International Standard

ISO/IEC 27561

First edition
2024-03

Information security, cybersecurity and privacy protection — Privacy operationalisation model and method for engineering (POMME)

Sécurité de l'information, cybersécurité et protection de la vie privée — Méthode et modèle d'opérationnalisation de la confidentialité pour l'ingénierie (POMME)

Reference number
ISO/IEC 27561:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Privacy principles and associated privacy control requirements face a number of challenges arising from the need to comply with consumer expectations and global regulations for privacy which are continually evolving, as well as the complex and rapidly changing ecosystem of devices, networks and applications through which personally identifiable information (PII) flows. To face these challenges, privacy principles and associated privacy control requirements are expected to be operationalized into sets of capability functions and mechanisms. The privacy operationalization model and method for engineering (POMME) addresses these challenges, particularly in interconnected and interdependent applications and rapid lifecycle development processes.

Achieving effective operationalization in this environment is a critical responsibility of privacy engineers and the developers and solution providers who support them. They should not only understand the technology interfaces and interdependencies among components as they design these systems, but also ensure that the appropriate privacy controls are selected and implemented across the entire data flow landscape relevant to their analysis.

POMME provides a structured and extensible analytic model and method to accomplish these objectives. It is based on the OASIS Privacy Management Reference Model and Methodology (PMRM),[1] and it reflects findings expressed in ISO/IEC TR 27550, which provides extensive information on privacy engineering that organizations can use to integrate privacy engineering into system lifecycle processes. It also describes the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, and risk management).

POMME supports the operationalization of privacy as it is defined in ISO/IEC 29100, utilizing a process following ISO/IEC/IEEE 24774. The primary focus of POMME is on the functional architecture and implementation details of privacy engineering, rather than the "policy" aspects of privacy, such as privacy principles, privacy impact assessments (PIAs) and privacy control statements. These policy elements are essential inputs into the engineering process and are already addressed by existing standards, codes of practice, and guidance listed in the Bibliography. POMME utilizes these elements to support the functional role of the privacy engineer.

Through the use of POMME, a privacy engineer can define the domain boundaries of a target of analysis (TOA) and research, document, and organize the information (e.g. standards, privacy policies, and technical data). By doing so, the capabilities necessary to implement privacy control requirements can be identified. This enables the privacy engineer to:

a) determine the functions needed to implement privacy control requirements;

b) understand the relationship among controls, particularly when controls are interdependent or networked or cloud-based;

c) select the specific implementation mechanisms (such as code or product configurations) that deliver the required privacy controls in their operational state.

An additional benefit of POMME is that its structured processes support improved usage and integration of privacy management tools, such as privacy-specific open source software.

Figure 1 and Table 1 illustrate the POMME operationalization model and method.

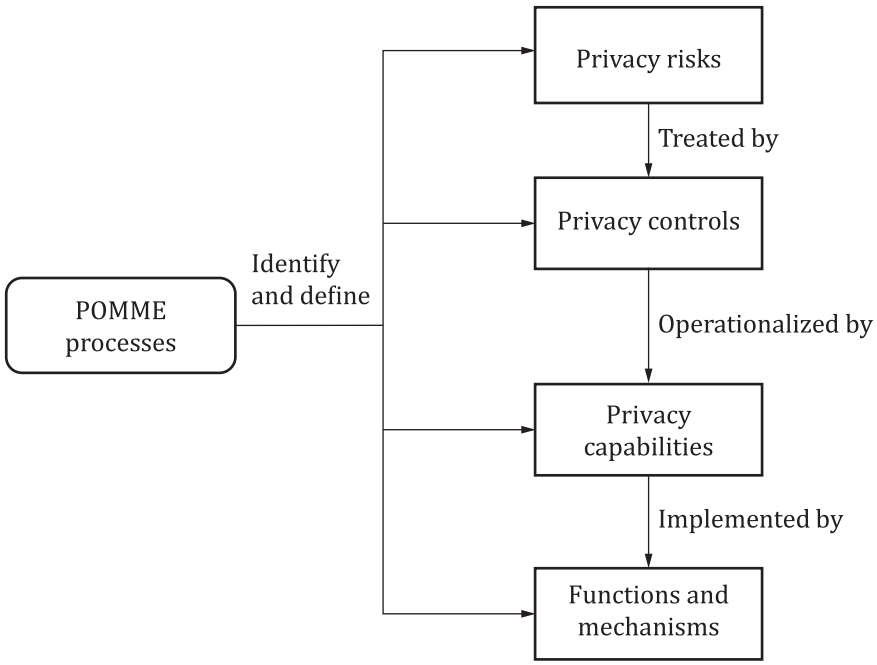

Figure 1 — POMME operationalization model

Table 1 includes an inventory process which consists of eight activities and an operationalization process which consists of five activities.

