically monitor and audit privacy controls and the effectiveness of internal privacy policy.

**A.10.5 PII protection awareness and training**

Objective: To provide suitable training and awareness concerning PII protection for the personnel of the PII controller who will have access to PII.

Organizations should implement appropriate measures to provide suitable training for the personnel of the PII controller.

**A.10.6 PII protection reporting**

Objective: To develop, disseminate, and update PII protection reports.

Organizations should develop, disseminate as appropriate, and update reports (for example, reporting on breaches, investigations, audits) to senior management and other personnel with responsibility for monitoring PII protection in order to demonstrate accountability with specific statutory and regulatory PII protection programme mandates.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.11 Information security

Objective: To ensure that PII is appropriately safeguarded in accordance with the results of a risk assessment.

PII in the care and custody of the organization should be protected by appropriate controls, in accordance with the results of a threat risk and/or privacy impact assessment.

# Pre-DIS 29151 Code of practice for PII protection

## Additional objectives and controls

### A.12 Privacy compliance

#### A.12.1 Compliance

Objective: To avoid breaches of legal, statutory, regulatory, privacy policy or contractual obligations related to privacy and to any privacy requirements.

Organizations should implement appropriate measures to ensure PII processing meets compliance requirements.

#### A.12.2 Cross border data transfer restrictions in certain jurisdictions

Objective: To protect PII when it is being transferred across borders.

Organization should implement appropriate measures to ensure that any transfers of PII across borders meets relevant compliance requirements.

# PIMS – New Work Item

## Enhancement to ISO/IEC 27001 for privacy management

1 Scope
2 Normative references
3 Terms and definitions
4 Privacy-specific requirements related to ISO/IEC 27001
4.1 Structure of this Standard
4.2 Privacy-specific requirements related to ISO/IEC 27001
4.2.1 Consideration of privacy principles and self-obligations
4.2.2 Appending the scope of the ISMS with the protection of PII
4.2.3 Privacy-specific policy
4.2.4 Privacy-specific responsibilities
4.2.5 Privacy risk assessment
4.2.6 Privacy risk treatment
4.2.7 Appending the mandatory control set for the protection of PII
4.2.8 Use of another reference controls list than Annex A of this International Standard
4.2.9 Privacy risk assessment in operation
4.2.10 Privacy risk treatment in operation

Annex A – Reference control objectives and controls

Follows ISO 27009 !!!

# 29134 Privacy Impact Assessment Methodology - Guidelines

## Enters CD, ready in ~2 years

### privacy impact assessment PIA

overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of PII, framed within an organization's broader risk management framework.

