TECHNICAL REPORT

ISO/IEC TR 27550

First edition
2019-09

Information technology — Security techniques — Privacy engineering for system life cycle processes

Technologies de l'information — Techniques de sécurité — Ingénierie de la vie privée pour les processus du cycle de vie des systèmes

Reference number
ISO/IEC TR 27550:2019(E)

© ISO/IEC 2019

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

© ISO/IEC 2019 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

© ISO/IEC 2019 – All rights reserved

Introduction

Privacy engineering is often associated with terms such as:

— privacy-by-design and privacy-by-default, coined by Ann Cavoukian[16] in the early nineties; or

— data protection by design and data protection by default, used in the European regulation published in April 2016[17].

In recent years, a number of concepts, principles and approaches have been proposed for privacy engineering. In a paper on privacy engineering[20], Spiekermann and Cranor contrast privacy-by-architecture from privacy-by-policy. The former focuses on data minimization, anonymization and client-side data processing and storage while the latter focuses on enforcing policies in data processing. In a paper on engineering privacy-by-design[21], Gürses, Troncoso, and Diaz state that data minimization should be the foundational principle for engineering privacy-respecting systems. In a paper on privacy-by-design in intelligent transport systems[22], Kung, Freytag and Kargl define three principles, minimization, enforcement and transparency. In a paper on protection goals for privacy engineering[23], Hansen, Jensen, and Rost identify three goals: unlinkability, transparency and intervenability. In two papers on privacy design strategies[29][30], Hoepman identifies four data oriented strategies (minimize, separate, abstract, hide), as well as four process oriented strategies (inform, control, enforce, demonstrate).

A number of global papers have been published. A privacy threat framework was defined by KU Leuven[24] that led to the LINDDUN methodology[25]. Two OASIS technical committees published specifications focusing on the implementation of privacy in systems: the *Privacy Management Reference Model and Methodology* (July 2013, updated in May 2016)[27] and the *Privacy by Design Documentation for Software Engineers* and *Companion committee note* published in June 2014[28]. The December 2014 ENISA report entitled *Privacy and Data Protection by Design — from Policy to Engineering*[26] provides a good overview on privacy policies and their influence on the definition of privacy engineering concepts. The December 2015 privacy and security-by-design methodology handbook from PRIPARE[31] provides a methodology which covers the whole engineering lifecycle integrating existing concepts, principles and methods. Joyee De and Le Métayer published in 2016 a book on privacy risk analysis[32]. The January 2017 NIST internal report[19] introduces a definition of privacy engineering, a privacy risk model and three privacy engineering objectives: predictability, manageability and disassociability.

Privacy engineering practice is supported by a growing body of standards on privacy, on security, and on software and system engineering.

Examples of useful privacy standards are:

— ISO/IEC 29100[10] which provides a high-level framework for the protection of PII within ICT systems. It is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework;

— ISO/IEC 29134[11] which gives guidelines for a process on privacy impact assessments (PIA) and a structure and content of a PIA report;

— ISO/IEC 29151[12] which establishes control objectives, controls and guidelines for implementing controls to meet the requirements identified by a risk and impact assessment related to the protection of PII;

— ISO/IEC 27018[13] which defines a code of practice for the protection of personally identifiable information (PII) in public clouds acting as PII processors;

— ISO/IEC 27552[14] which provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS); and

— OASIS privacy management reference model and methodology (PMRM)[27] which provides a guideline or template for developing operational solutions to privacy issues.

© ISO/IEC 2019 – All rights reserved

When the security of personally identifiable information (PII) is at stake, privacy engineering can be supported by security standards such as:

— ISO/IEC 27001[6] which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization;

— ISO/IEC 27002[7] which provides guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls;

— ISO/IEC 27005[8] on information security risk management which can be used as a reference for privacy risk management processes; and

— ISO/IEC 27034[9] on application security which can be used to assist organizations in integrating security concerns related to PII throughout the life cycle of their applications.

When the engineering of software products and systems is involved, privacy engineering can be supported by software and system engineering standards such as:

— ISO/IEC/IEEE 15288[1] on system life cycle processes which can be used to describe privacy engineering processes;

— ISO/IEC/IEEE 12207[2] on software life cycle processes; and

— ISO/IEC/IEEE 29148[3] on requirement engineering which can be used for the engineering of privacy requirements for systems and software products and services throughout the life cycle.

This document takes into account principles and concepts for privacy engineering as well as standards and practices related to privacy, security and system and software engineering. It extends ISO/IEC/IEEE 15288 by adding specific guidelines that will help organizations integrate advances in privacy engineering in their engineering practices.

Privacy engineering practice is also influenced by the following factors:

— the need to adapt privacy engineering to different system and software engineering practices such as agile programming;

— the need to have a multidisciplinary approach integrating different viewpoints such as citizen, societal, ethical, legal, technical, or business viewpoints;

— the need to adapt privacy engineering to the different organizational roles in a supply chain such as a system developer, a system integrator, or a system operator;

— the need to take into account the specific system and application needs of a sector such as smart grids, health, or transport; and

— the various interactions that engineers need to have with other stakeholders (e.g., product owner, system product manager, privacy officer) to take into account the multidisciplinary facets of privacy engineering.

This document also contains guidance on how an organization can adapt its privacy engineering practices to take into account these specific factors. Since this document is intended to encourage good privacy practice in the development of a wide range of ICT systems and applications, it does not contain system specific or application specific content.

© ISO/IEC 2019 – All rights reserved

Information technology — Security techniques — Privacy engineering for system life cycle processes

1 Scope

This document provides privacy engineering guidelines that are intended to help organizations integrate recent advances in privacy engineering into system life cycle processes. It describes:

— the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, risk management); and

— privacy engineering activities in key engineering processes such as knowledge management, risk management, requirement analysis, and architecture design.

The intended audience includes engineers and practitioners who are involved in the development, implementation or operation of systems that need privacy consideration, as well as managers in organizations responsible for privacy, development, product management, marketing, and operations.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org

3.1
activity
set of cohesive tasks of a process

[SOURCE: ISO/IEC/IEEE 15288:2015]

3.2
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC/IEEE 27000:2018]

3.3
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC/IEEE 27000:2018]

© ISO/IEC 2019 – All rights reserved

3.4
disassociability
property that enables the processing of PII or events without association to individuals or devices beyond the operational requirements of the system

[SOURCE: NISTIR 8062]

3.5
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018]

3.6
intervenability
property that ensures that PII principals, PII controllers, PII processors and supervisory authorities can intervene in all privacy-relevant data processing

Note 1 to entry: the extent to which any of these stakeholders can intervene in data processing may be limited by relevant legislation or regulation.

[SOURCE: ULD]

3.7
manageability
property that provides the capability for granular administration of PII including alteration, deletion, and selective disclosure

[SOURCE: NISTIR 8062]

3.8
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 1 to entry: 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.

[SOURCE: ISO/IEC 29100:2011]

3.9
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 1 to entry: 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.

[SOURCE: ISO/IEC 29100:2011]

3.10
PII principal
natural person to whom the personally identifiable information (PII) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.

[SOURCE: ISO/IEC 29100:2011]

© ISO/IEC 2019 – All rights reserved

3.11
PII processor
privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100:2011]

3.12
predictability
property that enables reliable assumptions by individuals, owners, and operators about PII and its processing by a system

[SOURCE: NISTIR 8062]

3.13
privacy breach
situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements

[SOURCE: ISO/IEC 29100:2011]

3.14
privacy engineering
integration of privacy concerns into engineering practices for systems and software engineering life cycle processes

3.15
privacy principles
set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems

[SOURCE: ISO/IEC 29100:2011]

3.16
privacy risk
effect of uncertainty on privacy

[SOURCE: ISO/IEC 29100:2011]

Note 1 to entry: Risk is defined as the "effect of uncertainty on objectives" in ISO Guide 73 and ISO 31000.

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

3.17
privacy risk source
element which alone or in combination with other elements has the intrinsic potential to give rise to *privacy risk* (3.16)

Note 1 to entry: also referred to as privacy risk factor in NISTIR 8062[18].

Note 2 to entry: also referred to as privacy threat in LINDDUN[22].

3.18
process
set of interrelated or interacting activities which transform inputs into outputs

[SOURCE: ISO/IEC 27000:2018]

© ISO/IEC 2019 – All rights reserved

3.19
process outcome
observable result of the successful achievement of the process purpose

[SOURCE: ISO/IEC/IEEE 15288:2015]

3.20
processing of PII
operation or set of operations performed upon personally identifiable information (PII)

Note 1 to entry: 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.

Note 2 to entry: also referred to as data action in NISTIR 8062[18]

[SOURCE: ISO/IEC 29100:2011]

3.21
risk
effect of uncertainty on objectives

[SOURCE: ISO/IEC 31000:2018]

3.22
task
required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a process

[SOURCE: ISO/IEC/IEEE 15288:2015]

3.23
touch point
intersections of data flows across domains or systems or processes within domains

[SOURCE: OASIS PMRM]

3.24
transparency
property that ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed

[SOURCE: ULD]

3.25
unlinkability
property that ensures that a PII principal may make multiple uses of resources or services without others being able to link these uses together

[SOURCE: ULD]

4 Abbreviated terms

CNIL	Commission Nationale de l'Informatique et des Libertés
DFD	Data flow diagram
ICT	Information and communication technology
IoT	Internet of things

© ISO/IEC 2019 – All rights reserved

LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
PET	Privacy enhancing technology
PIA	Privacy impact assessment
PII	Personally identifiable information
PMRM	Privacy management reference model and methodology
PRIPARE	PReparing the Industry to Privacy-by-design by supporting its Application in REsearch
STRIDE	Spoofing identity, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege

5 Privacy engineering

5.1 General

Privacy engineering deals with the integration of privacy concerns into engineering practices for systems and software engineering life cycle processes.

5.2 Relationship with system and software engineering

System and software engineering deal with the building of capabilities throughout a system and software's life cycle. A life cycle is defined as an abstract functional model that represents the conceptualization of a need for the system, its realization, utilization, evolution and disposal[1]. A life cycle model is described as a set of processes, their outcomes, relationships and sequence. Examples of life cycle models are the waterfall model or the agile programming model.

System and software engineering practice relies on conformance with a selected life cycle model and its associated processes. Privacy engineering practice extends system and software engineering practice through the integration of privacy concerns into the life cycle processes. It therefore has an impact on the description of the life cycle processes.

ISO/IEC/IEEE 15288 describes thirty processes structured into four categories:

— agreement processes which focus on activities related to supplier agreements;

— organizational project-enabling processes which focus on activities related to improvement of the organization's business or undertaking;

— technical management processes which focus on managing the resources and assets allocated to the engineering of a system; and

— technical processes which focus on technical actions throughout the life cycle.

This document, in particular Clause 6, focuses on the ISO/IEC/IEEE 15288 processes where the need for privacy engineering guidance has been identified.

© ISO/IEC 2019 – All rights reserved

5.3 Relationship with security engineering

The relationship between security and privacy (see Figure 1) is as follows:

— security risks arise from unauthorized system and user behaviour. Many security risks are not privacy risks, for instance the lack of protection for organization trade secrets;

— privacy risks arise as a by-product of unauthorized PII processing (e.g., the lack of consent management mechanisms, the lack of transparency capabilities, a breach incident); and

— some security risks are also privacy risks, for instance a lack of security of collected PII (e.g., health data, location data, etc.).

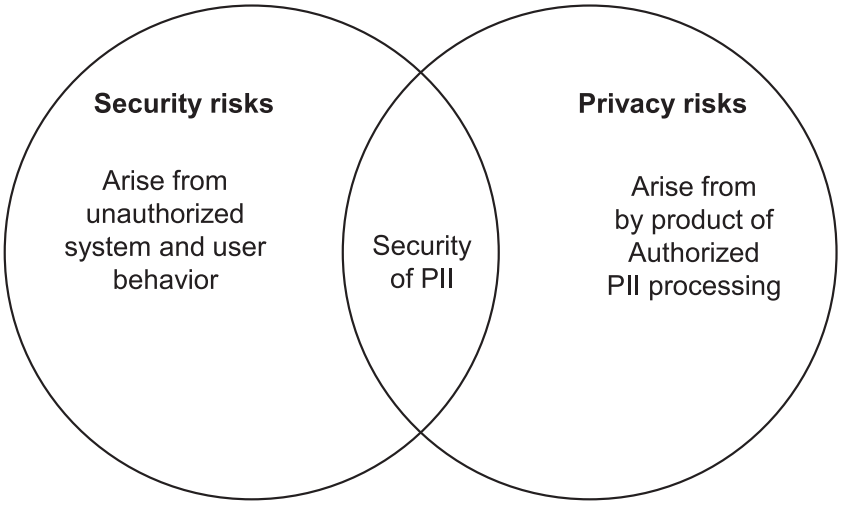

Figure 1 — Relationship between security and privacy

Security engineering focuses on objectives associated with attributes such as confidentiality, integrity, availability, and protection of ICT assets. Privacy engineering focuses on objectives associated with the operationalization of privacy principles listed in ISO/IEC 29100:

— 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; and

— privacy compliance.

Annex A provides further guidance on privacy engineering objectives.

© ISO/IEC 2019 – All rights reserved

5.4 Relationship with risk management

Risk management deals with the systematic application of management policies, procedures and practices to the tasks of communication, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk models[1)] are used in risk management to define the risk sources to be assessed and the relationships among the risk sources. Risk models provide a method to estimate the level of risk by considering and combining consequences and likelihoods, where a consequence is the outcome of an event that has an effect on objectives, and likelihood is the chance that the event can happen.

A widely used risk model consists in expressing the risk level as a function of the likelihood that an adverse outcome occurs multiplied by the magnitude of the adverse outcome if it occurs:

Risk level	=	Likelihood of an event occurrence	×	Impact of an event occurrence

Risk management practice in the engineering of a system needs to take into account several types of risks:

— privacy risks;

— security risks; and

— risks related to other system characteristics such as safety[2)], or reliability.

