IEEE SA
STANDARDS
ASSOCIATION

IEEE Standard for Data Privacy Process

STANDARDS

IEEE Computer Society

Developed by the
Software and Systems Engineering Standards Committee

IEEE Std 7002™-2022

IEEE

Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 18:38:35 UTC from IEEE Xplore. Restrictions apply.

IEEE Standard for Data Privacy Process

Developed by the

Software and Systems Engineering Standards Committee
of the
IEEE Computer Society

Approved 9 February 2022

IEEE SA Standards Board

Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 18:38:35 UTC from IEEE Xplore. Restrictions apply.

Abstract: The requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer, or other external user's personal data are defined by this standard. Organizations and projects that are developing and deploying products, systems, processes, and applications that involve personal information are candidate users of the IEEE Std 7002™ standard. Specific procedures, diagrams, and checklists are provided for users of the IEEE Std 7002 standard to perform conformity assessments on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.

Keywords: data protection, IEEE 7002™, privacy, privacy by design, privacy impact assessment, privacy controls, systems development life cycle

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 19 April 2022. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-8452-7 STD25252
Print: ISBN 978-1-5044-8453-4 STDPD25252

IEEE prohibits discrimination, harassment, and bullying.
For more information, visit https://www.ieee.org/about/corporate/governance/p9-26.html.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 18:38:35 UTC from IEEE Xplore. Restrictions apply.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

[1]Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2]Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are

[3]Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4]Available at: https://standards.ieee.org/standard/index.html.
[5]Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Participants

At the time this IEEE standard was completed, the Personal Data Privacy Working Group had the following membership:

Matthew Silveira, *Chair*
John Wunderlich, *Vice Chair*
Guy Cohen, *Editor*
Robert Donaldson, *Secretary*

Ted Bardusch
Kaitlin Boeckl
Diego Chiozzi
Jonathan Fox
Vicky Hailey
Naomi Lefkovitz
Zvikomnorero Murahwi
Brian Page
Randy K. Rannow
Denise Schoeneich
Mike Tibodeau

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Pieter Botman
Carl Eric Codere
Raul Colcher
Ronald Dean
Robert Donaldson
Donald Dunn
Jonathan Fox
David Fuschi
Paulo Goncalves
Didem Gurdur Broo
Mark Henley
A. Hessami
Werner Hoelzl
Dennis Holstein
Piotr Karocki
Edmund Kienast
Thomas Kurihara
Susan Land
Sean Laroque-Doherty
Naomi Lefkovitz
Claire Lohr
Javier Luiso
Lars Luenenburger
Lingzhong Meng
Joanna Olszewska
Brian Page
Beth Pumo
Randy K. Rannow
Annette Reilly
Maximilian Riegel
Pablo Rivas Perea
Robert Schaaf
Denise Schoeneich
Subrato Sensharma
John Sheppard
Matthew Silveira
Carl Singer
Robert Soper
Thomas Tullia
Kenneth Wallace
Eleanor Watson
John Wunderlich
Naritoshi Yoshinaga
Oren Yuen
Janusz Zalewski

When the IEEE SA Standards Board approved this standard on 9 February 2022, it had the following membership:

Gary Hoffman, *Chair*
Vacant Position, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Doug Edwards
Ramy Ahmed Fathy
J.Travis Griffith
Thomas Koshy
Joseph L. Koepfinger*
David J. Law
Howard Li
Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Chenhui Niu
Damir Novosel
Annette Reilly
Dorothy Stanley
Mehmet Ulema
Lei Wang
F.Keith Waters
Karl Weber
Sha Wei
Howard Wolfman
Daidi Zhong

*Member Emeritus

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Introduction

This introduction is not part of IEEE Std 7002-2022, IEEE Standard for Data Privacy Process.

This standard outlines a methodological approach to developing systems that meet an organization's privacy requirements. This standard represents a unique attempt to enable systems teams to follow a structured process for systems engineering that incorporates privacy or data protection considerations from conception to delivery through operations to when the product is no longer in the marketplace. Existing privacy standards, such as ISO/IEC 29100 (Privacy Framework) or ISO/IEC TR 27550 (Privacy engineering for system life cycle processes) (see [B8] and [B7]) are written as standards to be understood or implemented by privacy teams or privacy practitioners. This can result in disconnects between development and operating teams and privacy teams because of late engagement or miscommunications.

By targeting the end-to-end systems engineering process, IEEE Std 7002™ enables systems teams to proactively identify privacy related gaps and capabilities in their own processes. In turn this will facilitate better and more efficient communications of requirements and expectations early enough in the development process to reduce compliance costs and increase end user satisfaction related to privacy. This is, fundamentally, a standard for implementing demonstrable "Privacy by Design."

The standard breaks down the different components of that approach, with each clause from Clause 5 through Clause 9 covering a distinct element of that approach.

Clause 1 through Clause 4 provide supporting information. Clause 1 describes the scope, purpose, and usage of words that indicate normative requirements. Clause 2 states relevant references, and Clause 3 lists relevant definitions and abbreviations.

Clause 4 includes a discussion of key terms, provides guidance to the reader on use of the standard, and summarizes the remaining clauses.

Clause 5 through Clause 9 are the methodological approach and include the normative requirements of this standard. For a summary of these clauses see 4.3.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Contents

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

IEEE Standard for Data Privacy Process

1. Overview

1.1 Scope

This standard defines requirements for a systems engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer, or other external user's personal data. It extends across the life cycle from policy through development, quality assurance, and value realization. It includes a use case and data model (including metadata). It applies to organizations and projects that are developing and deploying products, systems, processes, and applications that involve personal information. By providing specific procedures, diagrams, and checklists, this standard enables users to perform a conformity assessment on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for identifying where privacy controls and measures are needed, and for confirming they are in place.

1.2 Purpose

The purpose of this standard is to provide an overall methodological approach that specifies practices to manage privacy issues within the systems engineering life cycle processes.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[6,7]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

[6]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
[7]The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

There are no normative references in this standard.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [8]Where a term is not defined in the core text, this clause, or the IEEE Standards dictionary, its intended meaning is the commonly used dictionary definition.

NOTE—For additional terms and definitions in the field of systems engineering, see ISO/IEC/IEEE 24765 [B14], which is published periodically as a "snapshot" of the SEVOCAB (Systems and software Engineering Vocabulary) database.[9,10]

accountability: Degree to which the actions of an entity can be traced uniquely to the entity.

authorized individual: Individual identified by an organization to make decisions, allocate resources, and accept risk, within a domain of responsibility.

business requirements: Business needs that the organization aims to meet.

contextual factors: Conditions that drive or affect the requirements for an organization or a system being developed.

NOTE—Contextual factors are likely to change, and so may need to be reviewed periodically where they have shaped requirements or controls.

control: Monitoring of system output to compare with expected output and taking corrective action when the actual output does not match the expected output

data actions: System operations on data elements.

data element: Item of data that conveys or contains meaningful information.

data flow: The movement of data through a system from one component to the next.

data map: Visual representation of data processing within the system.

data privacy: The fair and legitimate processing of personal data.

data processing: Systematic performance of operations upon data.

[8]*IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.
[9]Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.
[10]The numbers in brackets correspond to those of the bibliography in Annex B.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

data protection: Implementation of appropriate administrative, technical, or physical means to guard against unauthorized use, intentional or accidental disclosure, modification, or destruction of data, including static and dynamic data.

data subject: Natural person to whom personal data relates.

data system: Discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of data.

de-identification: Removal of personally identifiable data from a data set.

entity: Individual, group or organizational function that can be tasked with a given responsibility.

environment: Responsible organization, its systems, or processing activities it operates.

NOTE—There can be many aspects to an environment, and they can be viewed on different scales as relevant to the situations under consideration. For instance, an organization may consider the regulatory or cultural environments within which the organization operates.

functional requirement: Statement that identifies what results a system shall produce.

functionality: The set of capabilities, such as features, mechanisms, services, or procedures, allowable and actionable by the system.

governance: Process of establishing and enforcing strategic goals and objectives, organizational policies, and performance parameters.

guidelines: Official recommendation or advice that indicates policies, standards, or procedures for how something should be accomplished.

information security: Preservation of confidentiality, integrity, and accessibility of information.

NOTE 1—(See ISO/IEC/IEEE 24765c:2014 [B14].)

NOTE 2—In addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.

iterative process: Repeated process in which the output is evaluated and used as input for the next cycle.

nonfunctional requirement: Specification of how a system should be developed and maintained, or how it should be performed in operations.

organization: Group of people and facilities with an arrangement of responsibilities, authorities, and relationships.

organizational privacy requirements: Statements that reference key privacy objectives (e.g., Fair Information Practice Principles, or FIPPs) and specify capabilities and functions that a system must be able to perform.

organizational privacy framework: Set of principles, policies, and processes that describe what an organization may or may not do with personal data.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

personal data: Information related to a natural person.

