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 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

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*.

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.

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.

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]

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]

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]

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

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.

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.).

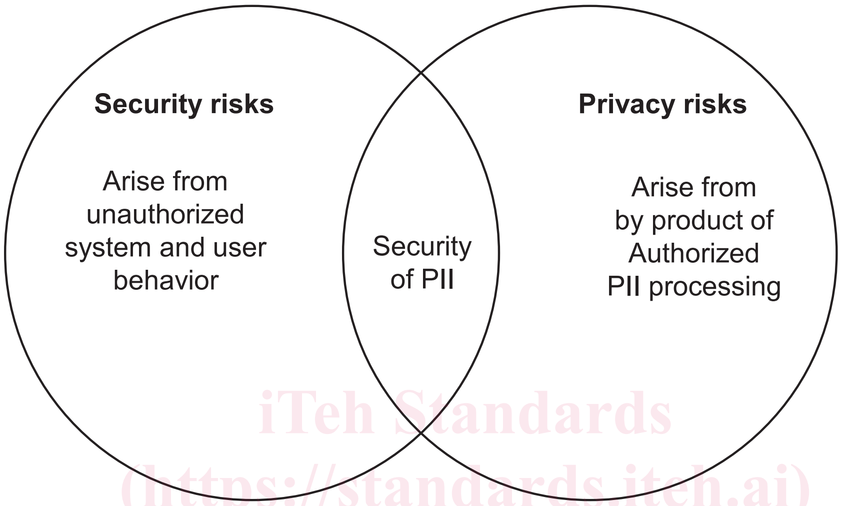

Figure 1 — Relationship between security and privacy

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.

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).

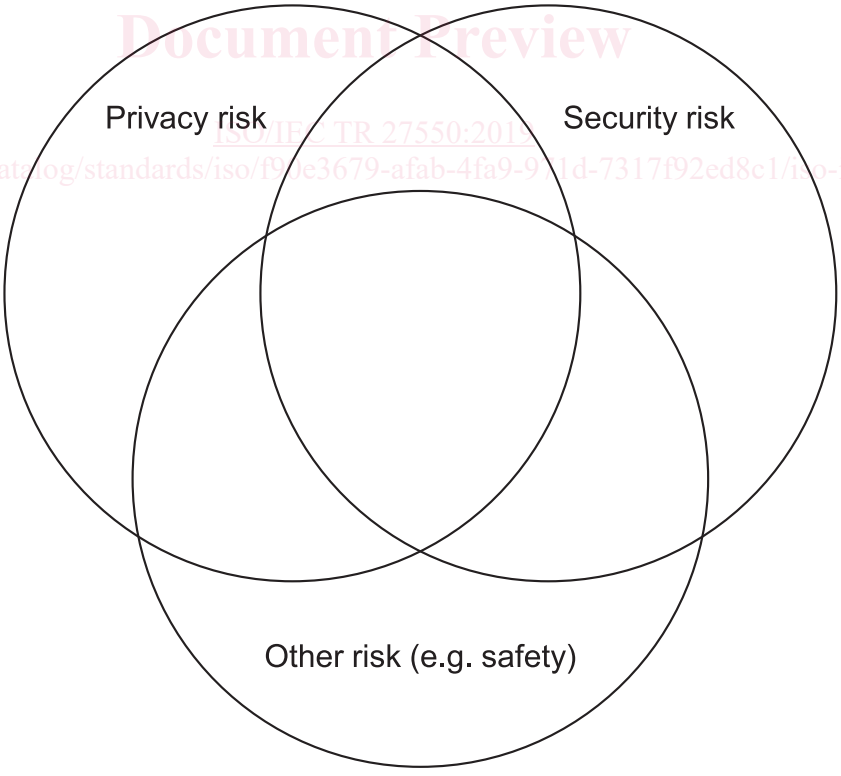

Figure 2 — Multiple risk concerns in system engineering

1) From NIST 800-30[33].

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

Privacy risk sources and consequences

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

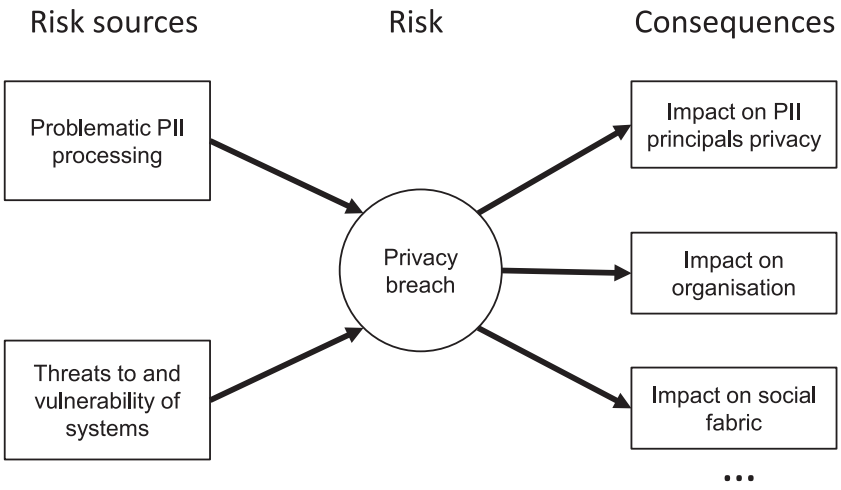

Figure 3 — Privacy risk sources and consequences

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.