An integrated approach is needed as shown in Figure 2. For instance, poor health data management can lead to privacy risks (e.g., PII is made public), to security risks (e.g., health data has been compromised and the health system is no longer accessible), or to safety risk (e.g., urgent medical treatment is not possible).

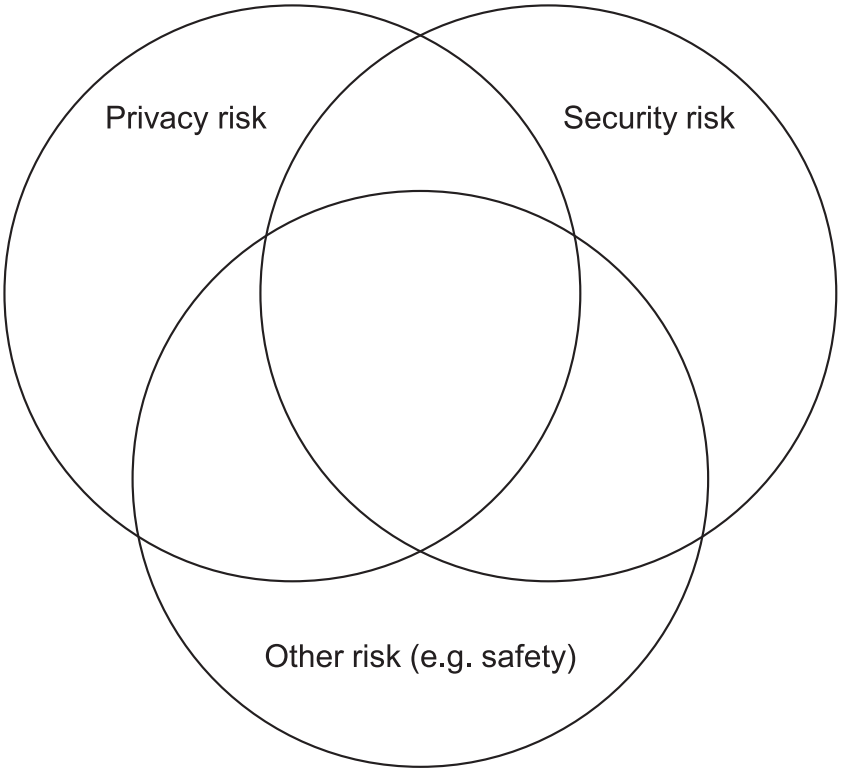

Figure 2 — Multiple risk concerns in system engineering

1) From NIST 800-30[33].

2) Ability that ensures that a system is unlikely to cause danger, risk, or injury.

© ISO/IEC 2019 – All rights reserved

Privacy risk sources and consequences

Figure 3[3)] shows the important types of risk sources and consequences for privacy.

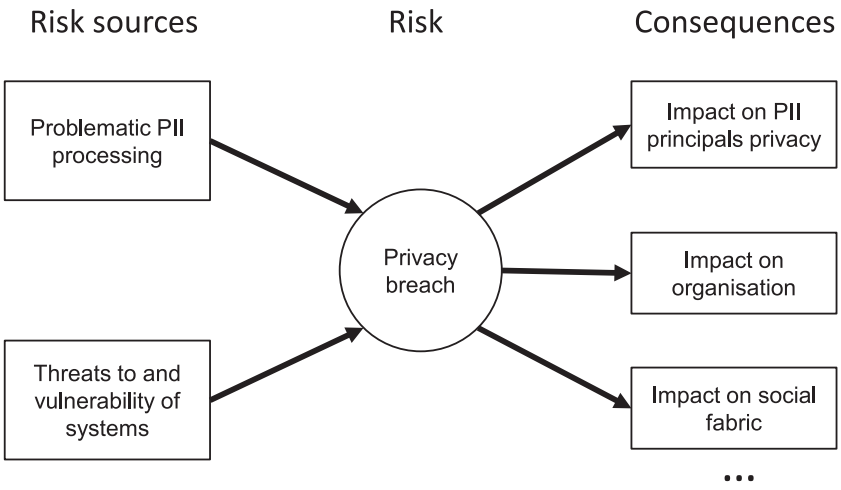

Figure 3 — Privacy risk sources and consequences

Privacy risk sources include:

— PII processing risks arising from the operations of the system itself. Annex C defines and explains a number of PII processing risks (e.g., distortion, surveillance, unanticipated revelation). Daniel Solove also provides a taxonomy of PII processing risks[38]; and

— risks caused by potential threats to and vulnerability of a system. These can result in a privacy breach due to weaknesses or failures in the security of PII in systems (e.g., unauthorized access to PII).

Consequences that can arise as a result of privacy risks include:

— impact on PII principals' privacy, such as:
  — loss of autonomy;
  — exclusion;
  — loss of liberty;
  — physical harm;
  — stigmatization;
  — power imbalance;
  — loss of trust; and
  — economic loss;

— impact on the operations and business of an organization. For instance, a privacy breach can result in the following costs:
  — non-compliance costs (i.e., impact on the organization of not complying with applicable laws, policies, contracts);
  — direct costs (e.g., potential for decrease in use of the system or other impediments to achieving its mission);

3) Called bow-tie diagram in risk management.

© ISO/IEC 2019 – All rights reserved

- reputational costs (e.g., negative impact on public trust in the organization);
- internal culture costs (e.g., negative impact on employee morale, retention, or other aspects of organization culture); and
- other costs specific to each organization's work, mission, structure, and customer base; and

— other types of impact such as the impact on the social fabric.

Annex D provides examples of risk models and associated methodologies.

Guidelines for privacy risk management are provided in ISO/IEC 29134[11]. This document extends ISO/IEC 29134 by adding considerations on the integration of the privacy impact assessment process in ISO/IEC/IEEE 15288 processes.

6 Integration of privacy engineering in ISO/IEC/IEEE 15288

6.1 General

ISO/IEC/IEEE 15288 [1] covers the following categories of process:

— agreement processes (e.g., the supply process);

— organizational project-enabling processes (e.g., the quality management process);

— technical management processes (e.g., the risk management process); and

— technical processes (e.g., the system requirements definition process).

ISO/IEC/IEEE 15288 describes a process as follows:

— it has a purpose;

— it creates outcomes; and

— it consists of activities which themselves consist of tasks.

The relationship between process, purpose, outcome, activity and task is shown in Figure 4 on the left. The specific dependencies between processes, activities and tasks are shown on the right.

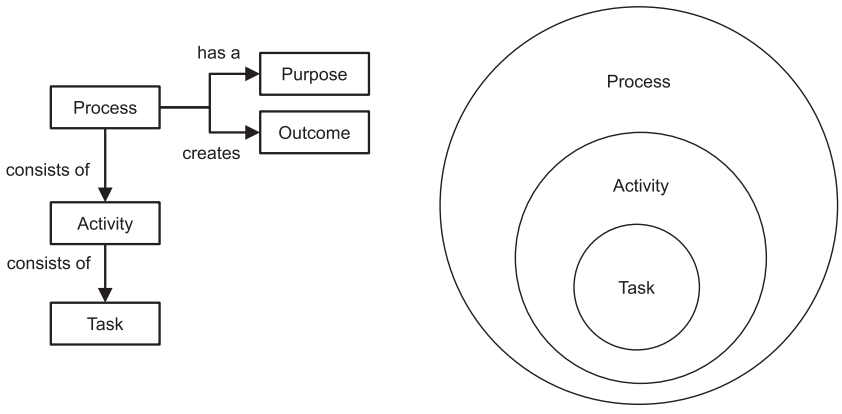

Figure 4 — Processes, activities and tasks

This document provides additional descriptions of processes, purposes, outcomes, activities and tasks concerning privacy engineering where appropriate. Covered ISO/IEC/IEEE 15288 processes are shown in Table 1.

© ISO/IEC 2019 – All rights reserved

Table 1 — Covered system life cycle processes

Type of process (ISO/IEC/IEEE 15288)	Covered system life cycle processes (ISO/IEC/IEEE 15288)	Privacy engineering issues
Agreement processes	Acquisition process	Supply chain involves PII
	Supply process	
Organizational project-enabling processes	Human resources management process	Privacy engineering human resource management
	Knowledge management process	Privacy engineering knowledge management
Technical management process	Risk management process	Privacy risk management
Technical processes	Stakeholder needs and requirements process	Stakeholders' privacy expectations
	System requirements definition process	Privacy principles operationalization
	Architecture definition process	Impact of privacy concerns on architecture
	Design definition process	Impact of privacy on design

The rationale for covering the above processes is as follows:

— acquisition and supply processes: guidelines on the relationships between stakeholders in the supply chain are needed to ensure that all relevant privacy requirements have been identified and documented and that they are provided to all sub-system suppliers as appropriate. This includes the relations between PII controllers and PII processors as well as the relationships between PII controllers/processors and suppliers;

— human resources management process: guidelines on privacy engineering human resource management are needed to ensure that relevant competency is available and becomes an integral part of an organization's culture and core values;

— knowledge management process: guidelines on how to carry out continuous improvement in privacy engineering are needed to ensure that best practices are updated within an organization;

— risk management process: guidelines on how to carry out a risk management process are needed to ensure that relevant privacy risk sources, as well as relevant impacts, are properly assessed. Risk sources stem from problematic PII processing as well as threats to and vulnerabilities of the system. The resulting impact may be on PII principals' privacy as well as organizations' operations and business;

— stakeholders needs and requirements process: guidelines on how to address stakeholders' privacy expectations are needed;

— system requirements definition process: guidelines on the transformation of privacy principles into a set of operational requirements is needed to ensure that these principles are taken into account from the start of the system life cycle;

— architecture definition process: guidelines on the definition of a system architecture are needed to ensure that privacy principles are taken into account. For instance, data minimization considerations can have an influence on the location of data storage; and

— design definition process: guidelines on the design of the system are needed to ensure that appropriate privacy controls are integrated.

6.2 Acquisition and supply processes

Purpose in ISO/IEC/IEEE 15288

 © ISO/IEC 2019 – All rights reserved

The purpose of the acquisition process is to obtain a product or service in accordance with the acquirer's requirements.

The purpose of the supply process is to provide an acquirer with a product or service that meets agreed requirements.

Additional purposes for privacy engineering

These processes need to include requirements related to privacy. The acquirer can be either a PII controller or a PII processor. The supplier can also be a PII processor when it provides a service to a PII controller or to another PII processor.

Additional outcomes for privacy engineering

Successful implementation of these processes should result in an agreement on respective privacy obligations being established between the acquirer and the supplier, for instance the delivery of a product or a service which meets the privacy obligations and requirements.

Guidelines for privacy engineering

The content of the agreement depends on the role of the acquirer and of the supplier:

— the supplier can be responsible for the provision of a complete solution (e.g., an end-to-end IoT solution);

— the supplier can provide data processing services (e.g., a cloud virtual machine); or

— the supplier can be responsible for the provision of a sub-system (e.g., a sensing device, or a specific software component).

The following elements can be integrated into the agreement:

— operational agreements when appropriate (e.g., between a PII processor and a PII controller). These agreements include legal obligations, insurance obligations, and incident management obligations as appropriate; and

— privacy engineering practice requirements (e.g., between a PII processor and an end-to-end solution provider). These requirements include agreement on privacy standards to use, agreement on privacy controls to use, identification and documentation of all relevant privacy requirements, verification, validation, acceptance and certification practices and conditions, and agreement on change procedures.

Specific obligations on suppliers and acquirers can exist in certain jurisdictions with respect to the processing of PII. These obligations should be taken into account in the development of any agreements between these two entities.

NOTE As part of these processes, the agreement is modified when a change request is agreed to by both the acquirer and supplier, including concerning privacy requirements.

6.3 Human resources management process

Purpose in ISO/IEC/IEEE 15288

The purpose of the human resource management process is to provide the organization with necessary human resources and to maintain their competencies, consistent with business needs.

This process provides a supply of skilled and experienced personnel qualified to perform life cycle processes to achieve organization, project, and stakeholder objectives.

Additional outcomes for privacy engineering

© ISO/IEC 2019 – All rights reserved

Successful implementation of the human resources management process should result in:

a) skills for privacy engineering required by projects being identified;

b) necessary human resources for privacy engineering being provided to projects; and

c) skills of personnel for privacy engineering being developed, maintained or enhanced.

Guidelines for privacy engineering

The human resources management process depends on:

— the role of the organization in the supply chain (e.g., PII controller, PII processor, supplier of a complete solution, supplier of a sub-system); and

— the domain (e.g., health, energy, automotive, transport).

Skills needed for privacy engineering include, but are not limited to:

— basic system and software engineering skills;

— specific skills on laws and social sciences;

— specific privacy engineering skills at organizational, management and technical levels. This includes an understanding of privacy engineering processes (e.g., based on this document), in particular:

  — the practice of privacy risk management;

  — the practice of privacy engineering taking into account privacy engineering objectives (see Annex A); and

— specific integration skills within a domain. This includes:

  — the integration of privacy risk management with other risk management activities (e.g., in domains where safety requirements are important); and

  — the integration of privacy engineering with other organization specific engineering practices (e.g., model-driven engineering, agile programming).

The process should include a program for privacy engineering skill development. This involves training and education (internal and/or external), the creation and maintenance of training material, and the monitoring of skills development within the organization.

The process can also be associated with an assessment and competency/skill certification process (e.g., certified privacy engineers).

6.4 Knowledge management process

Purpose in ISO/IEC/IEEE 15288

The purpose of the knowledge management process is to create the capability and assets that enable the organization to exploit opportunities to re-apply existing knowledge.

Additional purposes for privacy engineering

This process should be applied to knowledge resulting from privacy engineering practice.