NOTE 1—In some jurisdictions this is a legal term; in other jurisdictions other terms, such as personal information, are used.

NOTE 2—Personal Information (PI) and Personally Identifiable Information (PII) are terms used in some jurisdictions.

policy: Clear and measurable statements of preferred direction and behavior to condition the decisions made within an organization.

privacy capabilities: Ability to process personal data in a fair and legitimate manner.

privacy control: Monitoring prescribed for an information system, or an organization designed to achieve a privacy objective.

privacy framework: Structure that helps the organization meet its privacy requirements, including policies and procedures, roles and responsibilities, training, and governance functions.

privacy principles: Set of values that guide a system or an organization's personal data actions.

privacy requirements: Specifications for the processing of personal data to meet stakeholders' desired privacy outcomes and obligations.

NOTE—*See also:* **functional**, **nonfunctional requirements**, **organizational privacy requirements**, and **system privacy requirements**.

privacy risk: Combination of the likelihood and impact that individuals or organizations will experience problems resulting from exposure, use, theft, or alteration of personal data.

procedure: Information item that presents an ordered series of steps to perform a process, activity, or task.

regulatory context: Laws, regulations, or any other requirements within the jurisdictions where the system may operate.

risk: Effect of uncertainty on objectives.

stakeholder: Individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations.

risk mitigation: Response strategy whereby the project team acts to reduce the probability of occurrence or impact of a risk.

security control: A safeguard or countermeasure prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

system: Software and/or the combination of other components (including hardware and human managed processes).

system-of-interest: System whose life cycle is under consideration.

systems development life cycle: Activities associated with a system's development, encompassing the system's requirements, design, validation, deployment, maintenance, and end of life.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

training: Provision of formal and informal learning activities.

NOTE—Training can include roles, responsibilities, and related skills.

3.2 Acronyms and abbreviations

CIA	confidentiality, integrity, availability
DPIA	data protection impact assessment
GDPR	general data protection regulation
PIA	privacy impact assessment
PII	personally identifiable information
SDLC	systems development life cycle
SLA	service level agreement
SOI	system-of-interest

4. Process overview and scene setting

4.1 Key terminology

There is often uncertainty as to the distinction between certain key, and sometimes overlapping, terms that are often used when discussing privacy, including the following:

— Data privacy and privacy. Privacy is personal and contextual, experienced by each person in a variety of different ways. Data privacy is a subset of privacy, which relates to privacy considerations that arise from the processing of data that relates to individuals.

— Data privacy and information security. The goals of data privacy and information security are overlapping in some instances and distinct in others. The goals of information security are typically characterized by preventing the loss of confidentiality, integrity, and availability. In contrast, data privacy does not have equivalent, widely agreed upon goals, although it is often related to the fair and legitimate processing of personal data. As data privacy is just a part of the wider set of privacy issues, information security is just a part of the wider field of security. For more information about data privacy objectives, see 7.3.2.

— Data privacy and data protection. Some jurisdictions avoid the use of the term “privacy” (for instance it does not appear in the General Data Protection Regulation [GDPR]), but rather focus on the protection of data that relates to individuals, and the principles, rights, responsibilities, and obligations involved when processing personal data. While data protection laws and regulations often overlap with privacy and security issues, they are distinct. For example, group privacy, the privacy of groups as opposed to specific individuals, might be considered an issue in data privacy, but is generally not covered in data protection law. This standard recognizes but does not intend to restate or replace applicable laws and regulations regarding personal data, data privacy, and data security. Users of this standard are responsible for referring to and observing all such laws and regulations. Conformance with the provisions of this standard does not imply compliance with any applicable legal or regulatory requirements.

— Personal data/personal information, and personally identifiable information (PII). This standard uses the term “personal data,” although the standard can also apply in jurisdictions that use the term “personal information” (PII). These three terms are all used to describe information that relates to individuals. Depending on jurisdiction, different terms are used, with slightly different scopes

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

regarding what is relatable to an individual. In applying this standard an organization should use the term or terms most appropriate for their jurisdiction(s).

— Data privacy and confidential data. Data privacy is, as previously described, related to privacy considerations that arise from the processing of data that relates to individuals. Confidential data refers to agreed upon access restrictions to data that may or may not relate to individuals. This standard looks at the process for protecting data privacy, which might incorporate the protection of confidential data as it relates to individuals but extends beyond simply protecting such confidential data.

In addition to the terms covered in this subclause, 3.1 provides definitions and further context to other key terms used in this standard.

4.2 Guidance on using the standard

This standard recognizes but does not intend to restate or replace applicable laws and regulations regarding personal data, data privacy, and data security. Users of this standard are responsible for referring to and observing all such laws and regulations. Conformance with the provisions of this standard does not imply compliance with any applicable legal or regulatory requirements.

This standard addresses requirements, processes, and practices at multiple levels of the organization, from high-level policy to detailed operational procedures. This standard is designed to be applicable to a diverse set of use cases, it is iterative and modular in nature, and it will necessitate engagement (sometimes recurring engagement) from a variety of stakeholders involved in the system throughout its life cycles and user or implementer from different disciplines, at different levels, and across business lines.

Some entities may already have an organizational privacy framework in place while others may not. Those with existing frameworks in place may benefit from a gap assessment to identify what they already have in place, and what is needed to bring their frameworks into conformance with the standard.

Some organizations may be developing systems for internal use, while others may be developing systems that will be used by others, possibly in other jurisdictions or industries. Those developing systems for use by others should consider not just the contextual factors that affect them, but those that may affect the users of their system.

The standard is designed for iterative, recurring, and modular application, meaning that many of the actions may not happen in the order laid out or may need to be done more than once. The choice and order of actions to be applied to a system is contingent on the organization and design of the organization's privacy framework. At times, the user of the standard may need to repeat a process within one of the clauses or subclauses, for example a risk assessment may need to be repeated after changes to the system design. At other times users may find, through monitoring the wider context, organization, or system, that a change may need a response, which in turn requires further changes that cross from one section to another. For example, a change in the regulatory context, may lead to new privacy requirements that in turn affect the organizational privacy framework and system level requirements.

Managing privacy risk requires active engagement from a diverse set of stakeholders, including those responsible for development, business strategy, regulatory compliance and risk, and senior leadership, designers, producers, suppliers, and marketers who design, set requirements, or use/operate systems that process personal data. To deliver on the normative requirements in this standard it is critical to continuously engage with these diverse stakeholders.

4.3 High level process

This subclause summarizes the sections of the standard to help the reader understand how the components of the standard fit together.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Clause 5 discusses how an organization identifies its organizational privacy requirements. This involves looking at the context the organization exists in and the various types of contextual factors that may create and shape the organization's privacy requirements. In Figure 1, the circles represent some of the various contextual factors to be considered when identifying the organization's privacy requirements. The diagram represents the processing of these factors to identify the relevant requirements.

