INTERNATIONAL STANDARD

ISO/IEC 29134

First edition
2017-06

Information technology — Security techniques — Guidelines for privacy impact assessment

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'évaluation d'impacts sur la vie privée

Reference number
ISO/IEC 29134:2017(E)

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

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

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

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

A privacy impact assessment (PIA) is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information (PII) and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. A PIA report may include documentation about measures taken for risk treatment, for example, measures arising from the use of the information security management system (ISMS) in ISO/IEC 27001. A PIA is more than a tool: it is a process that begins at the earliest possible stages of an initiative, when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and even after, the project has been deployed.

Initiatives vary substantially in scale and impact. Objectives falling under the heading of "privacy" will depend on culture, societal expectations and jurisdiction. This document is intended to provide scalable guidance that can be applied to all initiatives. Since guidance specific to all circumstances cannot be prescriptive, the guidance in this document should be interpreted with respect to individual circumstance.

A PII controller may have a responsibility to conduct a PIA and may request a PII processor to assist in doing this, acting on the PII controller's behalf. A PII processor or a supplier may also wish to conduct their own PIA.

A supplier's PIA information is especially relevant when digitally connected devices are part of the information system, application or process being assessed. It may be necessary for suppliers of such devices to provide privacy-relevant design information to those undertaking the PIA. When the provider of digital devices is unskilled in and not resourced for PIAs, for example:

— a small retailer, or

— a small and medium-sized enterprise (SME) using digitally connected devices in the course of its normal business operations,

then, in order to enable it to undertake minimal PIA activity, the device supplier may be called upon to provide a great deal of privacy information and undertake its own PIA with respect to the expected PII principal/SME context for the equipment they supply.

A PIA is typically conducted by an organization that takes its responsibility seriously and treats PII principals adequately. In some jurisdictions, a PIA may be necessary to meet legal and regulatory requirements.

This document is intended to be used when the privacy impact on PII principals includes consideration of processes, information systems or programmes, where:

— the responsibility for the implementation and/or delivery of the process, information system or programme is shared with other organizations and it should be ensured that each organization properly addresses the identified risks;

— an organization is performing privacy risk management as part of its overall risk management effort while preparing for the implementation or improvement of its ISMS (established in accordance with ISO/IEC 27001 or equivalent management system); or an organization is performing privacy risk management as an independent function;

— an organization (e.g. government) is undertaking an initiative (e.g. a public-private-partnership programme) in which the future PII controller organization is not known yet, with the result that the treatment plan could not get implemented directly and, therefore, this treatment plan should become part of corresponding legislation, regulation or the contract instead;

— the organization wants to act responsible towards the PII principals.

Controls deemed necessary to treat the risks identified during the privacy impact analysis process may be derived from multiple sets of controls, including ISO/IEC 27002 (for security controls) and ISO/IEC 29151 (for PII protection controls) or comparable national standards, or they may be defined by the person responsible for conducting the PIA, independently of any other control set.

Information technology — Security techniques — Guidelines for privacy impact assessment

1 Scope

This document gives guidelines for

— a process on privacy impact assessments, and

— a structure and content of a PIA report.

It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.

This document is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO Guide 73:2009, *Risk management — Vocabulary*

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100, ISO/IEC 27000, ISO Guide 73 and the following apply.

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

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

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

3.1
acceptance statement
formal management declaration to assume responsibility for risk ownership, risk treatment and residual risk

3.2
asset
anything that has value to anyone involved in the processing of personally identifiable information (PII)

Note 1 to entry: In the context of a privacy risk management process, an asset is either PII or a supporting asset.

3.3
assessor
person who leads and conducts a *privacy impact assessment* (3.7)

Note 1 to entry: The assessor may be supported by one or more other internal and/or external experts as part of their team.

Note 2 to entry: The assessor may be an expert internal or external to the organization.

3.4
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: *ISO/IEC Directives, Part 1, Consolidated ISO Supplement*:2014, 3.12]

3.5
device
combination of hardware and software, or solely software, that allows a user to perform actions

3.6
privacy impact
anything that has an effect on the privacy of a PII principal and/or group of PII principals

Note 1 to entry: The privacy impact could result from the processing of PII in conformance or in violation of privacy safeguarding requirements.

3.7
privacy impact assessment
PIA
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework

Note 1 to entry: Adapted from ISO/IEC 29100:2011, 2.20.

3.8
privacy risk map
diagram that indicates the level of impact and likelihood of privacy risks identified

Note 1 to entry: The map is typically used to determine the order in which the privacy risks should be treated.