Additional outcomes for privacy engineering

Successful implementation of the knowledge management process should result in:

a) the requirements for privacy engineering knowledge being defined and the elements of a privacy engineering knowledge repository being identified and specified;

 © ISO/IEC 2019 – All rights reserved

b) a privacy engineering knowledge repository being available; and

c) knowledge management usage data being gathered and analysed.

Guidelines for privacy engineering

Privacy engineering necessitates multidisciplinary knowledge: technical, legal as well as socio-cultural and ethical knowledge.

The resulting knowledge can take various forms including, but not limited to:

— concepts;

— rules;

— guidelines;

— references;

— model descriptions (processes); and

— libraries of privacy controls.

Figure 5 shows the two activities that are involved:

— in the knowledge management process, ethical, legal and technical experts, including privacy engineers, create content for the privacy engineering knowledge repository; and

— in other processes, privacy engineers and other engineers reuse content from the repository.

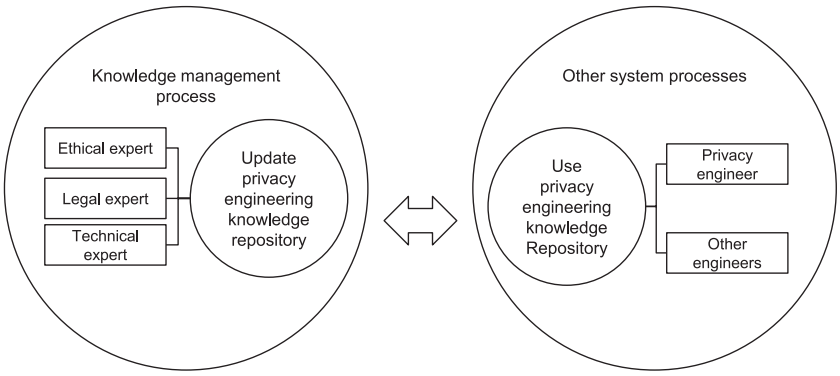

Figure 5 — Multidisciplinary knowledge creation and use

The knowledge repository may be structured in a number of different ways. For instance, the organization normative framework (defined as an organization-wide internal structure containing a set of normative application security processes and elements) described in ISO/IEC 27034[9] on application security can be used for privacy as shown in Figure 6, resulting in the following components:

— business context;

— regulatory context;

— technological context;

— application specifications repository;

— roles, responsibilities and qualifications;

— organization application privacy control library;

— processes related to application privacy; and

© ISO/IEC 2019 – All rights reserved

— application privacy lifecycle reference model.

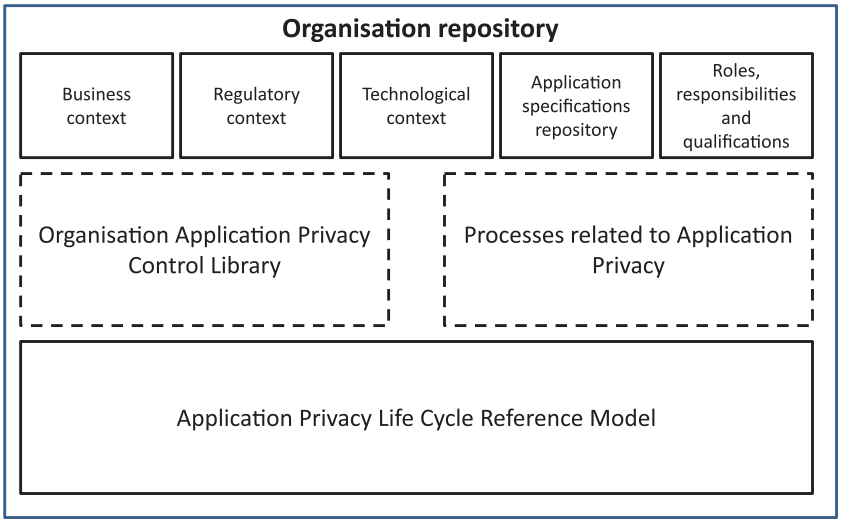

Figure 6 — Elements of a privacy engineering knowledge repository

Annex C contains information on a number of catalogues that are of interest in a privacy engineering knowledge repository:

— PII processing risks provided by NIST[18] (see C.2);

— privacy threats provided by LINDDUN[25] (see C.3);

— problems for individuals provided by NIST[18] (see C.4);

— privacy controls provided by ISO/IEC 27552[14] (see C.5) and by ISO/IEC 29151[12];

— privacy management services provided by OASIS PMRM[27] (see C.6); and

— privacy measures provided by LINDDUN[25] (see C.7).

A privacy engineering repository will also include reference documents such as:

— guidelines associated with the description of privacy principles in ISO/IEC 29100[10].

— guidelines for the operationalization of privacy principles and privacy control requirements provided by OASIS-PMRM[27]; and

— guidelines for a privacy-by-design methodology provided by PRIPARE[31].

6.5 Risk management process

Purpose in ISO/IEC/IEEE 15288

The purpose of the risk management process is to identify, analyse, treat and monitor risks continually.

The risk management process is a continual process for systematically addressing risk throughout the life cycle of a system product or service. It can be applied to risks related to the acquisition, development, maintenance, operation and eventual disposition (e.g., decommissioning) of a system.

Additional purposes for privacy engineering

The risk management process is applied to privacy risk sources and consequences.

Additional outcomes for privacy engineering

© ISO/IEC 2019 – All rights reserved

Successful implementation of the risk management process[4] should result in:

a) privacy risks being identified;

b) privacy risks and consequences being analysed and a privacy impact assessment having been carried out;

c) privacy risk treatment options being identified, prioritized, and selected;

d) appropriate treatment being implemented; and

e) privacy risks being evaluated to assess changes in status and progress in treatment.

Additional guidelines for privacy engineering

Guidelines provided by ISO/IEC 29134 should be followed. The text below shows how ISO/IEC 29134 can be integrated in the ISO/IEC/IEEE 15288 risk management process.

Additional activities and tasks for privacy engineering

ISO/IEC/IEEE 15288 describes the following risk management activities:

— plan (risk management);

— manage (the risk profile);

— analyze (risks);

— treat (risks); and

— monitor (risks).

The **analyse risk activity** for privacy engineering includes the following tasks:

1) identify risks associated with PII processing and identify threats to and vulnerabilities of the system(s) processing PII;

   NOTE 1 See C.2 for a catalogue of risks associated with PII processing.

   NOTE 2 The identification of threats to and vulnerabilities of the security of PII assets should be integrated into the organization's overall security risk management process. See ISO/IEC 27005 for guidelines on information security risk management[8].

   NOTE 3 See C.3 for a catalogue of privacy threats, as well as ISO/IEC 29134:2017, Annex B[11].

2) estimate the likelihood and consequences of each identified risk;

   NOTE 4 Organizations can support the assessment of likelihood in a number of ways: using information on customer demographics to estimate likelihood; extrapolating from information available about privacy risks in similar scenarios; or conducting focus groups or surveys to glean more thorough and specific information from users about privacy concerns.

   NOTE 5 The consequences include the impact on the PII principals' privacy and the impact on the organizations' business and operations. For consequences on PII principals' privacy, see C.4. For consequences on the organizations' business and operation, the impact may be felt in terms of penalties for non-compliance, operational costs, and reputational and internal culture damage.

   NOTE 6 ISO/IEC 29134:2017, Annex A[11] provides guidelines on how to estimate privacy risk likelihood.

3) evaluate and prioritize privacy risks; and

NOTE 7 See Annex D for examples of privacy risk analysis approaches.

4) Note that this process is iterative.

© ISO/IEC 2019 – All rights reserved

NOTE 8 ISO/IEC 29134:2017, Annex A[11] provides guidelines on how to estimate the impact.

NOTE 9 Prioritization helps organizations to align mission priorities and resources. Addressing PII processing with low likelihood and low impact of being problematic can be of a lower priority, while addressing those with high likelihood and high impact is of the highest priority. However, likelihood and impact do not always align. For example:

— **low likelihood/high impact:** While certain PII processing can be less likely to become problematic, they can have a severe impact. In these cases, an organization can prioritize mitigation of these problems because any incidence of this severe problem would have unacceptable consequences. For example, if researchers had access to a data set of individuals' health information, the likelihood that the researchers would use the information improperly cannot be low, but the consequences for individuals, and therefore, for the mission and reputation of the organization, can be severe if misuse did occur, given the sensitive nature of health information; or

— **high likelihood/low impact:** Alternatively, a problematic PII processing with a small impact can have a very high likelihood, leading an organization to prioritize controls for those problems in order to avoid negatively affecting such a large portion of their constituents, even if the impact is low. For instance, an organization can use a web analytics tool that raises concerns among users of the website. In this case, the impact for each customer can be very limited, but given that the tool affects all users, the likelihood would be high.

These prioritization decisions vary by organization and PII processing, but are much better informed if both likelihood and impact are systematically assessed for each PII processing. In many cases, a determination of likelihood and impact is not be a simple process; just as implementing controls requires investment, properly assessing risk requires investment. In some cases, research can be necessary to better understand the likelihood of a privacy problem occurring. In others, it can be more appropriate to rely on the knowledge of experts in the organization.

4) prepare documentation for privacy impact assessment based on ISO/IEC 29134[11], as well as other reference documents.

6.6 Stakeholder needs and requirements definition process

Purpose in ISO/IEC/IEEE 15288

The purpose of the stakeholder needs and requirements definition process is to define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment.

Additional purposes for privacy engineering

This includes defining requirements for system privacy capabilities.

Additional outcomes for privacy engineering

Successful implementation of the stakeholder needs and requirements definition process should result in:

a) the privacy role of the organization being defined;

b) stakeholders with a privacy interest being identified; and

c) privacy capabilities being defined.

Guidelines for privacy engineering

The following tasks can be carried out in this process:

— identification of the organization's role in the supply chain (e.g., PII controller, PII processor, supplier);

— identification of stakeholders (e.g., employees, PII principals, sub-contractors, business partners); and

 © ISO/IEC 2019 – All rights reserved

— identification of potential privacy preserving features (e.g., consent management, mechanisms for individuals to exercise their right of access, etc.).

Table 2 provides more information on roles for organizations. It also makes a distinction between systems and subsystems. The reason is that privacy engineering for subsystems is not the same as privacy engineering for systems, as suppliers of subsystems are generally not aware of the privacy requirements of the system in which the subsystem will be integrated. While this can be true, the owner/operator of the system should be aware of the privacy requirements and should specify these to the sub-system suppliers in any specification, design or contractual documents.

Table 2 — Role of the organizations

Organization role	System type	Definition	Example
PII controller	System	Stakeholder operating a service that involves personal data processing	An operator of a social care network to assist elderly people
PII processor	System	Stakeholder processing personal data on behalf of a PII controller	An organization operating a cloud platform
Supplier	System	Stakeholder developing a system and potentially integrating subsystems from other suppliers	The developer of a turnkey social care system
Supplier	Subsystem	Stakeholder developing a subsystem that is subsequently integrated into a system.	The designer of a sensor that can be integrated in the turnkey social care system The designer of a smart phone operating system that is subsequently used to run a social care network

6.7 System requirements definition process

Purpose in ISO/IEC/IEEE 15288

The purpose of the system requirements definition process is to transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution that meets the operational needs of the user.

Additional purposes for privacy engineering

This includes an operationalization activity that transforms privacy principles into system requirements, ensuring that all privacy principles in ISO/IEC 29100 are effectively taken into account.

Additional outcomes for privacy engineering

Successful implementation of the system requirements definition process should result in:

a) system privacy requirements being defined;

b) privacy management services and any other privacy related services being identified; and

c) a preliminary privacy risk analysis having been carried out.

Guidelines for privacy engineering

The operationalization of privacy principles is a requirements analysis activity that includes goal-oriented as well as risk-oriented activities:

— in the goal-oriented activities, each privacy principle is considered as a high-level concern that the system needs to fulfil. Each principle is then decomposed into a set of specific goals to meet the concern. Privacy control requirements are then identified to address the specific goals; and

© ISO/IEC 2019 – All rights reserved

— in the risk-oriented activities, the focus is on the identification of the threats to and vulnerabilities of the PII assets in the system, and the identification of the risks associated with PII processing that can compromise compliance with the privacy principles.

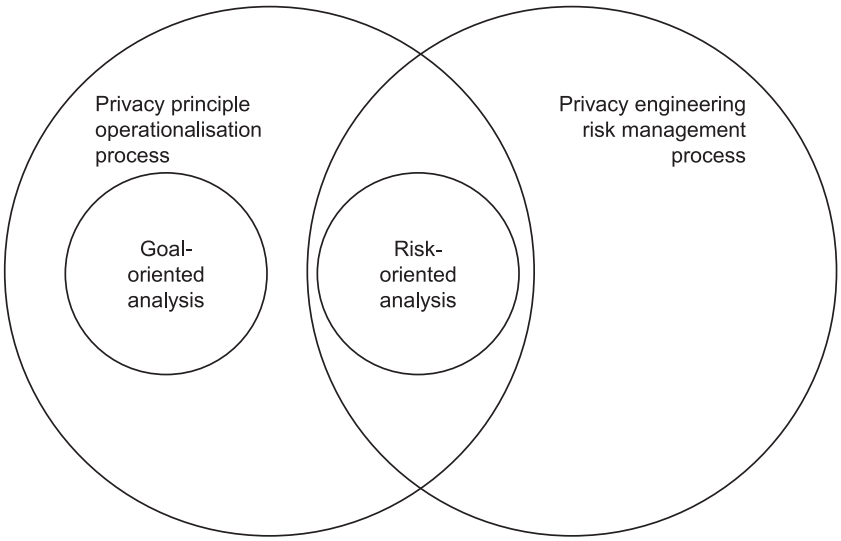

Figure 7 — Goal-oriented and risk-oriented requirement elicitation

The set of privacy control requirements derived from the requirements analysis are jointly referred to as operational requirements. As depicted in Figure 7, the risk-oriented activities are also part of the privacy engineering risk management activity.