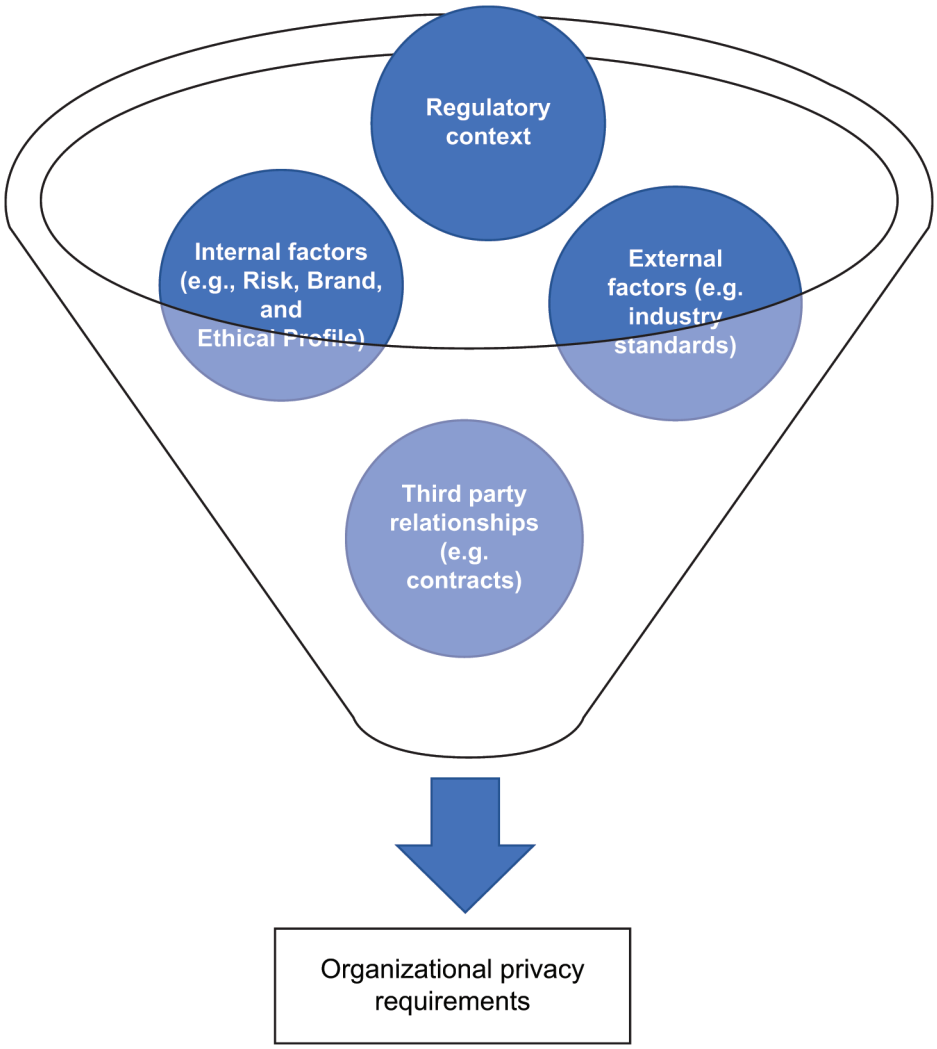

Figure 1—Organizational privacy requirements components

Clause 6 looks at the recommended components that make up an organization's privacy framework. This is the set of components that can collectively help the organization meet its privacy requirements.

Figure 2 shows the necessary components for an organizational privacy framework.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Organizational privacy framework			
Policies and procedures	Roles and responsibilities	Training	Governance functions

Figure 2—Organizational privacy framework components

Clause 7 discusses how an organization identifies the privacy requirements of a specific system, based on organizational privacy requirements, the system specifics, business objectives, and a risk assessment. In Figure 3, similarly, to Figure 1., the circles represent the factors that should be considered when identifying the system privacy requirements. The funnel represents the processing of these factors to identify the relevant requirements.

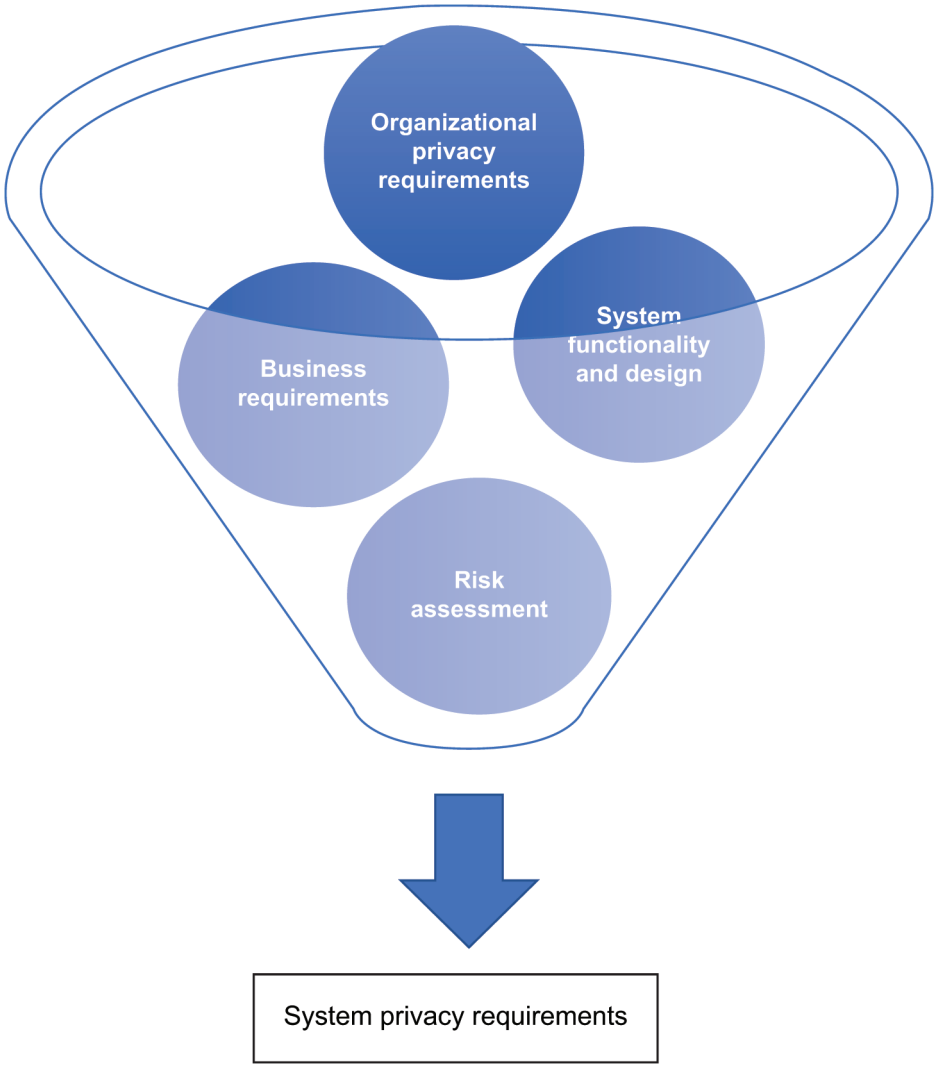

Figure 3—System privacy requirements components

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Clause 8 reviews how an organization examines a set of risk-based privacy requirements for a specific system and decides how to respond to the risks. This includes how to select, implement, and assess any controls used to mitigate and manage the identified risks, and how to monitor the system and its wider context to help meet its requirements. In Figure 3, the circle of boxes represents a repeating process where each box represents a stage in the iterative process. Overall, it aims to illustrate how privacy risk management is an evolving process due to the potential for the requirements or controls to change, and during system development and after the system has been launched.

Figure 4—Risk and controls cycle

Clause 9 discusses how privacy requirements are brought into the system development life cycle. Figure 4 highlights, how in a systems development life cycle, at each phase gate the user may need to go back to the previous stage or return to the start of the process entirely.

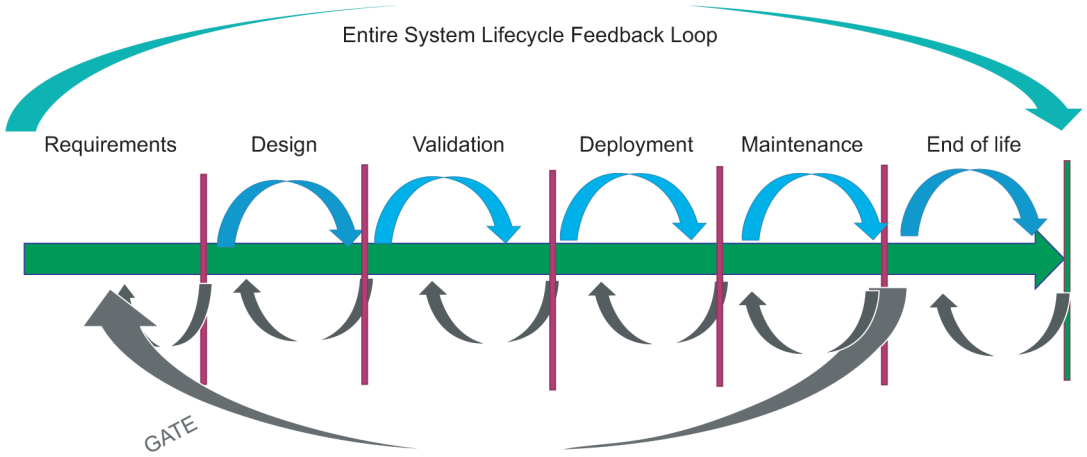

Figure 5—Systems development life cycle privacy phase gates

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

5. Defining organizational privacy requirements

5.1 Overview

This clause describes several different factors that can be used to define organizational privacy requirements, and in turn inform system-level privacy requirements and system design (see Clause 7).

The organization shall identify its organizational privacy requirements based on an assessment of the organizational context, including consideration of the regulatory context and other contextual factors.

When identifying the contextual factors for consideration, it is important to establish whether the system is going to be deployed internally or externally and/or operated by third parties. The contextual factors may change based on whether the design environment is different from the deployment environment.

Organizations may have already captured several contextual factors in an organizational privacy framework of some type (see Clause 6) and may find a review of that framework helpful when defining or reviewing organizational privacy requirements.

5.2 Regulatory context

The organization shall carry out a formal regulatory context assessment to accomplish the following:

— Identify the relevant laws or regulations with which the organization and intended system should comply, identifying which aspects of those legal requirements are relevant to the system.