3.9
programme
group of projects managed in a coordinated way to obtain benefits not available from managing them individually

[SOURCE: ISO 14300-1:2011, 3.2]

3.10
project
unique process, consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources

[SOURCE: ISO 9000:2015, 3.4.2]

3.11
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: *ISO/IEC Directives, Part 1, Consolidated ISO Supplement*:2014, 3.01]

3.12
severity
estimation of the magnitude of potential impacts on the privacy of a PII principal

3.13
system
information system
applications, services, information technology assets, or other information handling components

[SOURCE: ISO/IEC 27000:2016, 2.39]

3.14
stakeholder
person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: Includes PII principals, management, regulators and customers.

Note 2 to entry: Consultation with stakeholders is integral to a PIA.

[SOURCE: *ISO/IEC Directives, Part 1, Consolidated ISO Supplement*:2014, 3.02 – modified – The preferred term "interested party" has been removed from this entry.]

3.15
technology
hardware, software, and firmware systems and system elements including, but not limited to, information technology, embedded systems, or any other electro-mechanical or processor-based systems

[SOURCE: ISO/IEC 16509:1999, 3.3]

4 Abbreviated terms

API	application programming interface
BYOD	bring your own device
ICT	information and communication technologies
ISMS	information security management system
PII	personally identifiable information
SME	small and medium-sized enterprises

5 Preparing the grounds for PIA

5.1 Benefits of carrying out a PIA

This document provides guidance that can be adapted to a wide range of situations where PII is processed. However, in general, a PIA can be carried out for the purpose of:

— identifying privacy impacts, privacy risks and responsibilities;

— providing input to design for privacy protection (sometimes called privacy by design);

— reviewing a new information system's privacy risks and assessing its impact and likelihood;

— providing the basis for the provision of privacy information to PII principals on any PII principal mitigation action recommended;

— maintaining later updates or upgrades with additional functionality likely to impact the PII that are handled;

— sharing and mitigating privacy risks with stakeholders, or providing evidence relating to compliance.

NOTE A PIA is sometimes referred to by other terms, for example, a "privacy review" or a "data protection impact assessment". These particular instances of a PIA could come with specific implications for both process and reporting.

A PIA has often been described as an early warning system. It provides a way to detect potential privacy risks arising from the processing of PII and thereby informing an organization of where they should take precautions and build tailored safeguards before, not after, the organization makes heavy investments. The costs of amending a project at the planning stage will usually be a fraction of those incurred later on. If the privacy impact is unacceptable, the project may even have to be cancelled altogether. Thus, a PIA helps to identify privacy issues early and/or to reduce costs in management time, legal expenses and potential media or public concern by considering privacy issues early. It may also help an organization to avoid costly or embarrassing privacy mistakes.

Although a PIA should be more than simply a compliance check, it does nevertheless contribute to an organization's demonstration of its compliance with relevant privacy and data protection requirements in the event of a subsequent complaint, privacy audit or compliance investigation. In the event of a privacy risk or breach occurring, the PIA report can provide evidence that the organization acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.

An appropriate PIA also demonstrates to an organization's customers and/or citizens that it respects their privacy and is responsive to their concerns. Customers or citizens are more likely to trust an organization that performs a PIA than one that does not.

A PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions on privacy issues about the project. A PIA is a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision makers. A PIA can be a credible source of information.

A PIA enables an organization to learn about the privacy pitfalls of a process, information system or programme upfront, rather than having its auditors or competitors point them out. A PIA assists in anticipating and responding to the public's privacy concerns.

A PIA can help an organization gain the public's trust and confidence that privacy has been built into the design of a process, information system or programme.

Trust is built on transparency, and a PIA is a disciplined process that promotes open communications, common understanding and transparency. An organization that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them to do so too. A PIA is a way of educating employees about privacy and making them alert to privacy problems that might damage

the organization. It is a way to affirm the organization's values. A PIA can be used as an indication of due diligence and may reduce the number of customer audits.

5.2 Objectives of PIA reporting

The PIA reporting objective is to communicate assessment results to stakeholders. Expectations from a PIA exist from multiple stakeholders.

The following are typical examples of stakeholders and their expectations.

— PII principal – PIA is an instrument to enable subjects of PII to have assurance that their privacy is being protected.