Additional tasks and activities for privacy engineering

The system requirements definition process includes the following activities and tasks:

a) frame organization system objectives:

   1) describe the functionality of the system;

      NOTE 1 A use case description can be used as recommended in OASIS PMRM[27] as well as in NISTIR 8062[18].

   2) describe the business needs that the system serves; and

   3) describe what privacy-preserving functionality the system will have.

b) frame privacy governance:

   1) identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the system needs to operate. List any specific privacy requirements arising from these sources;

   2) identify any privacy-related principles (e.g., ISO 29100) or other commitments to which the organization adheres (e.g., industry code of practice);

   3) identify any privacy goals that are explicit or implicit in the organization's vision and/or mission; and

   4) identify any privacy-related policies or statements within the organization.

c) develop a privacy analysis:

   1) describe stakeholders, systems, business processes, data elements and data flows;

© ISO/IEC 2019 – All rights reserved

NOTE 2 Data elements and data flows are associated with PII processing such as collection, retention/logging, generation/transformation, disclosure/transfer, and/or disposal. The description can consist of a system map with associated tags. The description can use the model and methodology provided by OASIS PMRM[27].

NOTE 3 The description involves the identification of touch points (i.e., intersections between two domains). The objective is to clarify the data flows and ensure a complete picture of all domains, systems, and processes in which PII is used. OASIS PMRM[27] allows for the specification of privacy controls associated with PII. It includes not only the internal privacy controls created within the domain/sub domain, but also identifies privacy controls inherited and exported to/from other domains/ subdomains.

NOTE 4 The description can use the data flow diagram as proposed by LINDDUN[25] (see C.3).

2) describe general contextual factors;

NOTE Contextual factors have considerable influence on impact analysis. They can be at the organization level (e.g., the role of the organization in the supply chain), at the system level (e.g., a cloud provider will be involved), or at the PII principal level (e.g., PII is collected in a certain context); and

3) describe specific PII, PII processing and unique contextual factors.

NOTE 5 Unique contextual factors can include mandated privacy controls (inherited from a domain, imposed internally, or exported to another domain).

4) iterate the "analyse risk activity" of the risk management process;

5) evaluate the objectives for privacy engineering (see Annex A); and

6) prepare documentation for privacy impact assessment based on ISO/IEC 29134[11] as well as other reference documents.

d) define the system requirements concerning privacy:

1) identify services and functions to support privacy controls.

NOTE 6 Services and functions refer to privacy capabilities.

NOTE 7 A catalogue of privacy services, as defined in the OASIS PMRM, is presented in C.6.

6.8 Architecture definition process

Purpose in ISO/IEC/IEEE 15288

The purpose of the architecture definition process is to generate system architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views.

Additional outcomes for privacy engineering

Successful implementation of the architecture definition process should result in:

a) identified stakeholder privacy concerns being addressed by the architecture;

b) system elements and their interfaces being identified;

c) the impact of privacy related concerns on the architecture being assessed; and

d) privacy risk analysis being updated.

Additional activities and tasks for privacy engineering

ISO/IEC/IEEE 15288 describes the following activities:

— prepare for architecture definition;

© ISO/IEC 2019 – All rights reserved

— develop architecture viewpoints;

— develop models and views of candidate architectures;

— relate the architecture to design;

— assess architecture candidates; and

— manage the selected architecture.

The following additional guidelines are provided:

a) develop architecture viewpoints:

   1) apply privacy design strategies to develop architecture viewpoints;

      NOTE 1 This task can be guided by privacy design strategies[26][29][30]. Four data-oriented strategies (minimize, separate, abstract, hide) as well as four process-oriented strategies (inform, control, enforce, demonstrate) are identified. Table 3 provides examples of privacy controls associated with each privacy design strategy.

      NOTE 2 This task can be guided by privacy threat analysis (see C.3) and mitigation strategies (see C.7).

b) assess architecture candidates:

   1) iterate the "analyse risk activity" of the risk management process;

   2) evaluate the objectives for privacy engineering; and

   3) prepare documentation for privacy impact assessment based on ISO/IEC 29134[11] as well as other reference documents.

Table 3 — Privacy engineering design strategies

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 from becoming public or known.	Encryption Mixing Perturbation (e.g. differential privacy, statistical disclosure control) Unlinking (e.g. through pseudonymization) Attribute based credentials

© ISO/IEC 2019 – All rights reserved

Table 3 *(continued)*

Design strategy		Description	Privacy control examples
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 over 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

6.9 Design definition process

Purpose in ISO/IEC/IEEE 15288

The purpose of the design definition process is to provide sufficiently detailed data and information about the system and its elements to enable an implementation that is consistent with the architectural entities as defined in models and views of the system architecture.

Additional outcomes for privacy engineering

Successful implementation of the design definition process should result in:

a) privacy risk analysis being updated; and

b) privacy controls being identified and specified.

Additional activities and tasks for privacy engineering

ISO/IEC/IEEE 15288 describes the following activities:

— prepare for design definition;

— establish design characteristics and design enablers related to each system element;

— assess alternatives for obtaining system elements; and

— manage the design.

The following additional guidelines are provided:

a) establish design characteristics and design enablers related to each system element:

   1) apply privacy design strategies to develop architecture viewpoints; and

   2) identify the privacy capabilities to be provided by the system.

      NOTE 1 The guidelines provided in ISO/IEC 29151 or ISO/IEC 27018 apply.

      NOTE 2 The selection of privacy measures can be based on catalogues of privacy controls. See C.7 for an example.

© ISO/IEC 2019 – All rights reserved

NOTE 3 Each activity can be supported by a task to reuse knowledge from the repository maintained by the privacy engineering knowledge management process.

NOTE 4 OASIS PMRM[27] can be used in the design definition process. It provides for the development of privacy controls; the definition of the functions and services required to implement the privacy control; and the packaging of the controls into mechanisms that will implement the privacy controls. The mechanisms are also part of the repository maintained by the privacy engineering knowledge management process

b) assess alternatives for obtaining system elements:

   1) iterate the "analyse risk activity" of the risk management process;

   2) evaluate the objectives for privacy engineering (see Annex A);

   3) select privacy and security controls; and

   4) prepare documentation for privacy impact assessment based on ISO/IEC 29134[11] as well as other reference documents.

Figure 8 shows that the design of privacy controls [some controls can be referred to as privacy enhancing technologies (PETs)] is the outcome of three processes:

— system requirements definition;

— architecture definition; and

— design definition.

It also shows that privacy engineering can involve architecture change decisions.

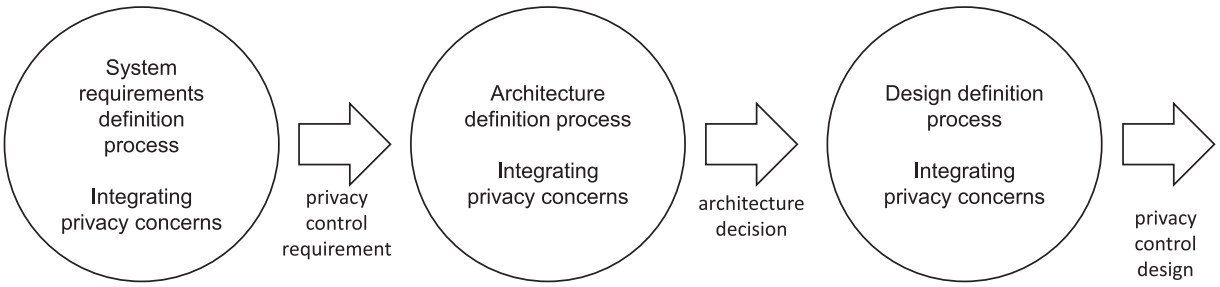

Figure 8 — Design of privacy controls

All the processes leading to the design of privacy controls include risk management activities as shown in Figure 9. Note that the outcome of the three processes can lead to modifications as to how the initial privacy control requirements will be met.

© ISO/IEC 2019 – All rights reserved

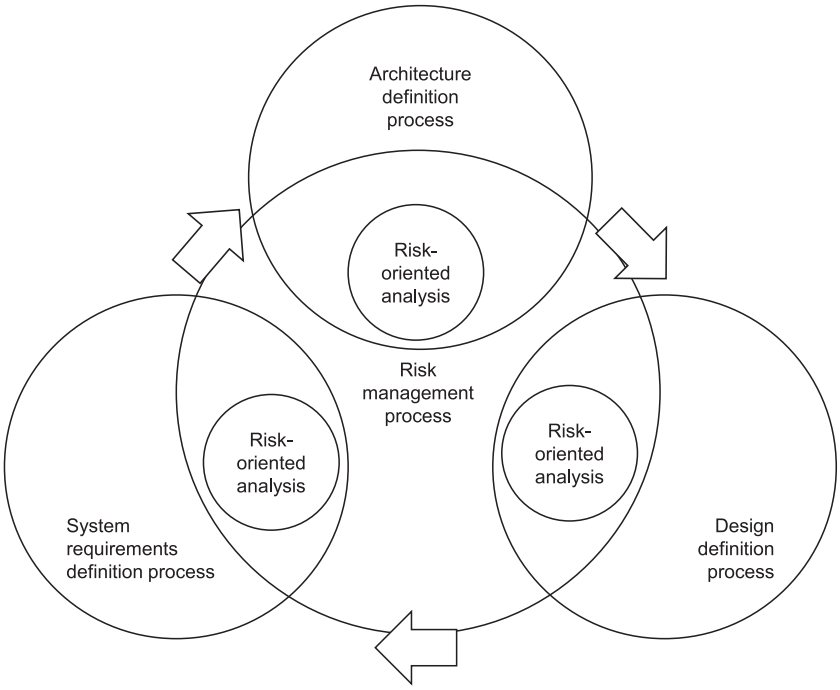

Figure 9 — Design of privacy controls and risk management

© ISO/IEC 2019 – All rights reserved

Annex A
(informative)

Additional guidance for privacy engineering objectives

A.1 NIST Privacy engineering objectives

A.1.1 General

The following privacy engineering objectives are defined by NIST[18] for the purpose of facilitating the development and operation of privacy-preserving systems:

— predictability;

— manageability; and

— disassociability.

These objectives are designed to enable system designers and engineers to build systems that are capable of implementing an organization's privacy goals and support the management of privacy risk.

A.1.2 Predictability

Predictability is about providing a reliable understanding about what is occurring with PII processing within a system. To achieve predictability, organizations need to consider:

— the integration of measures for purpose specification and use limitation: inherent in the rationale for use limitation and purpose specification is the recognition that changes in processing of PII are loci for privacy risk, and that consequently operators need to assess the impact of any changes and target the application of appropriate controls;

— the integration of measures for the treatment of privacy risks associated with PII processing (e.g., operators can implement controls to restrict access to or use of data). They can also consider de-identification controls so that individuals can make reliable assumptions about when a system would reveal certain information about them and when it would not; and

— the integration of measures for transparency: this does not necessarily require that individuals know all the technical details about how a system processes PII. Rather, it is about designing systems such that stakeholders are not surprised by the processing of PII. A range of organizational interpretations of transparency is possible (e.g., a value statement about the importance of open processes, or a requirements-based view that specific information should be shared).

Predictability provides organizations with both precision (in trust) and flexibility (in privacy preserving capability) so that they can design their information systems to support privacy-preserving user relationships.

A.1.3 Manageability

Manageability is about the administration of PII with sufficient granularity so that the right level of control can be applied: only necessary information can be collected or disclosed, inaccurate information can be identified and corrected, and obsolete information can be deleted. To achieve manageability, organizations need to consider the integration of:

— system capabilities to support the general right of individuals to control their information, while minimizing potential conflicts in system functionality. For instance, it can impair the functioning

© ISO/IEC 2019 – All rights reserved

of some systems for individuals to be able to edit or delete information themselves (e.g., fraud detection or proof of eligibility);

— system capabilities to allow appropriately privileged stakeholders to administer changes to maintain accuracy and fair treatment of individuals; and

— specific technical controls such as data tagging[5] or identity management approaches that relate to attribute-based authentication.

Manageability provides organizations with the fine-grained control over data that allows them to implement key privacy principles, including maintaining data quality and integrity, achieving data minimization, and implementing individuals' privacy preferences.

A.1.4 Disassociability

Disassociability is about the ability to actively protect or "blind" an individual's identity or associated activities from unnecessary exposure during transactions. Unlike confidentiality, which is focused on preventing unauthorized access to information, disassociability recognizes that privacy risks can result from exposures even when access is authorized or as a by-product of a transaction. To achieve disassociability, organizations need to consider the integration of:

— privacy risk assessment concerning exposures even when access is authorized or as a by-product of a transaction;

— cryptographic techniques associated with disassociability. This includes techniques for anonymity, de-identification, unlinkability, unobservability, pseudonymity or others; and

— appropriate measures when the exposure risk has been identified. For example, identity proofing or the direct provision of health care services can necessitate the association of information with an individual. Organizations can opt to accept the risk because of the difficulty in implementing appropriate controls or institute other compensating controls.

Disassociability advances the capabilities of a privacy-preserving system by engaging system designers and engineers in a deliberate consideration of the risks to an individual's identity or associated activities.

A.2 ULD Privacy protection goals

A.2.1 General

Privacy protection goals are defined by ULD[23] with a rationale to extend the classic security protection goals of confidentiality, integrity and availability[6]. Three further goals are defined:

— unlinkability;

— transparency; and

— intervenability.

The resulting privacy and security protection goals (unlinkability, transparency, intervenability, confidentiality, integrity and availability) are attributes that can be used to guide a number of privacy engineering processes such as privacy impact assessment, or the design of privacy controls.

---

5) Associating a term with a piece of information. Data can also be "tagged" with properties that indicate what processing operations (e.g., read, edit, store, print) are authorized for that data.

6) ULD work on privacy protection goals has been influenced by earlier terminology work on data minimization[39].