— Identify any controls mandated by the regulation(s), or any specific functionality that the organization and system are required to provide.

— Document the regulatory context assessment results, in accordance with the organization's standard operating procedure for regulatory reporting, as applicable.

Many countries and regions have data protection or privacy laws and regulations, which provide individuals with rights over data that relates to them, and place minimum requirements and responsibilities on those processing personal data. While there may be significant overlap among some of these laws and regulations, there may also be some divergence with differences in approach or intended effect.

As such, for systems that can or may be deployed across various jurisdictions, it is necessary to map out the regulatory context for each of the jurisdictions in which the system may run, or in which the data of those residing in those regions may be used. In some instances, this may mean designing and deploying the system to function differently from one region to another.

Some regions have omnibus privacy or data protection laws with cross sectors and geographical boundaries. Other laws are country or state specific, industry specific, or may be part of a wider law that looks at other issues as well as privacy in the processing of personal data. As such, understanding the various relevant legal requirements in one region can be a considerable undertaking and users of this standard should seek legal advice for questions regarding compliance with applicable rules and regulations.

5.3 Additional contextual factors

In addition to regulatory context, there are a range of other factors, such as industry standards and practices, which may affect the organizational privacy requirements.

An organization shall identify and consider other contextual factors and shall document the consideration and outcome.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Examples are listed in Table 1.

Table 1—— Examples of non-regulatory contextual factors

External factors	Internal factors	Third party relationships
Industry standards and practices Privacy principles and frameworks Ethical considerations and obligations reflecting the societies and communities within which organizations are designing or deploying systems	Risk tolerance Business strategy and practices (including business objectives which are contingent on data processing) The organization's technology capabilities and limitations Brand identity and reputation Values, ethics, and culture (including internally identified privacy principles and frameworks)	Contractual obligations Operational performance, monitoring, and validation of obligations Cascading of obligations on sub-contractors and sub-sub-contractors Privacy needs of customers or service users Privacy needs of suppliers and partners

5.3.1 Privacy principles

Privacy principles are an important part of many privacy frameworks and regulations. For organizations developing their own privacy framework, the adoption of privacy principles from widely used existing sources is recommended. For examples of existing privacy principles see Annex A.

6. Setting organizational privacy framework

6.1 General

The organization shall implement an organizational privacy framework and shall include the following:

— Policies, procedures, and guidelines in conformance with 6.2

— Roles and responsibilities in conformance with 6.3

— Training in conformance with 6.4

— Governance and accountability functions in conformance with 6.5

An organizational privacy framework is a set of principles, policies, and processes that describe what an organization may or may not do with personal data; how decisions about the processing of personal data are made and operationalized; and how the organization meets the privacy requirements identified in Clause 5 to help design and deploy systems that meet mission and business objectives while managing privacy risk. These objectives require an organization to set privacy policies and procedures, have defined roles and responsibilities, provide training, and implement governance functions.

Organizational privacy frameworks can be built in whole or in part from an external privacy framework, so long as the requirements of this clause are met. These privacy frameworks can originate from various sources, including the following:

— National or international laws, regulations, or standards

— Industry or public sector principles, standards, best practices, and models

The organization shall implement their organizational privacy framework to meet the organization's requirements.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

6.2 Organizational policies, procedures, and guidelines

Organizational policies, procedures, and guidelines shall document how the organization meets its privacy requirements. Organizational policies, procedures, and guidelines often parallel or align to system specific policies, procedures, and guidelines, but they are not the same.

The organization shall leverage existing organizational policies, such as those for information security and data governance, to reduce governance complexity and technical implementation.

This standard does not prescribe specific policies and procedures, but organizations shall as a minimum put in place policies and procedures that cover the following:

— Basis and purposes: The legal basis and purposes for which the organization process personal data. This should include the rationale for the legal basis(es) selected. Note some jurisdictions do not recognize employee consent to be a valid authorization for the use of employee data, in connection with employer organizational requirements.

— Definitions: Definitions of key terms.

— Governance and accountability: The policies and procedures will support the governance functions described in 6.5.

— International/cross-jurisdiction data transfers: The basis or legal mechanism under which the organization transfers data into a different jurisdiction and the policies will govern this process.

— Notice: The information that the organization provides on its personal data processing and to whom and how the notice will be made available.

— Principles: The privacy principles adopted by the organization (see 5.3.1).

— Retention: How long should data be kept, and how data will be deleted when the data retention period has ended, in compliance with applicable laws and regulations.

— Rights: The data subjects' rights the organization needs to address, and the procedures the organization should follow when requests are recieved relating to data subject rights, in compliance with applicable laws and regulations.

— Risk assessments: Privacy or data protection impact assessments, and when a risk assessment is executed.

— Security: The proceses and controls by which the organization ensures data security.

— Special categories: How the organization deals with special categories of data, such as children's data, criminal records data, or particularly sensitive data such as health data, in compliance with applicable laws and regulations.

— Third parties, e.g., vendors and suppliers: The policies that guide the organization's data sharing agreements and contracts with vendors, suppliers, partners, contractors, and other third parties.

NOTE—These policies and procedures are distinct from guidelines on how third parties should comply with the stated policies. These may be included in an organization's training materials, as discussed in 6.4.

Organizations should also put in place policies on the following:

— Incident response: How the organization responds to an incident, such as a data breach, including corrective actions.

— Privacy enhancing technologies and techniques: Which technologies the organization uses, and how and when these technologies are used. When and how data should be pseudonymized or anonymized.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

— Regulatory response: How the organization responds to and communicates with regulators and requests from law enforcement, in compliance with applicable laws and regulations.

For each policy, procedure, or guideline, organizations shall identify the different types of data subjects, such as end-users, customers, and employees who are affected by their policies and procedures, It is recommended that the organization determine if each type of data subject has specific policies, procedures, and guidelines. The consideration findings of types of data shall be documented.

It is important to distinguish between an organization's internal policies and procedures, which govern data and privacy issues from an organization's public privacy policy, which an organization publishes to notify potential data subjects of how data may be processed. In some areas the policies may overlap, in others they may not. Where they do overlap, internal and public policies should not be contradictory. Some organizations do publish some of their own internal policies as well. For examples, see Annex A.

6.3 Roles and responsibilities

For an organizational privacy framework to be effective, at a minimum, certain roles are required with certain responsibilities within the organization responsible for following the organizational privacy framework.

The organization shall have entities, which may be an individual, group, or function responsible for the following:

— Accountability
— Process development and management
— Risk management
— Ongoing privacy requirements gathering
— Incident response
— System privacy risk assessment
— Operationalization and maintenance
— Quality

One individual, group, or function may be responsible for more than one of these roles or components of these roles. Segregated duties are ideal but not a necessity.

Documentation requirements shall be included in the defined responsibilities such that each documentation requirement in this standard is attributed to a specific entity. An example of a documentation requirement for systems, is provided in 7.2. For examples of ways to map these processes to roles, see tasks and the associated "primary responsibility" roles presented in NIST SP 800-37 ([B17]).

It is recommended that users and implementers of IEEE Std 7002™ be familiar with IEEE/ISO/IEC 24774:2021(see [B16]) to help assist in establishing processes and process models.

Organizations shall have entities responsible for the organizational privacy framework.

For each of these roles, the organizational privacy framework shall provide that the following applies:

— The entity has the necessary authority to achieve its stated objectives.
— The entity is sufficiently resourced to achieve its stated objectives.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

— There is a record of the entity's role and responsibilities.

— Relevant stakeholders within the organization are aware of the responsibilities of the stated entities.

NOTE—It is worth considering how the relationship between those responsible for privacy and those responsible for information security, such as the office of the Chief Information Security Officer (CISO), should operate. The lines between privacy and information security issues can be hard to draw, and as both can affect the functionality of the system it is important that both groups are aware of the actions of the other. This is particularly important when selecting privacy controls (see 8.2). The organization should also be mindful of potential conflicts of interest when allocating responsibilities and designating authorized individuals to make decisions as information security and privacy objectives can be in tension.

— The entity has appropriate decision making authority and reporting responsibilities, and these are sanctioned by the relevant stakeholders.

6.4 Training

Those responsible for adhering to the organization's policies, procedures, and guidelines, shall receive formal or informal training regarding data privacy policies and related responsibilities. Training activities and resources shall be managed and logged to support evidence of conformance of this requirement.

Training of organizational leadership, business staff, and technical staff (as well as training of third parties, in conformance with applicable employment requirements) in the organization's privacy framework is an important administrative control, including training on topics such as the organization's policies and procedures, and roles and responsibilities. Without effective training, an organization's privacy framework may not be as effectively implemented.