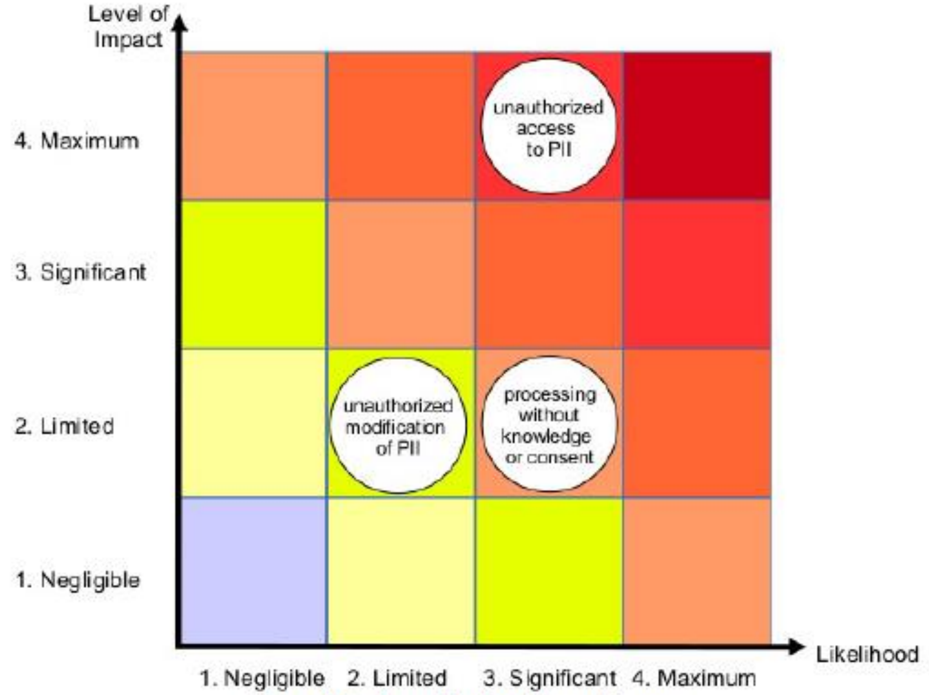
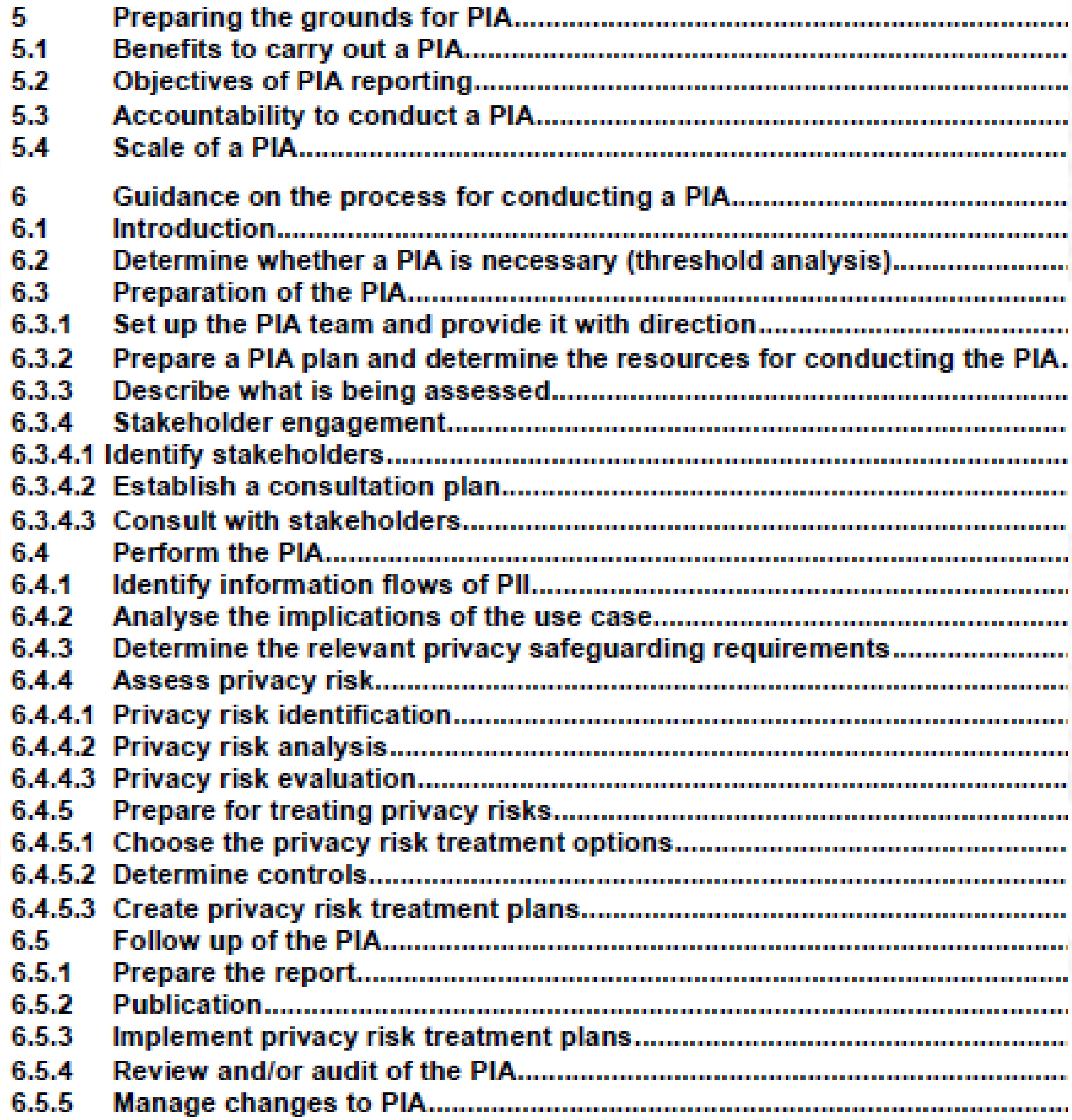