© ISO/IEC 2019 – All rights reserved

A.2.2 Unlinkability

Unlinkability ensures that a PII principal can make multiple uses of resources or services without others being able to link these uses together. The objective of unlinkability is to minimize the risk to privacy created by the potential linking of separate sets of PII, for instance:

— a customer uses two different accounts for navigation and for telephone calls; or

— a customer uses two different accounts for the same hotel booking service.

Unlinkability is a key property:

— for the data minimization principle as it separates PII from the related PII principals; and

— for the purpose legitimacy and specification principle as it separates PII sets belonging to different purposes.

When full unlinkability cannot be achieved, measures should be taken so that linking requires disproportionate effort for the entity establishing such linkage. Examples of measures for achieving and enhancing unlinkability comprise data avoidance, separation of contexts by different identifiers, pseudonymization mechanisms, anonymization mechanisms, and early erasure.

A.2.3 Transparency

Transparency ensures that an adequate level of clarity of the processes in privacy-relevant data processing is reached so that the processing of the information can be understood and reconstructed at any time. The objective is to allow involved parties (e.g., PII principals, PII controllers and PII processors) to know the risks to privacy (e.g., the processing of health data or location data) and have sufficient information on countermeasures, how to employ them and what limitations they have.

Transparency covers the entire system life cycle. It needs to cover not only the actual processing, but also the planned processing (ex-ante transparency) and the time after the processing has taken place to know what exactly happened (ex-post transparency). Transparency also involves all parties (i.e., PII principals, PII controllers, PII processors as well as supervisory authorities):

— transparency allows the PII principal to understand the specified PII required for the specified purpose, the specified purpose for PII collection, the specified processing (including collection, communication and storage mechanisms), and the consequences of such processing (e.g., in case of profiling), the types of authorized natural persons who will access the PII and to whom the PII can be transferred, and the specified PII data retention and disposal requirements;

— transparency allows PII controllers and associated PII processors to reconstruct and improve legal, technical and organizational controls in case it is needed, for instance when there is a privacy breach; and

— transparency allows supervisory authorities to reconstruct the PII processing activities of an organization. This allows the supervisory authority to properly exercise its supervisory responsibilities, including investigating breaches, auditing organizational practices, and making recommendations to the organization for improvements to those practices.

Examples for achieving or enhancing transparency comprise reporting mechanisms, understandable documentation covering technology, organization and responsibilities, source code, privacy policies, and communication with the PII principal.

A.2.4 Intervenability

Intervenability ensures that PII principals, PII controllers, PII processors and supervisory authorities can intervene in all privacy-relevant data processing. Note there can be legislative or regulatory limitations on the extent to which a data subject or supervisory authority can intervene in data

 © ISO/IEC 2019 – All rights reserved

processing. Intervenability can involve the application of corrective measures and counterbalances where necessary, including:

— PII principals can request data erasure or withdraw consent. Intervenability also addresses the PII principal's right to lodge a complaint or to raise a dispute to achieve a remedy (e.g., in the event of a breach);

— PII controllers can require PII processors to apply corrective measures for better protection. Intervenability addresses the PII controller's need to effectively control the PII processor and the IT systems being used by the processor to influence or stop the data processing at any time; and

— supervisory authorities can intervene by requesting or enforcing the blocking, erasure or destruction of data or even shutting off the system.

Mechanisms for achieving or enhancing intervenability include processes for influencing or stopping the data processing fully or partially, manually overturning an automated decision, data portability precautions to prevent lock-in at a PII processor, breaking glass policies, single points of contact for data subjects' intervention requests, switches for users to change a setting (e.g., changing to a non-personalized, empty-profile version of a search engine or recommendation system), or deactivating an auto pilot or a monitoring system for some time.

A.2.5 Confidentiality

Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. The objective of confidentiality is to prevent PII from reaching the wrong people, for instance preventing banking account data or location data being accessed by potential burglars.

Examples of measures for achieving or enhancing confidentiality include protected transmission of collected data, protected access with suitable authentication schemes, protected processing of data, and protected storage.

A.2.6 Integrity

Integrity ensures the accuracy and completeness of data over its entire life cycle. The objective of integrity is to prevent PII from being altered in unauthorized ways or by unauthorized entities, for instance the transfer of erroneous health data.

Examples of measures for achieving or enhancing integrity include schemes such as digital signatures.

A.2.7 Availability

Availability ensures accessibility and usability if an authorized entity requires it. The objective of availability is to provide information when it is needed, for instance the next arrival at a bus stop.

Examples of measures for achieving or enhancing availability include preventing service disruptions due to power outages, hardware failures, or security denial of service attacks using schemes such as redundant systems.

© ISO/IEC 2019 – All rights reserved

Annex B
(informative)

Additional guidance for privacy engineering practice

B.1 Applicability to domains and ecosystems

Practicing privacy engineering properly is a challenge. Figure B.1 shows examples of ecosystems (e.g., smart cities, IoT, big data), domains (e.g., smart grids, health, transport) and concerns (privacy, security, safety) that need to be taken into account.

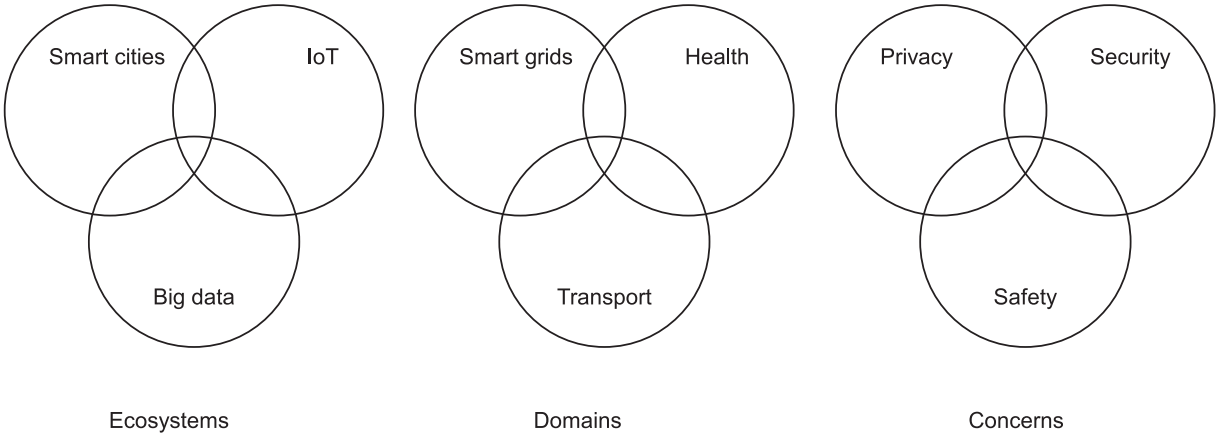

Figure B.1 — Examples of ecosystems, domains and concerns

The following stakeholders can be involved:

— public authorities:

  — supervisory authorities,

  — local authorities (e.g., a city, a region);

— operators: organizations which operate the systems involving PII processing, for instance a navigation application, or a mobile network. There are two types of operators, PII controllers and PII processors. The PII processor has some contractual relationship with the PII controller;

— suppliers: organizations which develop the systems and subsystems that will be used by the operators;

  — the suppliers of systems (e.g., a complete transport application) are aware of the PII processing activities of their systems, and therefore know the purpose for which PII is processed; and

  — suppliers to subsystems (e.g., a storage system, a traffic sensor device, a user interface subsystem) may not be aware of the purpose for which some PII can be processed when they design the subsystem they supply.

Examples of the privacy management duties of these stakeholders are described in Table B.1.

© ISO/IEC 2019 – All rights reserved

Table B.1 — Stakeholders privacy management practices

Example of stakeholders	Examples of duties
Public authority	Compliance check
Operator	Privacy impact assessment
Supplier of system	Privacy engineering for end-to-end system (awareness of purpose)
Supplier of subsystem	Privacy engineering for sub-system (may not be aware of purpose)

Suppliers of systems and subsystems should follow the guidelines provided in Clause 6. Further guidance is provided in Table B.2 and Table B.3.

Table B.2 — Additional guidance for suppliers of systems

Privacy engineering	High level guidelines
In the acquisition process	Where the supplier integrates subsystems, it should request documentation on the privacy controls that the suppliers of these subsystems are providing
In the supply process	Provide compliance documents to operator Provide information to operator on the supply chain, on the roles and duties of each stakeholder in the supply chain, and on the privacy controls that are provided by each stakeholder in the supply chain
In the human resources management process	Implement a fully-fledged privacy engineering competency/skill program
In the knowledge management process	Implement a fully-fledged knowledge management program — Inventory of design strategies and privacy controls — Inventory of architecture decisions associated with privacy controls — Architecture design practices — Architecture evaluation practices — Inventory of privacy patterns — Inventory of supplier products with privacy control support features — Privacy control usage lessons learned
In the risk management process	Implement a fully-fledged privacy risk management for the entire system
In the stakeholders' needs and requirements definition process	Carry out an analysis to understand the supply chain and the roles and duties of each stakeholder in the supply chain
In the system requirements definition process	Implement a fully-fledged design management program to integrate privacy engineering throughout the entire system lifecycle
In the architecture definition process	
In the design definition process	

© ISO/IEC 2019 – All rights reserved

Table B.3 — Additional guidance for suppliers of subsystems

Privacy engineering concerns	High level guidelines
In the acquisition process	Where the subsystem supplier further integrates subsystems into its own subsystem, it should request documentation on the privacy controls that the suppliers of these subsystems are providing
In the supply process	Provide documentation on the privacy controls that the subsystem supplier is providing, including the privacy controls that the subsystem supplier has integrated from other subsystems suppliers.
In the human resources management process	Implement a competency/skill program related to the privacy controls that the supplier is supporting
In the knowledge management process	Implement a knowledge management program related to the privacy controls that the supplier is supporting — Inventory of features — Inventory of architecture decisions related to privacy controls — Inventory of privacy control support features — Customer usage lessons learned
In the risk management process	Implement risk management for subsystems related to the privacy controls that the supplier is supporting
In the stakeholders' needs and requirements definition process	No additional guidance to Clause 6
In the system requirements definition process	Implement a design management program for entire system related to the privacy controls that the supplier is supporting
In the architecture definition process	
In the design definition process	

B.2 Applicability to software environments

B.2.1 Agile programming

The term agile has been used in the last 15 years in software development to promote adaptive planning, evolutionary development, early delivery, and continuous improvement. Agile development encourages rapid and flexible response to change. As stated by Jim Highsmith[7]:

The Agile movement is not anti-methodology, in fact many of us want to restore credibility to the word methodology. We want to restore a balance. We embrace modelling, but not in order to file some diagram in a dusty corporate repository. We embrace documentation, but not hundreds of pages of never-maintained and rarely-used tomes. We plan, but recognize the limits of planning in a turbulent environment.

7) http://agilemanifesto.org/history.html

© ISO/IEC 2019 – All rights reserved

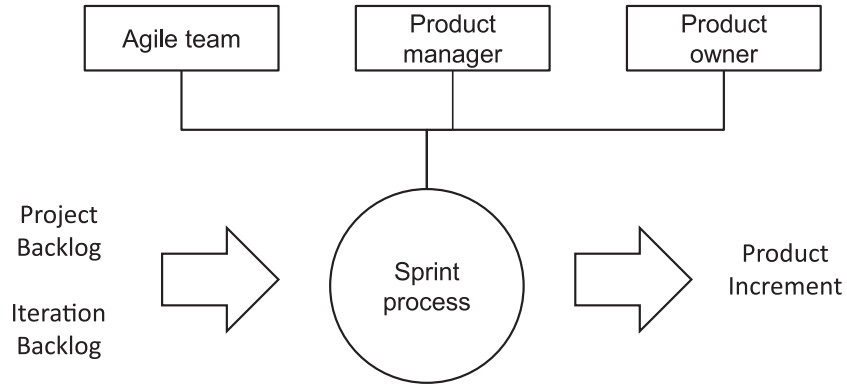

Figure B.2 — Agile programming

Figure B.2 shows the principles of agile programming: product development is carried out in short periods called sprints. The objectives of sprints are agreed by the agile programming team (e.g., engineers who apply the agile approach), the product manager and the product owner. The result of a sprint is executable and can be demonstrated. It can therefore be assessed by both the product owners and managers. Pending work that is not mature and therefore not yet integrated in the product is managed through project and iteration backlogs.

Figure B.3 shows the difference between conventional programming and agile programming. Lifecycle processes in conventional programming are carried out in sequence (e.g., A followed by B followed by C), while in agile programming each sprint process can contribute to an incremental outcome of A, B and C.

Consequently, processes described in Clause 6 can be applied to both conventional programming and to agile programming by clearly identifying the incremental outcome that has been achieved during a given sprint process.

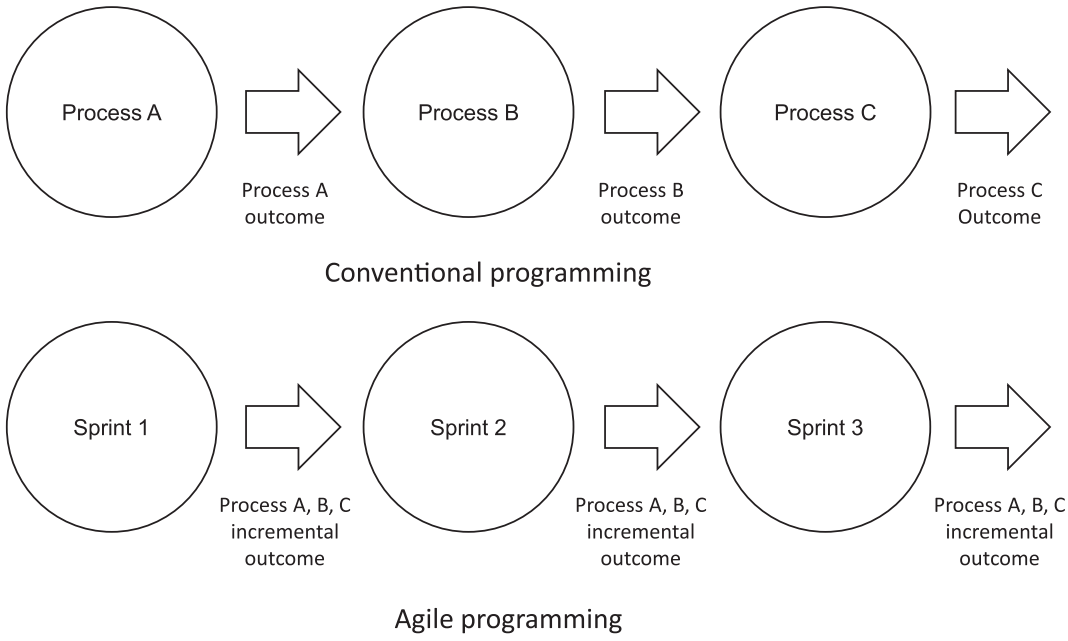

Figure B.3 — Conventional programming vs agile programming

Figure B.4 shows how privacy engineering can be integrated into agile programming:

— privacy concerns are added to the system under development;

© ISO/IEC 2019 – All rights reserved

— a product privacy owner is added to the team. The product privacy owner is a member of the chief privacy officer team or a member of another organization that is responsible for privacy within the organization; and

— the project backlogs and iteration backlogs integrate development plans for privacy.