6.5 Governance and accountability functions

The entity identified as being accountable for the organizational privacy framework shall help to adequately prepare the organization to act on the requirements of this standard and enable governance of the organization's privacy framework and its operation through the following:

— Identification of privacy leadership and management stakeholders within the organization

— Support by executive management of an organizational commitment to privacy and the allocation of resources

— Confirmation that the organization has sufficiently resourced those responsible for the organization's privacy framework to so it is able to function as intended

— Assessment of the organizational readiness and maturity with regards to privacy management capabilities

The entity shall also be responsible for demonstrating conformity with certain requirements of this standard. This includes demonstrating that the following applies:

— The organizational privacy requirements have been validated by the privacy leadership and management.

— The existing organizational privacy policies and procedures, relevant roles and responsibilities, and staff training, meet the stated requirements (see 6.2 through 6.4) or, if not existent or sufficient, the entity has arranged for the creation or amendment of such requirements.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

— There is a process for risk assessments (see 7.4) to be performed consistently, formally, and of sufficient quality to enable the process detailed in 8.1; and to enable a determination by an authorized individual whether or not to accept the remaining risk.

— There are mechanisms in place, with audits at an appropriate accepted frequency, to validate that the organization's policies and procedures are effective and, if not, to manage a process for improvement, as well as validating that the policies are accessible and adherence to them is demonstrable.

— The SDLC process (see 9.2) is followed, with each phase gate passed.

The entity identified as accountable for the organizational privacy framework shall be accountable and. responsible to the organizations existing governance functions to enable organizational alignment, accountability, and responsibility.

7. Characterizing the system environment

7.1 Overview

Clause 5 addressed the various general factors to be considered to set the high-level organizational privacy framework (Clause 6). However, as the data processed, functionality, and design of each system is different, the high-level requirements should be considered regarding the specific use case of the environment and system in question.

Clause 7 addresses how the system specific privacy requirements are identified. It is the combination of the system privacy requirements and the organizational privacy requirements (identified in Clause 6) that characterize the system and allow for the appropriate selection of privacy controls or other privacy risk response methods (Clause 8).

The organization shall identify its system privacy requirements based on the identified mission and business needs (see 7.2), aspects of system functionality and design (see 7.3), the results of the privacy risk assessment (see 7.4), and in conformance with the organization's policies (see 6.2).

For some organizations, many of the steps in Clause 7 may be included in 7.4. This largely depends on what is covered within the risk assessment process. Regardless, the risk assessment process in 7.4 and the resulting actions taken in Clause 8 may or may not significantly change the system environment, necessitating an iterative process. As actions taken in Clause 8 may change the system environment, the process outlined in Clause 7 may need to be repeated, necessitating a new assessment and new controls. This may in turn trigger further iterations of the cycle between Clause 7 and Clause 8 until the assessment in Clause 7 does not result in any further changes to the system environment.

It is recommended that users and implementers of this standard be familiar with IEEE Std 802.1Q™-2014 [B2] as a part of the effort in evaluating and characterizing the system environment relative to the organizational privacy requirements considerations.

7.2 Business need

Identification of business mission and business needs shall be done as early as practicable and no later than the drafting of the high-level system design (see 7.3).

In doing this it is important to capture not just the value to the business, but how valuable to the business it is, and what is necessary for this value to be released. This can help the organization to inform the appropriate budget for the project and controls selection and implementation.

The business need and business mission for the system shall be documented.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

The system specific privacy requirements shall be identified and documented when identifying other business requirements.

Inventorying privacy requirements during the business requirements phase is important because it may identify resources required to implement the following:

- Establish or revise business workflows and processes for appropriately handling the selection, implementation and assessment of privacy controls (see 8.2)
- Determine if additional budget funding is required for privacy controls
- Provide for appropriate staffing resources, with relevant subject matter expertise and skills to provide for adequate and effective operational activities, compliance activities, training activities, and monitoring activities (see Clause 6)

7.3 System functionality and design

Organizations shall identify and document aspects of system functionality and design that are desired or necessary to meet business needs.

System functionality and design shall include the analysis and documentation to provide for the following:

- Privacy, security, and quality expressed through functional and nonfunctional requirements as appropriate to the system (this will be dealt with in greater detail during the risk assessment)
- Wider stakeholder mapping for the system, capturing dependencies, and where agreements, such as Service Level Agreements (SLAs) or other specific agreements such as data use contracts, exist or are needed
- Designs sufficiently detailed to capture the control model, data flow model, and data life cycle by means of text and graphic representations
- Any other variables that may have a significant impact on the functioning of the system, such as model parameters

Determination of the privacy, security, audit, and quality requirements shall be done simultaneously with other functional and non-functional system requirements.

This understanding enables the definition of system privacy requirements for privacy protection and support or to help improve intended or critical system functions and design.

Security and privacy teams should coordinate to identify areas of overlap between their respective domains and help the system's design address privacy and security requirements. For further information on the relationship between privacy and security, see 6.3.

As stated in 6.2, it is potentially of particular importance to establish mutually agreed SLAs for the engagement with the accountable authority (as identified in 6.3)

It is important when thinking about system design to consider the specific potential vulnerabilities of the system design. Changes to these components and ingredients can result in new specific privacy risks that are not expected. For example, the increasing and evolving prevalence of interconnected devices changes the risk profile of the system environment, introducing new threats and potential privacy risks.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

As such, the responsible entity shall review and record the findings of potential limitations in network security and privacy capabilities of the system and assess the privacy vulnerabilities of the architecture and the system's implementation.

7.3.1 Data map

Organizations shall map the system's processing of data to a level of detail that is commensurate with the risk. This process may be an evolving process as more detail is added to the map over time.

In order that the processing of the data can be appropriately understood, the data map shall include the following:

- The data being processed, including the specific data elements and the sensitivity of these elements
- Discrete data actions or operations the system is taking
- Components of the system involved in the data actions
- The owners or operators of those components
- Where the data is being processed (e.g., the data processing environment, whether it is by a third party entity, and the geography and jurisdictions involved)
- The mechanism by which the data is being processed (e.g., if the data action is visible to the individual or is processed on the backend of the system, for instance by an algorithm or an individual, automated or not)
- The purposes for which the data is being processed
- The data map may include the roles of the entities involved in the data actions

7.3.2 Privacy capabilities and objectives

Privacy capabilities can be used to describe the system property or feature that produces the desired privacy outcome. Some organizational privacy requirements or principles are easily translated into privacy capabilities. For instance, if individuals have a right to request data deletion, then the system shall support capabilities for identifying information about a given individual and deleting it, if in compliance with applicable laws and regulations. Other privacy requirements or principles can be more challenging to translate into capabilities. What do the principles of fairness, transparency, or data minimization mean in engineering terms? To help bridge between principles and engineering it can be helpful to consider privacy engineering objectives. Security system engineers use the security objectives of confidentiality, integrity, and availability to consider the security capabilities for a system. Organizations can use privacy engineering objectives to support the determination of privacy capabilities, considering mission/business needs, risk tolerance, and organizational privacy requirements (see Clause 5).

These objectives are properties of the system that align with the principles and are testable statements. For instance, the principle of data minimization, whereby only the minimum data that is necessary for a given purpose should be processed, can be made actionable by considering whether there is data processed by the system that could be removed without affecting the functionality of the system. An aspect of the principle of fairness is that individuals be treated in line with their reasonable expectations; this can be evaluated by looking at whether data is processed for purposes that the user would have predicted or expected.

An organization may also use privacy engineering objectives as a prioritization tool. Systems that are low in these objectives may be a signal of increased privacy risk, and therefore merit a more comprehensive privacy risk assessment. Although the privacy capabilities inform the privacy risk assessment (see 7.4) by supporting risk prioritization decisions, the privacy capabilities may also be informed by the risk assessment and adjusted to support the management of specific privacy risks or address changes in the environment,

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

including design changes to the system. While a risk assessment can help to identify specific risks in a system, layering privacy engineering objectives into the design process can help the system protect privacy by design and default, potentially mitigating unforeseen risks. Objectives also enable engineers to communicate about system properties using a common and meaningful description, which allows systems to be compared based on defined testable statements about their properties.

One example is the NIST privacy engineering objectives as follows:

— Predictability: Enabling reliable assumptions by individuals, owners, and operators about data and its processing by a system. How can the system enable reliable assumptions about data processing?

— Manageability: Providing the capability for granular administration of data including alteration, deletion, and selective disclosure. What data needs to be managed and how?

— Disassociability: Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system. How can data be dissociated from individuals or devices while still permitting functionality in the system?

The European Network and Information Security Agency (ENISA) in the EU has proposed data protection goals of unlink ability, transparency, and intervenability. These goals can provide an additional perspective for organizations to consider in deriving system capabilities.

