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/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols and abbreviated terms ... **7**

5 Context of privacy operationalization ... **7**
5.1 General ... 7
5.2 Privacy engineering viewpoint ... 7
5.3 Privacy engineering operationalization model ... 8
5.4 Privacy engineering operationalization method ... 8
5.5 POMME processes overview ... 8
5.6 Privacy and security ... 9

6 Initial information inventory process ... **10**
6.1 Purpose ... 10
6.2 Outcomes ... 10
6.3 Define and describe the TOA ... 10
6.4 Participant and information source identification ... 11
6.5 Systems and processes identification ... 11
6.6 Domains and domain owners identification ... 11
6.7 Intra-domain roles and responsibilities identification ... 12
6.8 Touch points identification ... 12
6.9 Data flows identification ... 12
6.10 PII identification ... 12

7 Privacy controls, privacy control requirements, capabilities, risk assessment and iteration process ... **13**
7.1 Purpose ... 13
7.2 Outcomes ... 13
7.3 Privacy control specification ... 14
7.4 Privacy control requirement specification ... 14
7.5 Capabilities specification ... 14
7.6 Risk assessment ... 15
7.7 Iteration ... 15

8 Privacy capabilities ... **16**
8.1 Capabilities overview ... 16
8.2 Capability details and associated functions ... 17
8.2.1 Core policy capabilities ... 17
8.2.2 Privacy assurance capabilities ... 18
8.2.3 Presentation and lifecycle capabilities ... 18

Annex A (informative) **Mapping of the privacy principles from ISO/IEC 29100 to POMME capabilities** ... **19**

Annex B (informative) **Lifecycle process example involving a PII controller and a solution provider** ... **20**

Annex C (informative) **POMME capability functions and mechanisms in a consumer application use case** ... **23**

Bibliography ... **28**

© ISO/IEC 2024 – 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 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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

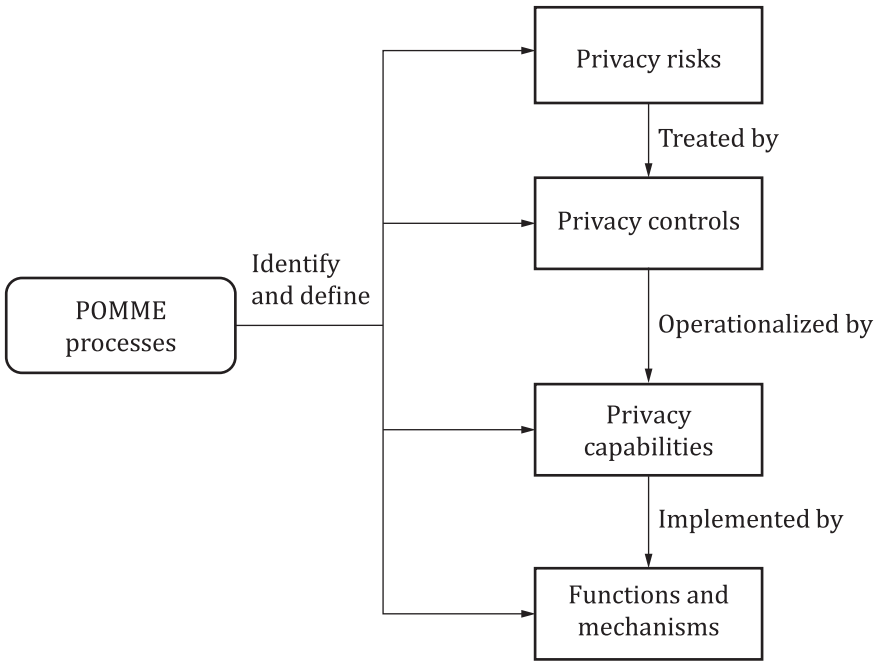


Figure 1 — POMME operationalization model

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

© ISO/IEC 2024 – All rights reserved

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

© ISO/IEC 2024 – All rights reserved