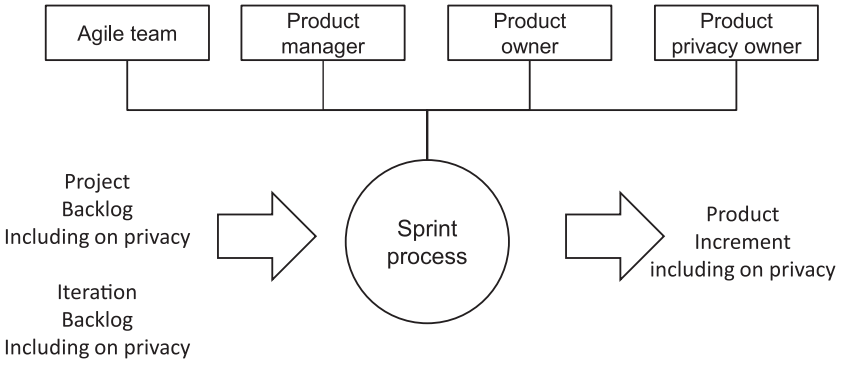

Figure B.4 — Integration of privacy engineering in agile programming

It should be noted that ISO/IEC/IEEE 15288 does not necessarily call for sequential processes. For instance, the privacy risk management process shown in Figure 9 runs parallel to three technical processes: the privacy principle operationalization process, the privacy architecture definition process and the privacy design definition process. Additional guidelines for agile programming are shown in Table B.4.

Table B.4 — Additional guidance for agile programming

Privacy engineering concerns	High level guidelines
In the acquisition process (from suppliers)	No additional guidance to 6.2
In the supply process (to operators)	No additional guidance to 6.2
In the human resources management process	No additional guidance to 6.3
In the knowledge management process	Add requirements for agile programming expertise
In the risk management process	Ensure that sprint processes will include incremental outcomes on privacy that will contribute to the desired outcome of the following processes: — risk management process — system requirements definition process — architecture definition process — design definition process — outcome, on requirements, architecture and design The rationale is that any change in requirements, architecture and design can have an impact on risks, which in turn will have an impact on the requirements, architecture and design

© ISO/IEC 2019 – All rights reserved

Table B.4 *(continued)*

Privacy engineering concerns	High level guidelines
In the stakeholders' needs and requirements definition process	Integrate in the agile team a privacy product owner
In the system requirements definition process	Ensure the following constraints: — the final outcome of the privacy principles operationalization process needs to be synchronized with the final outcome of the requirements process — the final outcome of the privacy engineering architecture definition process needs to be synchronized with the final outcome of the architecture definition process — the final outcome of the privacy engineering design definition process needs to be synchronized with the final outcome of the design definition process
In the architecture definition process	
In the design definition process	

B.2.2 Support for small organizations

The ISO/IEC 29110 series[4] is of particular interest when small enterprises are involved. A very small entity (VSE) is an entity (enterprise, organization, department or project) having up to 25 people.

The ISO/IEC 29110 series is intended for organizations which view ISO/IEC/IEEE 15288 as too complex. ISO/IEC/IEEE 15288 defines 30 processes while in contrast, ISO/IEC 29110 defines two processes:

— the project management process, with the following activities:
  — planning;
  — execution;
  — evaluation;
  — and closure;
— the implementation process, with the following activities:
  — initiation;
  — analysis;
  — design;
  — construction;
  — integration and test; and
  — delivery.

To cope with the large diversity of VSEs, the following options are defined:

— system engineering or software engineering;

— profile groups representing domains (at this point only one profile group, the generic profile group, has been defined); and

— profiles. Four profiles are defined:
  — entry profile;

© ISO/IEC 2019 – All rights reserved

— basic profile;

— intermediate profile; and

— advanced profile.

The resulting integration of privacy engineering in ISO/IEC 29110 is described in Table B.5.

Table B.5 — VSE processes and activities

Category	System life cycle artefacts (ISO/IEC 29110)	Privacy engineering artefact
Acquirer	Statement of work	Statement of work
	Product	Product with privacy capabilities
Organizational management	External entity	External entity
Project management process	Risk management activity	Privacy risk management activity
System definition and realization process	System definition and realization initiation	Stakeholders privacy expectations activity
	System requirements engineering	Privacy principles operationalization activity
	System architectural design	Privacy engineering architecture activity Privacy engineering design definition activity
	System construction activity	—

© ISO/IEC 2019 – All rights reserved

Annex C
(informative)

Catalogues

C.1 General

The purpose of this annex is to provide examples of catalogues that can be useful to carry out privacy engineering activities. The catalogues are not meant to be comprehensive and other references including future standards can augment or replace them. These catalogues should be maintained within the knowledge management process described in 6.4.

C.2 PII processing risks

This catalogue of PII processing risks is based on NISTIR 8062[18]. It should be used in the privacy risk management process to identify privacy risk sources.

NOTE NISTIR 8062[18] uses the term data action instead of PII processing

Table C.1 — PII processing risks

Appropriation	Personal information is used in ways that exceed an individual's expectation or authorization. *Appropriation* occurs when personal information is used in ways that an individual would object to or would have expected additional value for, absent an information asymmetry or other marketplace failure. Privacy harms that *Appropriation* can lead to include loss of trust, economic loss or power imbalance.
Distortion	The use or dissemination of inaccurate or misleadingly incomplete personal information. *Distortion* can present users in an inaccurate, unflattering or disparaging manner, opening the door for discrimination harms or loss of liberty.
Induced disclosure	Pressure to divulge personal information. *Induced disclosure* can occur when users feel compelled to provide information disproportionate to the purpose or outcome of the transaction. *Induced disclosure* can include leveraging access or privilege to an essential (or perceived essential) service. It can lead to harms such as power imbalance or loss of autonomy.
Insecurity	Lapses in data security. Lapses in data security can result in a loss of trust, as well as exposing individuals to economic loss, and stigmatization.
Surveillance	Tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service. The difference between the PII processing of monitoring and the problematic PII processing of surveillance can be very narrow. Tracking user behaviour, transactions or personal information may be conducted for operational purposes such as protection from cyber threats or to provide better services, but it becomes surveillance when it leads to harms such as power imbalance, loss of trust or loss of autonomy or liberty.
Unanticipated revelation	Non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways. *Unanticipated revelation* can arise from aggregation and analysis of large and/or diverse data sets. *Unanticipated revelation* can give rise to stigmatization, power imbalance and loss of trust and autonomy.
Unwarranted restriction	*Unwarranted restriction* to personal information includes not only blocking tangible access to personal information, but also limiting awareness of the existence of the information within the system or the uses of such information. Such restriction of access to systems or personal information stored within that system can result in harms such as exclusion, economic loss and loss of trust.

© ISO/IEC 2019 – All rights reserved

C.3 Privacy threats

LINDDUN[25] provides a catalogue of privacy threats[8] which can be used in a privacy risk management process to identify privacy risk sources. The catalogue is based on the following:

— A data flow diagram (DFD) describes the system. This description is typically specified in the system requirements definition process (see Clause 6). A DFD consists of a structured, graphical representation of the system based on four building blocks:

  — entities;

  — data stores;

  — data flows; and

  — processes.

Figure C.1 shows an example of a DFD for a social network where the social network user is a DFD entity, the social network data is a DFD data store, and the social network portal and associated service are processes.

— A categorization based on the LINDDUN mnemonic (Table C.2). This is the counterpart of the STRIDE mnemonic for security threats[37].

— Each pair [threat category, building block] is associated with a privacy threat tree. Figure C.2 shows the privacy threat tree for the pair "[linkability, entity]":

  — it includes "and/or" nodes. For instance, the "linkable login using untrusted communication" threat is an "and" node consisting of the "linkable login" and the "untrusted communication" threats;

  — it includes other threat trees. For instance, the "[Linkability, data store]" and "[Information disclosure, data flow]" threat trees are part of the "[linkability, entity]" threat tree; and

  — it includes subtrees from other threat trees (e.g., the "linkability of contextual data" subtree of the "[linkability, data flow]" threat tree).

In the social network example of Figure C.1, one threat associated with the "user" entity can be its "linkability". In the "[linkability, entity]" tree of Figure C.2 the "untrusted communication" threat is either:

— an "[information disclosure, data flow]" threat;

— an "untrusted receiver" threat"; or

— a "[linkability, data store]" threat.

8) The most recent version of this catalogue is available on the LINDDUN website[25].

© ISO/IEC 2019 – All rights reserved

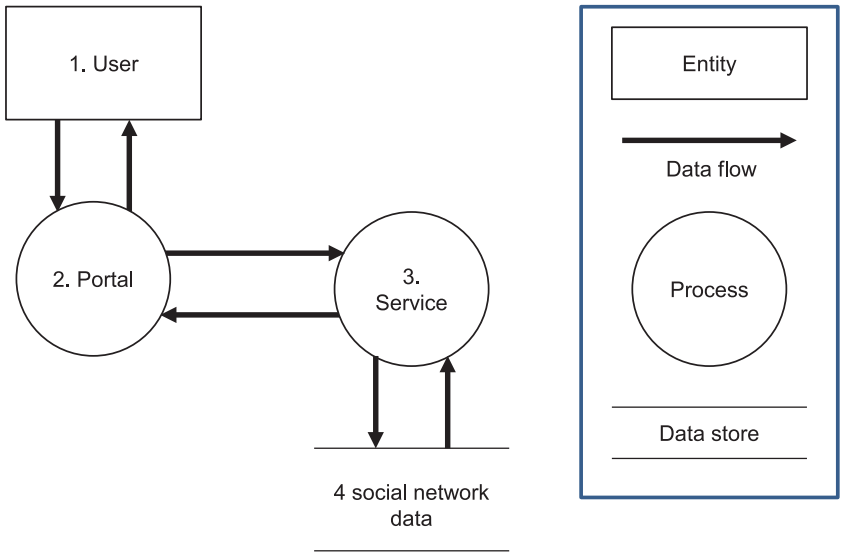

Figure C.1 — Example of a data flow diagram for a social network

Table C.2 — Privacy threat categories

Type	Property	Privacy threat	Privacy threat description
Hard privacy	Unlinkability	Linkability	Establishing the link between two or more actions, identities, and pieces of information.
	Anonymity	Identifiability	Establishing the link between an identity and an action or a piece of information
	Plausible deniability	Non-repudiation	Inability to deny having performed an action that other parties can neither confirm nor contradict
	Undetectability and unobservability	Detectability	Detecting the PII principal's activities
Security	Confidentiality	Disclosure of information	Disclosing the data content or controlled release of data content
Soft privacy	Content awareness	Unawareness	PII principals being unaware of what PII about them is being processed
	Policy and consent compliance	Non compliance	PII controller fails to inform the data subject about the system's privacy policy, or does not allow the PII principal to specify consents in compliance with legislation

© ISO/IEC 2019 – All rights reserved

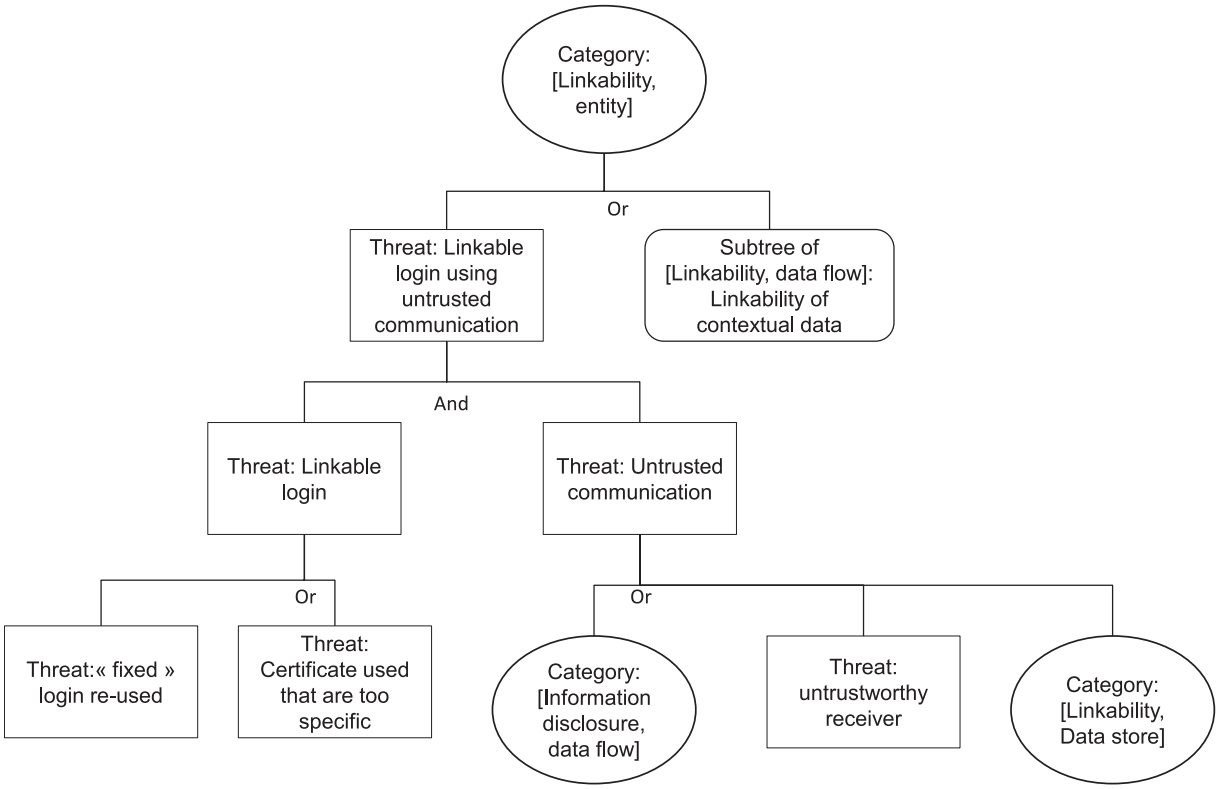

Figure C.2 — Example of privacy threat tree[25]

C.4 Risks to individuals

This catalogue of risks to individuals is based on NISTIR 8062[18]. It is used in the privacy risk management process to identify the consequences of privacy risks to the PII principals' privacy.