These goals should be seen not as specific principles or requirements, rather these are suggested capabilities to consider including in organizational framework (Clause 6) and can provide a way of assessing and reasoning about the privacy properties of a system. They may be complementary to regulatory requirements, principles, and standards, but do not necessarily map directly to them and may be in addition to those requirements.

7.4 Risk assessment

The aim of a data privacy process is to design systems that can deliver the desired functionality and satisfy the privacy requirements. This is done by first identifying all the relevant inputs for mapping the system requirements, with respect to functionality and privacy. A special category of input is a privacy risk assessment. A privacy risk assessment is a process by which an organization can identify, given the intended system design and functionality, the potential risks that may result from the processing of personal data, and where system changes or controls may be required, and should recommend that the risks be prioritized. What constitutes a privacy risk and how privacy risk is perceived may vary across different cultures and within different legal jurisdictions. There exists a variety of sources that explore what constitutes privacy harms in detail. For examples see Annex A.

Looking at potential risks may help organizations turn high-level requirements into more specific requirements which can be satisfied through privacy controls.

An assessment may cover the system's life cycle, including its development. It may include a conceptual, logical, and physical assessment of the system in the context of the organizational environment as set out above. It should also address the life cycle of the data in the system, which may not be the same as the life cycle of the system. A completed privacy risk assessment shall include recommendations that may include key controls or metrics to provide for identified risks to be managed.

Prior to carrying out a formal risk assessment, organizations may first carry out a preliminary evaluation to determine whether and to what degree a more in-depth risk assessment is needed.

For further guidance on how to decide when to do a risk assessment, see examples in Annex A.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

A privacy impact assessment (PIA) or data protection impact assessment (DPIA) is a structured form of risk assessment, typically formalized by a standards body or law. Some regulations, such as the GDPR, require impact assessments to be carried out in some situations, and describe requirements for these processes. Risk assessments of this kind combine an assessment of risk with specific processes and other legal requirements. They may also dictate how the organization needs to respond to identified risks (see 8.1). As such, there are benefits of adopting a formalized PIA or DPIA process, but it is worth considering which it is most appropriate to adopt given the organization's privacy context and organizational privacy framework.

Various existing and widely used methodologies for conducting a privacy risk assessment are available. For examples, see Annex A. Some of these are formulated with specific privacy requirements already in mind, such as the data protection impact assessment methodologies designed by the UK's ICO, France's CNIL, or Singapore's PDPC, which are designed for the purpose of complying with the GDPR. Additionally, NIST has defined a risk assessment methodology. Which methodology it is most advisable to use will vary depending on the user.

When an organization carries out a privacy risk assessment, the risk assessment shall be conducted using a documented risk assessment methodology based on the policy established in 6.2 and be proportional to the overall privacy risk of the product/system/application. A risk assessment methodology shall include:

— A risk model: This identifies the factors to be analyzed and the relationship between those factors.

— An analysis approach: For instance, what are the potential risks that could result from attacks on or misuse of the system, or what attacks or types of misuse would the system be vulnerable?

— An assessment approach to identify and analyze privacy risks: This allows an organization to prioritize and categorize the identified risks based on qualitative, quantitative, or semiquantitative approaches, e.g., a heat map.

— An associated action plan for the assessment (see Clause 8).

Combining the various elements, business needs, system functionality and design, including data map, and the risk assessment provides the minimum system characterization.

8. Privacy risk management

8.1 Responding to risks in the proposed system environment

The desired output of the risk assessment process described in 7.4 is a set of prioritized risks. There are four ways of responding to risks as follows:

— Control/modify/mitigate: Implement actions to reduce the impact or likelihood of the risk (e.g., the use of privacy controls to mitigate and manage identified risks). While risk cannot be eliminated entirely, and some degree of residual risk may always exist, risk should be reduced to an acceptable degree through mitigation.

— Transfer/sharing: Reassign accountability, responsibility, and authority to a third-party willing to accept the risk (e.g., utilize a third-party service provider with stronger privacy controls and capabilities).

— Avoidance: Adjust system requirements to eliminate or reduce any exposure to the risk when unwanted negative consequences exceed the level of the organization's risk tolerance. (e.g., remove feature, process, or cancel project).

— Acceptance/retention: Acknowledge the existence of a particular risk and accept it without engaging in further efforts to control it. Approval of stakeholders and ongoing monitoring is required (i.e., noting the risk and proceeding).

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

It is recommended that implementers be familiar with ISO/IEC 27005:2018 (see [B6]) as a helpful reference.

Subclause 8.3 looks at how privacy risk can be mitigated and to a certain the extent of how risk can be shared, for instance through amending a privacy notice.

How an organization responds to identified risks may largely be dictated by the organizational privacy framework (see Clause 6), the business need (see 7.2) and the risk assessment (see 7.4). Note that, like other stages of this standard, this is an iterative process. It may be that controls need to be explored, a new risk assessment carried out, and then a new decision on the residual risk evaluated.

In deciding how to respond to risks it is important to weigh the potential benefit against these risks. If the risks outweigh the benefits, and feasible controls are not able to mitigate these risks effectively, the organization may need to change the system and potentially lose some of the key functionality of the system and the subsequent desired business benefit or drop the project altogether. Similarly, if the risks are acceptable, an appropriate response may be to accept them. Given that risk can never be eliminated entirely this may be part of the response to any assessment.

Where the decision is made to accept a risk, or not meet a privacy or business requirement, organizations shall have an authorization process whereby relevant stakeholders are included to agree to that decision and that the determination is made by an authorized individual (see 6.3).

In some instances, this may also need to include external stakeholders, such as a partner or regulator. What is deemed an acceptable level of risk is a decision for the organization to make based on its organizational privacy requirements (see Clause 5), and should be reflected in its organizational privacy framework (see Clause 6).

For each requirement and risk organizations shall document the risk response decision. This documentation may include the justification for this decision, mapping each requirement and risk to a response, such as a control, or a decision to accept a risk.

This is important for a range of reasons, including defending a decision in the event an accepted risk results in that risk being realized, or if a business line is affected by changes to the system due to avoidance and wants to understand the justification for this.

8.2 Privacy controls for risk mitigation

The organization shall identify an external controls baseline set, or develop its own internal set, and map the requirements to this set.

The organization shall document an architecture diagram displaying the attributes within the architecture, and the ontology of these key attributes.

Privacy control baseline sets are predefined collections of controls specifically assembled to address the protection needs of groups, organizations, or communities of interest. These sets may be altered over time through a tailoring process, should it become clear that requirements cannot be met with the baseline set. Not all controls in the baseline set will always be needed for each system.

Privacy controls encompass any technical or organizational approach that mitigates an identified privacy risk and satisfies an identified privacy requirement. System requirements (see Clause 7) include requirements that certain risks are mitigated to an acceptable degree, so that there is an acceptably low risk of inadvertent disclosure, as well as specific functional requirements, e.g., allowing data to be amended.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Privacy controls should be selected based on the identified system privacy requirements (see Clause 7). Once implemented the privacy controls efficacy with respect to those requirements should be assessed, with possible changes then made.

Before implementing any controls, it is worthwhile to carry out an initial review where the impact of the controls is assessed and the various system design mapping, evaluation, and first order risk assessment processes are redone, if appropriate. Several variations or iterations of this may be required before deciding on which controls will be used in practice.

Once a set of privacy controls has been assessed as being sufficient, the controls still need to be monitored over time to continue to be effective ways of achieving their stated objectives.

Note that there is significant overlap between privacy and security controls, although each may be aiming to achieve different things. For instance, access controls may be security controls to prevent unauthorized access by a third party, but they can also be used as privacy controls to limit what an internal party is able to do with the data. As such, it may be advisable to consider the planned or actual security controls alongside the planned or actual privacy controls.

Various resources are available which list commonly used privacy controls, although how these controls are categorized varies, for instance, by the nature and type of control, by the privacy principle the control delivers on, or by the strategy the control is aiming to deliver. For an example list of privacy controls by NIST see Annex A.

8.2.1 Privacy control selection

Organizations shall select appropriate privacy controls to meet their identified system requirements and document their selection.

A risk assessment should be used to identify the scale and nature of the risk, so an appropriate mitigation or other response, such as transfer of risk, can be identified. Privacy controls should then be selected considering the system requirements. Some privacy controls may limit desired system functionality and may not be appropriate for a given system, or the necessity of those requirements may need to be reviewed. Once a set of privacy controls has been selected, it should be reviewed with respect to the risk assessment and organizational requirements.