**Figure D2 —Example of a privacy risk map**

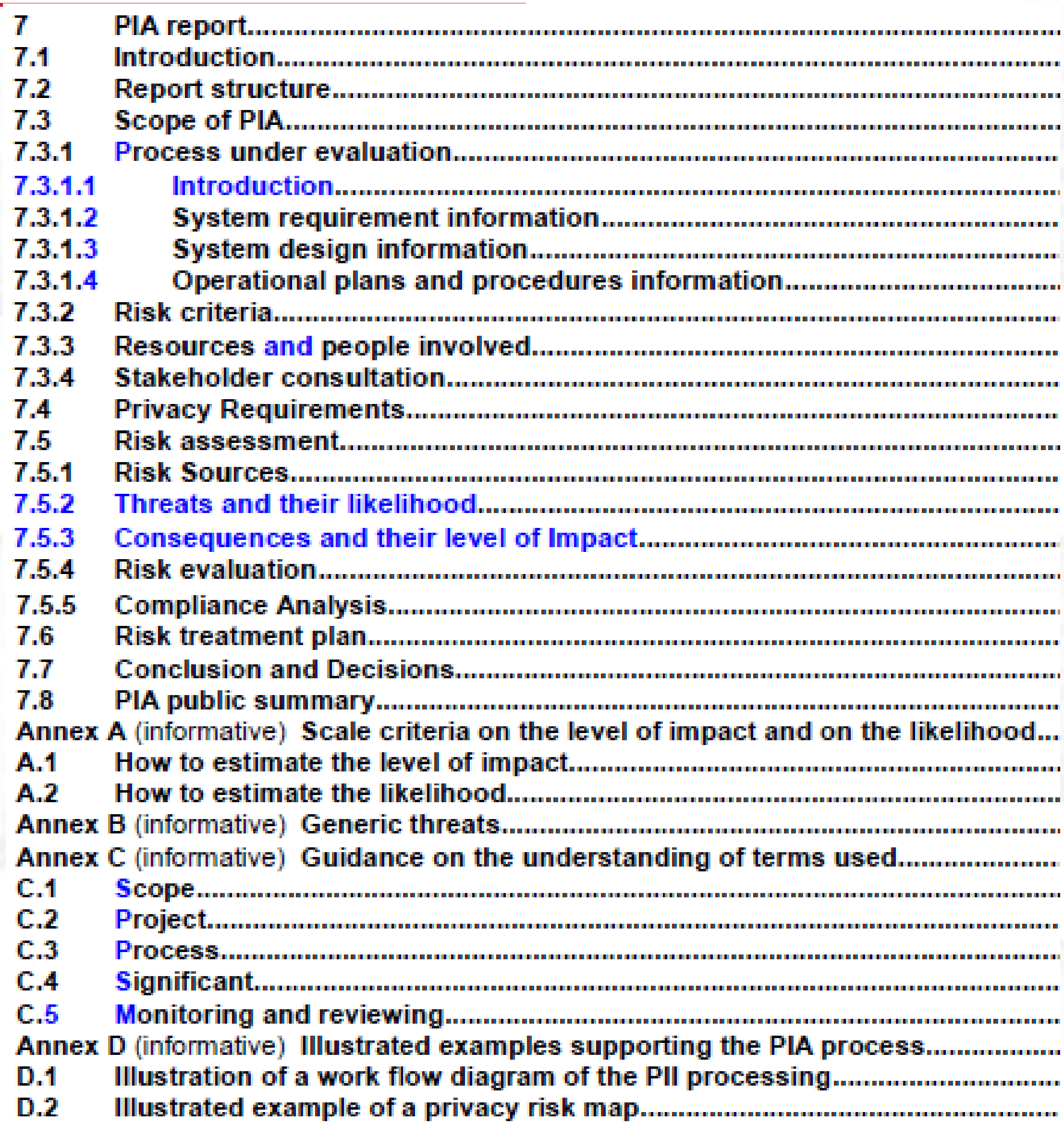
# 29134 Privacy Impact Assessment Methodology - Guidelines

## ToC



# 29134 Privacy Impact Assessment Methodology - Guidelines

## ToC



itrust
consulting

# Thank you for your attention!