Table 1 — POMME method

POMME process	Clause	Activity
Initial information inventory process	6.3	Define and describe the TOA
	6.4	Participant and information source identification
	6.5	Systems and processes identification
	6.6	Domains and domain owners identification
	6.7	Intra-domain roles and responsibilities identification
	6.8	Touch points identification
	6.9	Data flows identification
	6.10	PII identification
Privacy controls, privacy control requirements, capabilities, risk assessment and iteration	7.3	Privacy control specification
	7.4	Privacy control requirement specification
	7.5	Capabilities specification
	7.6	Risk assessment
	7.7	Iteration

Information security, cybersecurity and privacy protection — Privacy operationalisation model and method for engineering (POMME)

1 Scope

This guidance document describes a model and method to operationalize the privacy principles specified in ISO/IEC 29100 into sets of controls and functional capabilities. The method is described as a process that builds upon ISO/IEC/IEEE 24774.

This document is designed for use in conjunction with relevant privacy and security standards and guidance which impact privacy operationalization. It supports networked, interdependent applications and systems. This document is intended for engineers and other practitioners developing systems controlling or processing personally identifiable information.

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 terminology databases for use in standardization at the following addresses:

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

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

3.1
access capability
functionality enabling *personally identifiable information (PII) principals* (3.27) to access their *PII* (3.25) and propose changes, correction, or deletion

3.2
activity
set of cohesive tasks of a *process* (3.38)

[SOURCE: ISO/IEC/IEEE 15288:2023, 3.3]

3.3
actor
individual, or a digital proxy for an individual, who interacts with a *system* (3.41) that is processing *personally identifiable information* (3.25)

3.4
agreement capability
functionality that defines and documents the rules and options for the handling of *personally identifiable information* (3.25), consent documentation, as well as modifications to, and withdrawal of, consent

3.5
assurance capability
functionality that ensures that any *actor* (3.3), *domain* (3.10), *system* (3.41), or system component has the functionality necessary to carry out their assigned roles in processing *personally identifiable information* (3.25)

3.6
audit control
process (3.38) designed to provide reasonable assurance regarding the effectiveness and efficiency of operations and compliance with applicable policies, laws, and regulations

3.7
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.8
capability
ability of a *system* (3.41) to deliver a *function* (3.14), feature, or service

EXAMPLE "Provide confidential communication of PII in transit" is an example of a capability, whereas "encrypt data communicated to the server using TLS" is an example of a function.

[SOURCE: ISO/TR 4804:2020, 3.4, modified — substituted "product" with "system"; Note 1 to entry has been replaced by an example.]

3.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or *processes* (3.38)

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.10
domain
set of assets and resources subject to a common privacy and security policy

[SOURCE: ISO/IEC 27033-1:2015, 3.35, modified — deleted "security" from "security domain"; added "privacy and" before "security policy".]

3.11
domain owner
stakeholder (3.40) responsible for ensuring that *privacy controls* (3.30) are implemented and managed in a *system* (3.41)

Note 1 to entry: A domain owner can be a *personally identifiable information (PII) controller* (3.26), *PII processor* (3.28), or *PII principal* (3.27) depending on the system(s) being analysed.

3.12
enforcement capability
functionality that achieves compliance with accountability requirements

Note 1 to entry: This *capability* (3.8) can initiate response actions, policy execution, recourse when audit controls and monitoring indicate operational faults and failures, record and report evidence of compliance to stakeholders, and provide evidence necessary for accountability.

3.13
exported privacy control
privacy control (3.30) that is transmitted to a *personally identifiable information (PII) controller* (3.26) or *PII processor* (3.28) in another *domain* (3.10) or *system* (3.41)

Note 1 to entry: An exported privacy control can be included in a data sharing agreement.

3.14
function
<capability> technical or manual process component of a *capability* (3.8)

EXAMPLE "Encrypt data communicated to the server using TLS" is an example of a function whereas "provide confidential communication of PII in transit" is an example of a capability.

Note 1 to entry: A function, feature or service is expressed at a more granular level than a capability.

3.15
incoming PII
personally identifiable information (PII) (3.25) flowing into a *domain* (3.10), or a *system* (3.41) or *process* (3.38) within a domain

3.16
inherited privacy control
privacy control (3.30) that is received by a *personally identifiable information (PII) controller* (3.26) or *PII processor* (3.28) from another *domain* (3.10) or *system* (3.41)

Note 1 to entry: An inherited control can be found in a data sharing agreement.