Privacy controls vary significantly in various ways, including but not limited to the following:

- The cost of implementation, in terms of the cost of implementing the control and the operating cost
- The size of impact with respect to the residual risk and the utility of the data (e.g., pseudonymizing data by removing identifiers will have less of an impact than anonymizing a data set through more advanced de-identification)
- Scalability (e.g., the use of a secure location for sensitive analysis may be an effective control, but expensive to maintain and difficult to scale)
- Supporting architectures (e.g., whether the system has a centralized architecture or a distributed one. There may be equivalent controls to achieve similar results in either, but how it is done may be different.)
- The nature of impact (e.g., one control might reduce the identifiability of an individual, while another provides the individual with more control over how data is processed)
- The type of control (i.e., a technical control that alters or acts on the data in some way, versus an organizational control that creates a new governance process that alters the way those interacting with the system behave)

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

— Complexity or accessibility (i.e., more advanced controls such as differential privacy can provide powerful privacy guarantees, but may require significant expertise to deploy)

When selecting controls organizations should consider not just the efficacy of the control in mitigating a given risk, but also factors such as the cost and expertise required to implement the control, or the dependencies or restrictions resulting from the selected control. There are often many ways in which privacy risk can be managed, and direct comparison of the efficacy of different controls and between systems may be difficult. Privacy risk is inherently contextual and dependent on the data, the intended processing, and the environment in which the processing will take place. In particularly complex situations it may be advisable to consult with those with experience in the field during control selection to help your organization achieve the desired privacy properties.

8.2.2 Privacy control implementation

Control implementation will vary with the stated control and may be system dependent. Controls should be implemented within the SDLC process (see Clause 9).

The organization shall identify any material differences between the controls planned and the controls that are implemented, and shall update plans to reflect the actual implementation.

In some instances, controls planned in the initial review may not be possible or may require refinement in practice. Where the controls are not possible or vary markedly from the plan, it may be necessary to go back to the control selection stage.

It is recommended that those implementing controls follow best practices for the implementation of specific controls, and in some instances that the implementation strategy be reviewed by one skilled in the art or practice.

8.2.3 Privacy control assessment

All privacy controls shall be assessed to confirm that they are implemented correctly, operating as intended, and producing the desired outcome or meeting the system privacy requirements.

The privacy control assessment results in a reporting of the findings, including recommendations for correcting deficiencies in the implemented controls. This should be carried out by assessors with the necessary skills to perform the assessment effectively. In some instances, it may be appropriate for these assessors to be independent of the system owner. The assessment should follow an assessment plan or procedure that details how the efficacy of the controls will be assessed., and what means of assessment will be utilized—reviewing documents, interviewing staff, penetration testing, etc.

Where controls are found to be deficient to meet the system requirements and identified privacy risks, the controls need to be reviewed and the control selection or implementation process revisited, or the system needs to be changed in some other way that alters the system requirements. Where the system is live and immediate remediation is not possible, a plan of action should be drawn up that details how the issue(s) will be resolved and responded to, which shall include ownership of any risk by the appropriate individual or entity.

Once new controls have been implemented, another assessment shall be done, and the process repeated until the implemented controls can be shown to meet the stated requirements.

8.3 Ongoing system privacy risk management

The various factors that shaped the decision-making process around how privacy was managed within a given system are all subject to change. The privacy context can be dramatically altered by new regulations or changes in the stage of the life cycle of the system. The business need can alter based on product and business strategy

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

changes, as well as the organization's view of risk based on cultural changes and current events. New controls and technologies can offer new ways of responding to identified risks. Additionally, systems themselves are often changed over time and many controls require ongoing actions and effectiveness reviews. For example, training may need to be repeated or altered as staff and roles change over time.

Organizations shall continually monitor changes in the system and the context it operates within, including changes to the wider context the organization is in, the organization's privacy framework, and the operations of the systems and the ongoing efficacy of their privacy controls.

One way of doing this is by carrying out periodic audits and reviews. This should be covered in the organizational privacy framework (Clause 6). These reviews should be expansive in nature, looking at the following:

— Have the requirements changed because of changes in the organizational privacy framework or system characterization?

— Was the reasoning for the selection of the controls and their objectives sound? Does it continue to be sound considering any changes since their selection and implementation?

— Do the controls continue to achieve their intended purpose? Do they pass a predefined quality assurance process?

— Has the implementation been changed by system alterations?

9. Privacy in the systems development life cycle

9.1 General

The systems development life cycle (SDLC) is a model used to develop technology within a stepwise process. Defining the functional requirements for a system is an essential part of the SDLC, regardless of the methodology used (e.g., waterfall, agile). This subsection describes a process to identify, define, support, and implement qualitative system privacy requirements in the traditional SDLC process.

The SDLC model provides logical input and output points to enable privacy and security controls (technical and administrative) to be inserted, validated, operated, and monitored for effectiveness. These stages are life cycle development agnostic and, for instance, should be applicable for waterfall and agile development methodologies. Figure 6 shows a phase-gate model[11] that inserts six key control points into the standard.

[11]There are numerous development life cycle models with varying terms, for purpose of this standard this SDLC was selected to ensure a broad range of phases, steps, or gates would be covered in this standard.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

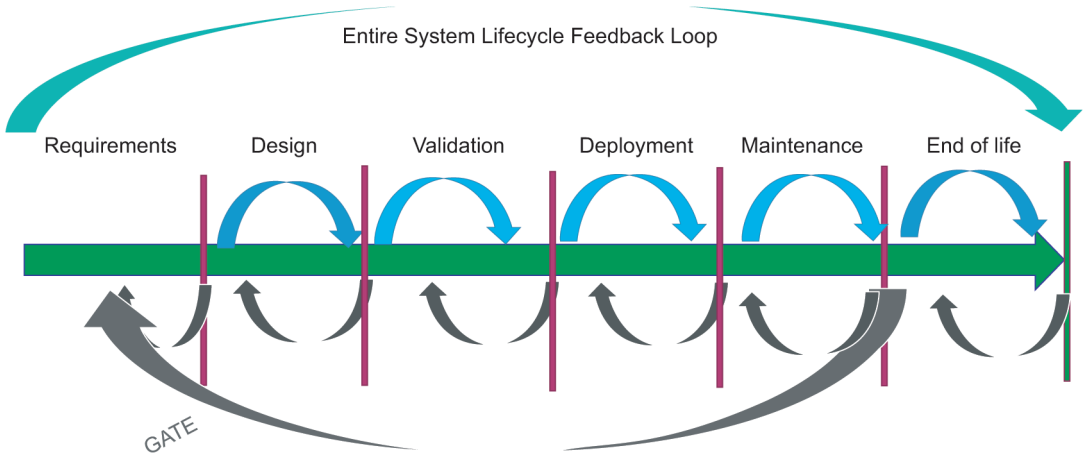

Figure 6—Systems development life cycle privacy phase gates

The six phase-gates follow each major step within the SDLC to help manage privacy requirements and controls. The phase-gates are to be considered project and program governance points that establish specific criteria for privacy and security controls to be designed, tested, implemented, operated, and monitored in a manner that is consistent with applicable laws, regulations, standards, and principles.

9.2 Privacy life cycle management

IEEE Std 7002 is compatible with existing product and system development practices, including iterative and incremental life cycle models, as well as agile methods. The intent of IEEE Std 7002 is to assist stakeholders in understanding that personal data management is part of the system life cycle and that addressing each stage of the development process is appropriate to ensure compliance and integrity. It is recommended that users and implementers of IEEE Std 7002 be familiar with ISO/IEC/IEEE 15288:2015 (see [B12]).

Table 2 shows the SDLC stages and phase gates. The SDLC process shall, in some form, address each of the phase gates.

Table 2—Systems development life cycle privacy phase descriptions

Stage	Description	Phase gate
Pathfinding or concept development	This is phase in which the idea for what is being developed is researched and committed to.	Identify what personal data will be processed and underlying personal data actions.
Requirements	The requirements phase integrates privacy into the SDLC process. A risk assessment is completed, and privacy requirements and controls are identified to mitigate the risk.	Identify what the privacy controls should be (see Clause 7 and Clause 8).
Design	The design phase translates privacy requirements and controls into features or functionalities.	Analyze the implementation of planned privacy controls designed to deliver the intended functionality based on the requirements, standards, and principles that were determined by the processes stated above.
Validation	The validation phase validates traceability to all privacy requirements and transforms the design into the final system attributes. All privacy requirements should be met and operate as expected, in accordance with applicable laws and regulations.	Verify that the privacy controls are effective, meet privacy requirements, and conform to the applicable laws, regulations, standards, and principles.