Table C.3 — Risks to individuals

Loss of self determination	Loss of autonomy	Loss of autonomy includes needless changes in behaviour, including self-imposed restrictions on freedom of expression or assembly.
	Exclusion	Exclusion takes place when individuals are systematically blocked from (or denied full access to) various rights, opportunities and resources that are normally available to members of a different group, and which are fundamental to social integration within that particular group.
	Loss of liberty	Improper exposure to arrest or detainment. Even in democratic societies, incomplete or inaccurate information can lead to arrest, or improper exposure or use of information can contribute to instances of abuse of governmental power. More life-threatening situations can arise in non-democratic societies.
	Physical harm	Actual physical harm to a person.

© ISO/IEC 2019 – All rights reserved

Table C.3 *(continued)*

Discrimination	Stigmatization	Personal information is linked to an actual identity in such a way as to create a stigma that can cause embarrassment, emotional distress or discrimination. For example, sensitive information such as health data or criminal records or merely accessing certain services such as food stamps or unemployment benefits may attach to individuals creating inferences about them.
	Power imbalance	Acquisition of personal information that creates an inappropriate power imbalance, or takes unfair advantage of or abuses a power imbalance between acquirer and the individual. For example, collection of attributes or analysis of behaviour or transactions about individuals can lead to various forms of discrimination or disparate impact, such as differential pricing or the improper association of the PII principal to a cohort of individuals barred from accessing home mortgage loans.
Loss of trust		Loss of trust is the breach of implicit or explicit expectations or agreements about the handling of personal information. For example, the disclosure of personal or other sensitive data to an entity is accompanied by a number of expectations for how that data is used, secured, transmitted, shared, etc. Breaches can leave individuals reluctant to engage in further transactions.
Economic loss		Economic loss can include direct financial losses as the result of identity theft or the failure to receive fair value in a transaction involving personal information

C.5 Examples of privacy controls

A reference catalogue which can be used is found in ISO/IEC 27552. The catalogue of privacy controls below is based on NIST Special Publication 800-53 rev4[34]. Such catalogues, including those provided in ISO/IEC 29100, ISO/IEC 27018, and ISO/IEC 29151 should be used in the design definition process to identify and specify privacy controls.

Table C.4 — Examples of privacy controls

Category	Privacy controls
Authority and purpose	Authority to collect
	Purpose specification
Accountability, audit, and risk management	Governance and privacy program
	Privacy impact and risk assessment
	Privacy requirements for contractors and service providers
	Privacy monitoring and auditing
	Privacy awareness and training
	Privacy reporting (to demonstrate accountability)
	Privacy-enhanced system design and development
	Accounting of disclosures
Data quality and integrity	Data quality
	Data integrity
	Data integrity board
Data minimization and retention	Minimization of PII
	Data retention limitations
	Disposal schedules
	Minimization of PII used in testing, training and research

© ISO/IEC 2019 – All rights reserved

Table C.4 *(continued)*

Category	Privacy controls
Individual participation and redress	Consent
	Individual access
	Redress
	Complaint management
Security	Inventory of PII
	Privacy incident response
Transparency	Privacy notice
	Transparency reporting
	Dissemination of privacy program information
Use limitation	Internal use limitations
	Information sharing agreements with third parties

C.6 Privacy management services

This catalogue of privacy management services is based on OASIS PMRM[27]. It is used in operationalization of privacy principles operationalization and privacy control requirements.

Table C.5 — Privacy management services

Service		Purpose	Description
Core policy services	Agreement	Manages and negotiates permissions and rules	Defines and documents permissions and rules for the handling of PII based on applicable policies, data subject preferences, and other relevant factors; provides relevant Actors with a mechanism to negotiate, change or establish new permissions and rules; expresses the agreements such that they can be used by other services
	Usage	Controls PII use	Ensures that the use of PII complies with the terms of permissions, policies, laws, and regulations, including PII subject to information minimization, linking, integration, inference, transfer, derivation, aggregation, anonymization and disposal over the lifecycle of the PII

© ISO/IEC 2019 – All rights reserved

Table C.5 *(continued)*

Service		Purpose	Description
Privacy assurance services	Validation	Ensures PII quality	Evaluates and ensures the information quality of PII in terms of accuracy, completeness, relevance, timeliness, provenance, appropriateness for use and other relevant qualitative factors
	Credential certification	Ensures appropriate management of credentials	Ensures that the credentials of any actor, domain, system, or system component are compatible with their assigned roles in processing PII and verifies their capability to support required privacy controls in compliance with defined policies and assigned roles.
	Enforcement	Monitors proper operation, responds to exception conditions and reports on demand evidence of compliance where required for accountability	Initiates monitoring capabilities to ensure the effective operation of all services. Initiates response actions, policy execution, and recourse when audit controls and monitoring indicate operational faults and failures. Records and reports evidence of compliance to stakeholders and/or regulators. Provides evidence necessary for accountability.
	Security	Safeguards privacy information and operations	Provides the procedural, organizational and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PII; makes possible the trustworthy processing, communication, storage and disposition of PII; ensures that the operational functionalities provided by other Services are protected to maintain their reliability and trustworthiness
Presentation and lifecycle services	Interaction	Provides Information presentation and communication functionality	Provides generalized interfaces necessary for presentation, communication, and interaction of PII and relevant information associated with PII, encompassing functionality such as user interfaces, system-to-system information exchanges, and agents
	Access	Enables viewing and proposing changes to PII	Enables PII principals, as required and/or allowed by permission, policy, or regulation, to review their PII that is held or processed within a domain and to propose changes, corrections or deletion for their PII

C.7 Mitigation strategies and privacy measures

This catalogue of mitigation strategies and privacy measures is based on LINDDUN[40]. It is used in the privacy engineering design process to identify potential privacy and security controls.

The catalogue is based on the taxonomy of privacy risk treatments shown in Figure C.3. The taxonomy is based on two main categories:

— measures which control associations between PII principals, their transactions and PII in order to ensure that the PII principal shares as little information as necessary with the system. These are proactive measures;

— measures which aim at limiting damage by controlling associations after disclosure. To achieve this, the exposure of these associations needs to be restricted to the minimum. These are reactive measures.

© ISO/IEC 2019 – All rights reserved

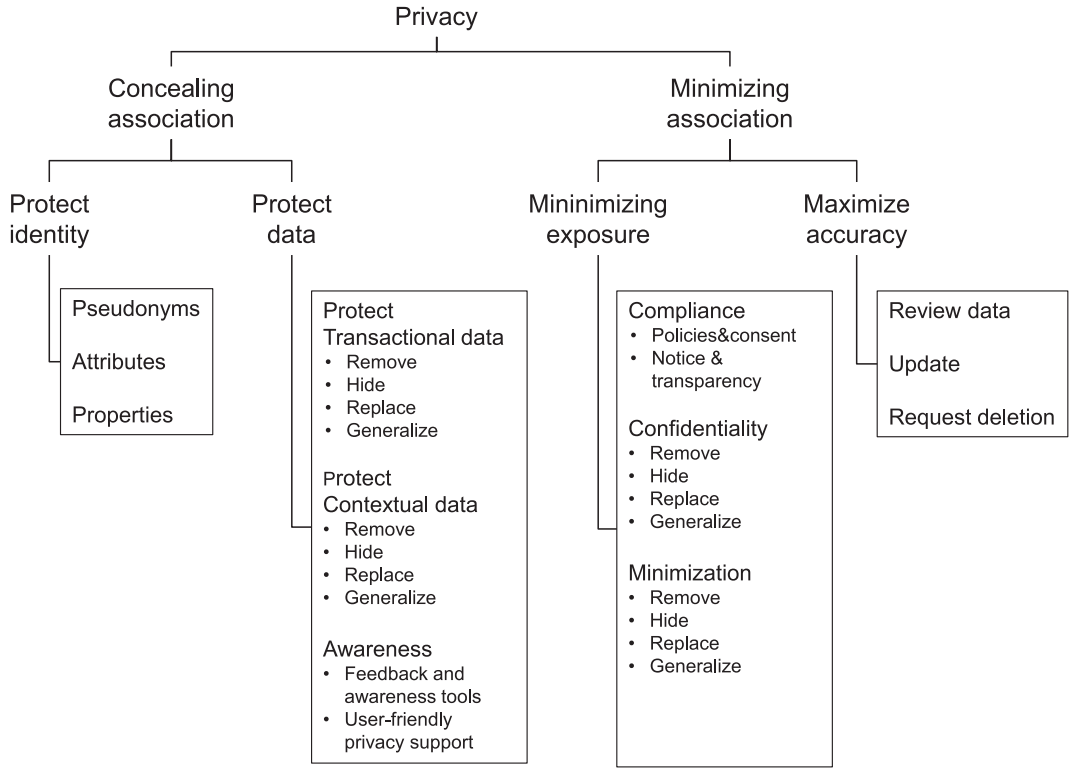

Figure C.3 — Taxonomy of privacy risk treatment measures

In the taxonomy, concealing the association is further divided into two categories:

— protect identity: protect the identity of the PII principal during authentication. This can be achieved through:

  — pseudonyms (i.e., an alias instead of the real identity);

  — attributes (such as a certificate); and

  — properties, using anonymous credentials or other zero-knowledge proofs as authentication mechanisms;

— protect data: this can be achieved through:

  — measures to protect transactional data (e.g., transferred data) and contextual data (e.g., meta data related to transferred data). Strategies to protect data include removing the (sensitive) information, hiding the data, replacing (part of) the information or generalizing it; and

  — measures to raise awareness regarding the sharing of information such as feedback and awareness tools or user-friendly privacy support to help manage privacy settings.

In the taxonomy, minimizing the association is further divided into two categories:

— minimizing exposure of PII by applying measures:

  — to obtain data protection compliance which are related to consent and policies, and notice and transparency;

  — to ensure confidentiality which correspond to security measures such as access control and data encryption; and

© ISO/IEC 2019 – All rights reserved

  - to minimize data collected.
- maximizing the accuracy of PII by applying measures:
  - allowing PII principals easy access to the collected data about themselves in order to review the data; and
  - allowing the PII principal to request updates or even deletion of PII.

Table C.6 — Privacy measures

Taxonomy				Privacy measures[a]
Protect identity	Pseudonyms			Privacy enhancing identity management systems User controlled identity management systems
	Attributes			Privacy preserving biometrics Private authentication
	Properties			Anonymous credentials
Protect data	Transactional data	Remove		Data removal tools (e.g., spyware removal, browser cleaning tools, activity traces eraser, hard disk data eraser)
		Hide	Data-flow specific	Multi-party computation (secure function evaluation) Anonymous buyer-seller watermarking protocol
			General	Symmetric and public key encryption, deniable encryption, homomorphic encryption, verifiable encryption
		Replace		Data masking
		Generalize		K-anonymity, I-diversity
	Contextual data	Remove		Mix-networks, ISDN-mixes, onion routing, Tor
		Hide	General	Crowds, low-latency communication, Java anonymous proxy
			Undetectability	Steganography, covert communication, spread spectrum
			Repudiability	Deniable authentication, off-the record messaging
		Replace		Single proxy, anonymous remailer
		Generalize	Undetectability	Dummy traffic, DC-networks
	Awareness	Feedback and awareness tools		Feedback tools for user privacy awareness
		User-friendly privacy support		See protect data – transactional data – remove

[a] The table represents work in progress and therefore some entries are empty.

© ISO/IEC 2019 – All rights reserved

Table C.6 *(continued)*

Taxonomy				Privacy measures[a]
Minimize exposure (of data, associations, and so on)	Compliance	Policies and consent		Policy communication, policy enforcement, consent management
		Notice and transparency		
	Confidentiality	Encryption		See protect data – transactional data – hide - general
		Access control		Context-based access control, privacy-aware access control
	Minimization	Remove		
		Hide	Receiver privacy	Private information retrieval, oblivious transfer
			Database privacy	Privacy preserving data mining, searchable encryption, private search
			General	See minimize exposure – confidentiality – encryption
		Replace		
		Generalize		K-anonymity model, I-diversity
Maximize accuracy	Review data			
	Update/request deletion			

[a] The table represents work in progress and therefore some entries are empty.