3.17
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.18
interaction capability
functionality that provides interfaces for presentation, communication, and interaction of *personally identifiable information (PII)* (3.25) and relevant information associated with the PII

Note 1 to entry: This can include user interfaces, system-to-system information exchanges, and agents.

3.19
internally generated PII
personally identifiable information (PII) (3.25) created within the *domain* (3.10) or *system* (3.41)

3.20
internal privacy control
privacy control (3.30) that is required within a *domain* (3.10) or *system* (3.41)

3.21
mechanism
<capability> specific implementation method of a *function* (3.14) in a *system* (3.41)

EXAMPLE Software, software configurations, firmware, technical products and solutions, technical settings, or detailed manual procedures.

Note 1 to entry: A mechanism is expressed at a more granular level than a function.

3.22
operationalization
knowledge compilation by conversion from a declarative form into a procedural, that is, operational form

[SOURCE: ISO/IEC 2382:2015, 2123014, modified — notes to entry have been deleted.]

3.23
outgoing PII
personally identifiable information (PII) (3.25) flowing out of a *domain* (3.10), or out of a *system* (3.41) within a domain to another system within the domain

3.24
participant
stakeholder (3.40) responsible for operational privacy management

3.25
personally identifiable information
PII
personal information
personal data
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the PII principal. 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 29100:2024, 3.7, modified — admitted terms have been added; removed "any"; substituted "can" for "might".]

3.26
PII controller
personal information controller
data controller
privacy *stakeholder* (3.40) (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.25) 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 29100:2024, 3.8, modified — admitted terms have been added]

3.27
PII principal
natural person to whom the *personally identifiable information (PII)* (3.25) relates

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

[SOURCE: ISO/IEC 29100:2024, 3.9, modified — Note 1 to entry has been added.]

3.28
PII processor
personal information processor
data processor
privacy *stakeholder* (3.40) that processes *personally identifiable information (PII)* (3.25) on behalf of and in accordance with the instructions of a *PII controller* (3.26)

[SOURCE: ISO/IEC 29100:2024, 3.10, modified — admitted terms have been added.]

3.29
privacy by design
approach in which privacy is considered at the initial design stage and throughout the complete lifecycle of products, *processes* (3.38) or services that involve processing *personally identifiable information* (3.25)

[SOURCE: ISO/IEC TS 27570:2021, 3.21, modified — removed hyphens from the term]

3.30
privacy control
measure that treats privacy risks by reducing their likelihood or their consequences

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

Note 2 to entry: Control is also used as a synonym for safeguard or countermeasure.

[SOURCE: ISO/IEC 29100:2024, 3.12]

3.31
privacy control requirement
specification for a *system* (3.41), product or service functionality to implement a *privacy control* (3.30) and operationalize the *stakeholders'* (3.40) desired privacy outcomes

Note 1 to entry: A privacy control requirement can be based on legal, regulatory, operational, or business/contractual requirements.

3.32
privacy engineer
individual with specialized knowledge of *privacy engineering* (3.33) concepts and practices and the ability to integrate privacy concerns into engineering practices for *systems* (3.41) and software engineering lifecycle *processes* (3.38)

3.33
privacy engineering
integration of privacy concerns into engineering practices for *systems* (3.41) and software engineering lifecycle *processes* (3.38)

[SOURCE: ISO/IEC TR 27550:2019, 3.14]

3.34
privacy impact assessment
PIA
overall *process* (3.38) of identifying, analysing, evaluating, consulting, communicating, and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information (PII)* (3.25), framed within an organization's broader risk management framework

[SOURCE: ISO/IEC 29134:2023, 3.7]

3.35
privacy management
collection of policies, *processes* (3.38) and methods used to protect and manage *personally identifiable information (PII)* (3.25)

3.36
privacy policy
overall intention and direction, rules and commitment, as formally expressed by the *personally identifiable information (PII) controller* (3.26) related to the processing of *PII* (3.25) in a particular setting

[SOURCE: ISO/IEC 29100:2024, 3.14, modified – changed term to singular]

3.37
privacy principle
set of shared values governing the protection of *personally identifiable* information *(PII)* (3.25) when processed in information and communication technology systems

[SOURCE: ISO/IEC 29100:2024, 3.16]

3.38
process
interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1, modified — deleted "set of", notes to entry have been deleted]