Table continues

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Table 2—Systems development life cycle privacy phase descriptions *(continued)*

Stage	Description	Phase gate
Deployment	In the release phase a final privacy review is completed to help understand any residual risk and provide input into the deployment decision.	Confirm the privacy controls are functioning properly in the environment to which they are deployed.
Maintenance	The maintenance phase provides for a consistent disclosure and response process for dealing with privacy, and monitors changes to the environment and applicable privacy requirements.	Monitor the appropriate environment for changes that may alter the system requirements and confirm that the controls selected continue to be effective, that they fulfill on-going compliance requirements, and that they are properly configured and implemented to detect privacy vulnerabilities, threats, and risks.
End of life	The phase includes secure disposition of the data, including archiving or transfer.	Delete, transfer, or archive the data as required based on a retention timeline, which specifies how long data should be retained in the system based on the relevant requirements. Retention schedules may be mandated by specific legal or legitimate business requirements. Closed-loop product life cycle is an attempt to extend a system or product's use and may include refurbishing or redesign. The end-of-life (EOL) phase of a product life cycle may now constitute contrasting scenarios that may include refurbishing, reuse, component disassembly and refurbishment, material reclamation (no disassembly), material reclamation (with disassembly), or complete disposal (with or without incineration). With today's evolving technology, product and EOL planning may be an integral part of the system life cycle management process, so it is recommended that privacy requirements be considered through the product life cycle, and for different EOL scenarios.

Governance of the SDLC process operates at two levels. First, the process of governing the inclusion of privacy controls into the SDLC. Second, the governance that the SDLC process is being followed in conformance with the organizational privacy framework and the governance structures therein.

Within the maintenance phase, organizations should consider the retirement of its systems and data and how this will be managed. This should be with respect to the data life cycle and the system life cycle.

As described in Clause 7, any changes resulting from the SDLC process should be documented and resulting actions completed in the iterative way described.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Annex A

(informative)

Examples

A.1 Examples from Clause 5

Examples of existing privacy principles (see 5.3.1) include the following:[12]

— Fair Information Practices (FIPs). First developed by the US Government in 1973, FIPs, aka Fair Information Practice Principles (FIPPs), have evolved over time.[13,14]

— Building on the US Government's initial work on FIPS, the Organization for Economic Co-operation and Development (OECD) issued their own set of principles in 1981.[15]

— In 1981 the Council of Europe passed the first legally binding international instrument for data privacy principles, called Convention 108. This served as a basis for the principles in the first wave of data protection legislation in the 80s and 90s, first in Europe and then globally.[16]

— An alternative approach to the FIPS principles was developed in the mid-90s by Canadian and Dutch Government bodies. This work was published in 2009 and 2011 by the Provincial Government of Ontario in Canada, as the seven foundational privacy by design principles. Like the FIPs, privacy by design, or PbD, principles have evolved over time.[17]

— In 2005 ministers of the Asia-Pacific Economic Cooperation (APEC) group adopted the APEC privacy framework. As with other sets of principles it was similar to those that came before. The framework was updated in 2015.[18]

— In 1995 the European Union passed the Data Protection Directive, which included a set of principles. These were then updated in 2016 with the General Data Protection Regulation (GDPR). Article five of the GDPR cites seven general principles of data protection.[19]

A.2 Examples from Clause 6

For examples of organizations' privacy policies (see 6.2) that have been published online, see the following:

— The Kantara Initiative has posted guidance on certain key privacy policy topics.[20]

— Intel Corporation's internal policy rules.[21]

— Cisco's Global Privacy Policy.[22]

[12]For a more thorough discussion of the history of privacy principles, see: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.
[13]The first set of FIPs can be found here: https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
[14]A more recent version can be found on the website of the International Association of Privacy Professionals (IAPP): https://iapp.org/resources/article/fair-information-practices/.
[15]Principles issued by OECD can be found at: http://oecdprivacy.org/.
[16]More information can be found at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.
[17]More information on PbD principles can be found at: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf and at http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf .
[18]More information on the APEC framework can be found at: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).
[19]For more information on the Data Protection Directive, see: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.
[20]See https://kantarainitiative.org/reports-recommendations.
[21]See https://www.intel.com/content/www/us/en/privacy/eea-binding-corporate-rules.html.
[22]See https://www.cisco.com/c/en/us/about/trust-center/data-protection-and-privacy-policy.html.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

A.3 Examples from Clause 7

For examples of data maps (see 7.3.1) see the following:

a) Cisco hosts a range of example data maps online[23]

b) NIST provides an example data map in Worksheet 2 of the NIST Privacy Risk Assessment Methodology (PRAM)[24]

c) For examples of data privacy harms (see 7.4), see the following:

   1) The work of Professor Solove[25]

   2) The US National Institute for Standards and Technology (NIST) Internal Report 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems[26]

   3) Legal scholar Ryan Calo's "The Boundaries of Privacy Harm"[27]

   4) The Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection regulator, knowledgebase for privacy impact assessments[28]

   5) Recital 75 of the GDPR[29]

For guidance on when to carry out a risk assessment (see 7.4), see the following:

— The EU's A29WP guidance on when to do a Data Protection Impact Assessments[30]

— Appendix D of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0[31]

For examples of risk assessments (see 7.4) see the following:

— The PDPC's guide to data protection impact assessments[32]

— CNIL's guide to risk assessment[33]

— The ICO's guidance on carrying out a DPIA[34]

— The European Data Protection Board's guidance on carrying out DPIA[35]

— NIST Privacy Risk Assessment Methodology (PRAM)[36]

A.4 Examples from Clause 8

See NIST SP 800-53 ([B18]) on controls.[37]

[23]See https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html#~privacydatadocs.
[24]See https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources#pram.
[25]See https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf.
[26]See https://doi.org/10.6028/NIST.IR.8062 https://doi.org/10.6028/NIST.IR.8062.
[27]See http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf.
[28]See https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf.
[29]See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.
[30]See https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[31]See https://www.nist.gov/document/nist-privacy-frameworkv10pdf.
[32]See https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-dpias---011117.pdf.
[33]See https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf.
[34]See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.
[35]See https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.
[36]See https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources#pram.
[37]See https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

A.5 General resources

For more information on current privacy engineering projects, see The Internet Privacy Engineering Network.[38]

[38]See https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards.

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

Annex B

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] GDPR—General Data Protection Regulation—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.

[B2] IEEE Std 802.1Q™-2014, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks.[39,40]

[B3] ISO/IEC 15408-1:2009, Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model.[41,42]

[B4] ISO/IEC TS 19608:2018, Guidance for developing security and privacy functional requirements based on ISO/IEC 15408.

[B5] ISO/IEC 27001, Information Security Management.

[B6] ISO/IEC 27005:2018, Information technology—Security techniques—Information security risk management.

[B7] ISO/IEC TR 27550:2019, Information technology—Security techniques—Privacy engineering for system life cycle processes.

[B8] ISO/IEC 29100:2011, Information technology—Security techniques—Privacy framework,ISO 29101.

[B9] ISO/IEC 29134:2017–06 Information technology—Security techniques—Guidelines for privacy impact assessment.

[B10] ISO/IEC 38505-1:2017, Information technology—Governance of IT—Governance of data—Part 1: Application of ISO/IEC 38500 to the governance of data.

[B11] ISO/IEC/IEEE 12207:2017, Systems and software engineering—Software life cycle processes.

[B12] ISO/IEC/IEEE 15288:2015, Systems and software engineering—System life cycle processes.

[B13] ISO/IEC/IEEE 16085, Systems, and software engineering—Life cycle processes—Risk management.

[B14] ISO/IEC/IEEE 24765, Systems and software engineering—Vocabulary.

[39]The IEEE standards or products referred to in Annex B are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.
[40]IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).
[41]IEC publications are available from the International Electrotechnical Commission (https://www.iec.ch) and the American National Standards Institute (https://www.ansi.org/).
[42]ISO publications are available from the International Organization for Standardization (https://www.iso.org/) and the American National Standards Institute (https://www.ansi.org/).

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

[B15] ISO/IEC/IEEE 24748-3:2020(E) Systems and software engineering—Life cycle management —Part 3: Guidelines for the application of ISO/IEC/IEEE 12207 (software life cycle processes).

[B16] ISO/IEC/IEEE 24774:2021 Systems and software engineering—Life cycle management—Specification for process description.

[B17] NIST Special Publication 800–37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (2018). [43]

[B18] NIST Special Publication 800–53, Revision 5, Security and Privacy Controls for Information Systems and Organizations.

[B19] NIST Special Publication 800–122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

[43]NIST publications are available from the National Institute of Standards and Technology (https://www.nist.gov/).

Copyright © 2022 IEEE. All rights reserved.
Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 16:38:35 UTC from IEEE Xplore. Restrictions apply.

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Twitter: twitter.com/ieeesa
Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE

Authorized licensed use limited to: Sanad AlArousi. Downloaded on December 07,2024 at 18:38:35 UTC from IEEE Xplore. Restrictions apply.