© ISO/IEC 2019 – All rights reserved

Annex D
(informative)

Examples of risk models and methodologies

D.1 General

This annex provides a description of the risk models developed by NIST[18] and by CNIL[35]. The two risk models are described using Figure 3

NOTE The described risk models include a series of assumptions and mappings from qualitative to quantitative scales, including an arbitrary numerical transformation from a multidimensional to a one-dimensional scale, which means they are a priori not comparable. Other models can be adopted by organizations.

D.2 NIST privacy risk analysis

NIST uses a risk model where the focus in terms of risk source[9] is the problematic data action[10] where:

Privacy risk level	=	Likelihood of a problematic data action	×	Impact of problematic data action

— Likelihood is assessed as the probability that a data action will become problematic for a PII principal whose PII is being processed by the system; and

— Impact is defined as the magnitude of the problematic data action on the individual if it occurs. Given that it may be extremely difficult to assess the impact of a problematic data action on an individual (or individuals), organizational impact factors may be used as proxies to help account for individual impact. Four organizational impact factors are defined:

  — non compliance cost;

  — direct cost;

  — reputational cost; and

  — internal culture cost.

The risk assessment includes the following steps:

— frame the business objectives and organizational privacy governance related to the system;

— assess system design by mapping the data actions within the system and PII associated with each data action, then cataloguing associated contextual factors and summary issues[11];

— identify the problematic data actions and potential problems for individuals (see C.4) associated with each summary issue;

9) Or risk factor.

10) NISTIR 8062[18] uses the term data action instead of PII processing. Table C.1 provides a non-exhaustive set of problematic data actions.

11) Examples of contextual factors are: “organization will use specific supplier”, “PII principal is technically sophisticated”. An example of summary issue is “access to extended PII principal profile data”.

© ISO/IEC 2019 – All rights reserved

— evaluate the likelihood that a data action will become problematic for a representative or typical individual whose PII is being processed by the system. This can be represented by a value from 1 (low likelihood) to 10 (high likelihood), or by a different categorization preferred by the organization;

Likelihood of problematic data action (1–10)

— evaluate the impact of a data action creating a risk for a representative or typical individual whose PII is being processed by the system, calculated as the sum of the effect of each impact factor (for example, non-compliance cost, direct cost, reputational cost, internal culture cost). Each effect is represented by a value, which can be from 1 (low effect) to 10 (high effect), or a different categorization preferred by the organization;

Impact of a specific problem to individuals of a problematic data action internalized as costs to organizations (1–40)	=	Non-compliance cost (1-10)	+	Direct cost (1–10)	+	Reputational cost (1–10)	+	Internal culture cost (1–10)

NOTE An organization can request to add other factors. In that case, the range of values can change (e.g., from 1 to 50)

— calculate the risk per potential problem to individuals of a problematic data action as a value ranging from 1 to 400;

Risk of potential problem to individuals of a problematic data action (1–400)	=	Likelihood of problematic data action (1–10)	X	Impact of specific problem to individuals of a problematic data action (1–40)

— calculate the risk of a problematic PII processing as the sum of all the risks per potential problem to individuals of a problematic PII processing;

Risk of a problematic data action (*N*–*N**400)	=	Risk of potential problem 1 to individuals of a problematic data action (1–400)	+	Risk of potential problem 2 to individuals of a problematic data action (1–400)	+	…	+	Risk of potential problem *N* to individuals of a problematic data action (1–400)

[a] *N* is the number of problems to individuals identified for a problematic PII processing.

© ISO/IEC 2019 – All rights reserved

— analyse the risks:

  — compare and rank the risk of each problematic data action; and

  — present the risks on a risk map (see, for example, Figure D.1) with one dimension representing the likelihood of a data action becoming problematic for an individual and the other dimension representing the impact of a data action becoming problematic for an individual.

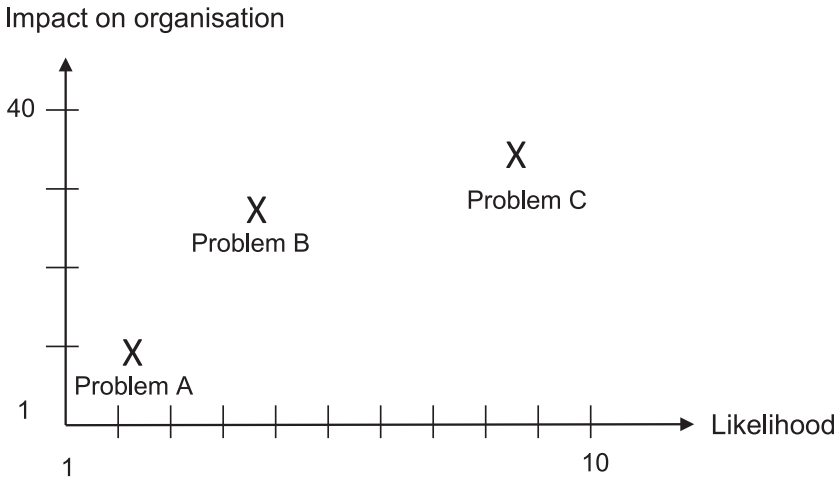

Figure D.1 — NIST risk map

Here is an example based on a messaging service:

— the PII processing is the collection of PII as a result of the use of the messaging service;

— the problematic PII processing is an unanticipated revelation of a confidential message (see C.2);

— the potential problem for individuals is stigmatization (see C.4);

— the likelihood of the problematic PII processing is 7;

— the impact has a value of 23, consisting of the sum of the following:

  — non-compliant cost is 7,

  — direct business cost is 6,

  — reputational cost is 6,

  — internal culture cost is 4,

— the resulting risk is 7x23 (161)

D.3 CNIL privacy risk analysis

CNIL uses a risk model where the privacy risk level is based on the impact on PII principals' rights and freedoms:

Privacy risk level	=	Likelihood of a privacy breach	×	Severity of the privacy breach on PII principals

[a] Also known as "feared event".

© ISO/IEC 2019 – All rights reserved

It is composed by two distinct factors that should be combined where:

— likelihood is viewed as the feasibility of a risk to occur. The likelihood can be estimated using the following scale:

  — negligible (1): it does not seem possible for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets[12)];

  — limited (2): it seems difficult for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets;

  — significant (3): it seems possible for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets; and

  — maximum (4): it seems extremely easy for the selected risk sources to materialize the threat by exploiting the vulnerabilities of supporting assets;

— severity is viewed as the magnitude of the risk. The severity can be estimated using the following scale:

  — negligible (1): PII principals either will not be affected or can encounter a few inconveniences, which they will overcome without any problem;

  — limited (2): PII principals can encounter significant inconveniences, which they will be able to overcome despite a few difficulties;

  — significant (3): PII principals can encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties; and

  — maximum (4): PII principals can encounter significant, or even irreversible, consequences, which they may not overcome.

The risk assessment follows the following steps:

— identify the risk sources (e.g., human or not, intentional or not);

— for each potential privacy breach (e.g., unauthorized access to, undesired modification of, and disappearance of data), determine its potential impacts on PII principals and estimate its severity (negligible, limited, significant and maximum);

— for each potential privacy breach, identify the threats and determine the likelihood (negligible, limited, significant and maximum); and

— for each potential privacy breach, determine the risk level as follows:

Risk Level (1-16)	= f (	Highest likelihood of the threats that can lead to a privacy breach (1-4)	×	Severity of the privacy breach (1-4)	)

— present the risks on a risk map with one dimension representing the likelihood of a privacy breach and the other dimension representing the severity of the privacy breach to PII principals.

12) For instance, hardware systems, software components, networks, or people.

© ISO/IEC 2019 – All rights reserved

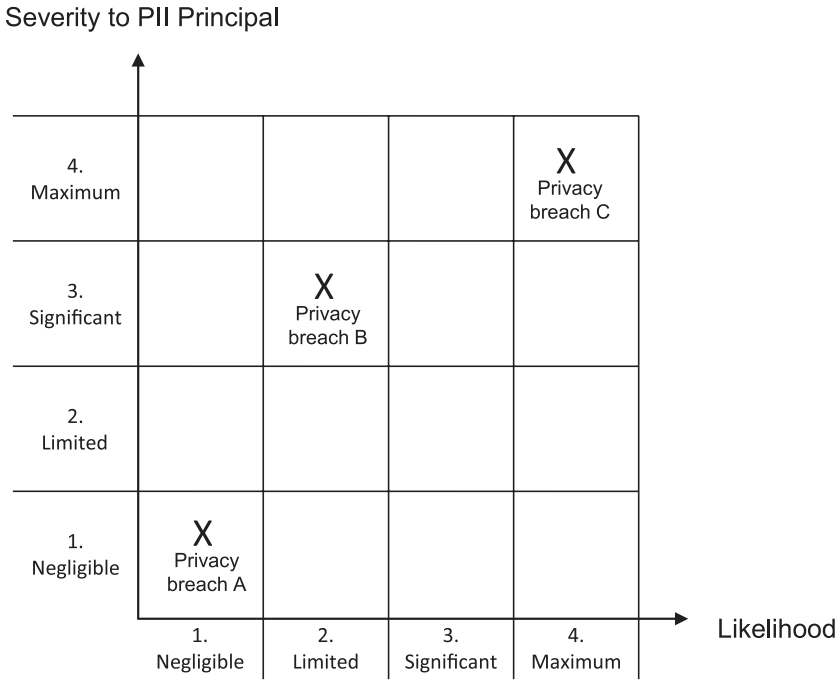

Figure D.2 — CNIL risk map

Here is an example based on a messaging service:

— the risk source is an internal IT operation acting intentionally;

— the threat is the collection of PII in the course of using the messaging service directly from the server;

— the privacy breach (or feared event) is an unanticipated revelation of a confidential message (see C.4);

— the likelihood is "limited" (2);

— the potential impact on PII principles is stigmatization;

— the severity is "significant" (3); and

— the resulting risk is Likelihood (2) × Severity (3).

© ISO/IEC 2019 – All rights reserved

Bibliography

[1] ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

[2] ISO/IEC/IEEE 12207, *Systems and software engineering — Software life cycle processes*

[3] ISO/IEC/IEEE 29148, *Systems and software engineering — Life cycle processes — Requirements engineering*

[4] ISO/IEC/IEEE 29110, *Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs). Freely*, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[5] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[6] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[7] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[8] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27034, *Information technology — Application security*

[10] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[11] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[12] ISO/IEC 29151, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[13] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[14] ISO/IEC 27552, *Information technology — Security techniques — Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management – Requirements and guidelines*

[15] ISO 31000, *Risk management — Guidelines*

[16] Cavoukian A., "7 Foundational Principles of Privacy by Design", Information & Privacy Commissioner, Ontario, Canada. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. May 4th, 2015.

[18] NISTIR 8062. *"Introduction to Privacy Engineering and Risk Management in Federal Systems"*. January 2015. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf

[19] NISTIR 8062*"An Introduction to Privacy Engineering and Risk Management in Federal System"*. January 2017. http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[20] Spiekermann S., Cranor L.", Privacy Engineering". IEEE Transactions on Software Engineering, Vol. **35**, Nr. 1, January/February 2009, pp. 67-82.

© ISO/IEC 2019 – All rights reserved

[21] Gürses S. F., Troncoso C., Diaz C., "Engineering Privacy-by-Design". Computers, Privacy & Data Protection, 2011

[22] Kung A., Freytag J., Kargl F., "Privacy-by-design in ITS applications". 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks, June 20, 2011, Lucca, Italy

[23] Hansen M., Jensen M., Rost M., "Protection Goals for Engineering Privacy"; in 2015 International Workshop on Privacy Engineering (IWPE). http://ieee-security.org/TC/SPW2015/IWPE/2.pdf

[24] Deng Mina, Kim Wuyts, Riccardo Scandariato, Bart Preneel, Wouter Joosen, A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements, *Requirements Engineering Journal*, volume **16**, issue 1, pages 3-32, 2011

[25] LINDDUN privacy threat analysis methodology, https://www.linddun.org/

[26] Danezis G., Domingo-Ferrer J., Hansen M., Hoepman J.-H., Le Métayer D., Tirtea R. et al. , ENISA Report, Privacy and Data Protection by Design — from policy to engineering. December 2014. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

[27] Organization for the Advancement of Structured Information Standards (OASIS) Privacy Management Reference Model and Methodology, (PMRM), Version 1.0. July 2013, updated May 2016. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

[28] Organization for the Advancement of Structured Information Standards (OASIS) PbD-SE, June 2014. http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.pdf and http://docs.oasis-open.org/pbd-se/pbd-se-annex/v1.0/cnd01/pbd-se-annex-v1.0-cnd01.pdf

[29] Jaap-Henk Hoepman, Privacy design strategies – (extended abstract). In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings, pages 446–459, 2014

[30] Colesky M., Hoepman J.-H., Hillen C., A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering – IWPE'16, pages 33-40, San Jose, CA, USA, May 26 2016

[31] Alberto Crespo García, Nicolás Notario McDonnell, Carmela Troncoso, Daniel Le Métayer, Inga Kroener, David Wright, José María del Álamo, Yod Samuel Martín. PRIPARE consortium. Privacy and security-by-design methodology handbook. December 2015. http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

[32] Sourya Joyee De *Danial Le Métayer. Privacy Risk Analysis. Synthesis lecturers on information security, privacy and trust*, Morgan and Claypool publishers, 2016.

[33] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012.

[34] NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. April 2013 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[35] CNIL PIA manual 1- methodology: how to carry out a PIA. June 2015 Edition. https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

[36] CNIL PIA manual 1- tools (templates and knowledge bases). https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

[37] The STRIDE threat model; https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx. Note that the page states the following: This documentation is archived and is not being maintained.

© ISO/IEC 2019 – All rights reserved

[38] Solove D.J., A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129.

[39] Pfitzmann A., Hansen M., A terminology for talking about privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity and identity management. Aug. 2010. https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

[40] LINDDUN mitigation strategies and solutions. https://linddun.org/solutions.php

© ISO/IEC 2019 – All rights reserved

ICS 35.030

Price based on 52 pages

© ISO/IEC 2019 – All rights reserved