— Management – Several viewpoints apply with

  — PIA as an instrument to manage privacy risks, create awareness and establish accountability; visibility over PII processing within the organization, and possible risks and impacts of the same; inputs to business or product strategy;

  — Building the PIA into the earliest stages of the project ensures the privacy requirements are included in the functional and non-functional requirements; are achievable, viable and traced through change and risk management and may result in the project not happening or being cancelled. The effort to classify and manage project PII should be funded as a separate investment line item and amount in a project or programme budget, acceptable to all stakeholders;

  — PIA as an opportunity to better understand privacy requirements and assess activities against these requirements; inputs for product or service design and delivery; reviewed and amended through the change management process after delivery;

  — PIA as an instrument to understand the privacy risks at the function/project/unit level; consolidation of risks; input to privacy policy design and enforcement mechanisms; inputs for re-engineering privacy processes.

— Regulator – PIA is an instrument that contributes evidence supporting compliance with applicable legal requirements. It can provide evidence of due diligence taken by the organization in case of breach, non-compliance, complaint, etc.

— Customer – PIA is a means to assess how the PII processor or PII controller is handling PII and provides evidence that it follows the contractual obligations.

PIA reporting should fulfil two basic functions. The first (Inventory) keeps the specific stakeholders informed of identified affected entities, affected environment and privacy risks about the life cycle of the affected entities, whether it is inherent or mitigated. The second (Action items) is a tracking mechanism on the actions/tasks that improve and/or resolve the identified privacy risks. Sensitivity to the distribution and release of the reporting information needs to be clearly assessed and classified (private, confidential, public, etc.).

5.3 Accountability to conduct a PIA

A PIA should be undertaken of processes or information systems by one of a number of different entities within the organization, but may also be carried out on a process, information system or programme by consumer organizations or non-governmental organizations.

Typically, the responsibility for ensuring that a PIA is undertaken should, in the first instance, lie with the person in charge of PII protection, otherwise with the project manager developing the new technology, service or other initiative that may impact privacy.

Accountability for ensuring the PIA is undertaken and the quality of the result (PIA accountability) should lie with the top management of the PII controller. The person who has been assigned responsibility for conducting the PIA may conduct it themselves, may enlist the help of other internal

and/or external stakeholders or may contract an independent third party to do the work. There are advantages and disadvantages to each approach.

However, when the PIA is performed directly by the organization, end-user associations or governmental agencies may request to have the PIA's adequacy verified by an independent auditor.

The organization should ensure that there is accountability and authority for managing privacy risks, including the implementation and maintenance of the privacy risk management process and for ensuring the adequacy and effectiveness of any controls. This can be facilitated by

— specifying who is accountable for the development, implementation and maintenance of the framework for managing privacy risk, and

— specifying risk owners for implementing privacy risk treatment, maintaining privacy controls and reporting of relevant privacy risk information.

5.4 Scale of a PIA

The scale of the PIA will depend on how significant the impacts are assumed to be. For example, if the impacts are assumed to affect only employees of the organization (e.g. the organization may wish to improve its access control by means of a biometric such as a thumbprint from each employee), then the PIA could engage only employee representatives and be relatively small scale. However, if a government department wishes to introduce a new identity management system for all citizens, it will need to conduct a much larger PIA involving a wide range of external stakeholders.

Organizations should provide self-assessment on the required scale of the PIA, in compliance with laws and regulations. The amount and granularity of the PII per person, the degree of sensitivity of PII, the number of PII principals and the number of people who have access to the PII that will be processed are the critical factors in determining this scale.

In the case of SMEs, non-profit or governmental organizations, the determination of the appropriate scale of the PIA can be jointly, but not bindingly, achieved by the person conducting a PIA (as per 5.3), the SME's senior management and/or advice from external experts as appropriate.

6 Guidance on the process for conducting a PIA

6.1 General

The scope of a PIA, the specific details of what it covers and how it is conducted all need to be adapted to the size of the organization, the local jurisdiction and the specific programme, information system or process that is the subject of the PIA. In Clause 6,

— the "Objective" is something that should be achieved,

— the "Input" provides guidance about what information may be needed to achieve the "Objective",

— the "Expected output" is the recommended target for the "Actions",

— "Actions", or their equivalents, are guidance on activities that may need to be carried out to achieve the "Objective" and create the recommended "Expected output", and

— "Implementation Guidance" provides more details of matters that may need to be considered in performing the "Actions".

The "Actions" in this clause, or equivalents, adapted to the desired scope and scale of a PIA may be implemented stand-alone by an organization. They are intended to form a reasonable basis for planning, implementing and following up the PIA in a wide range of circumstances.

The organization conducting a PIA process may wish to directly adapt the process guidance below to its specific PIA scale and scope or as one possible alternative to select a suitable risk-based management

system, such as ISO/IEC 27001, and integrate into it appropriately adapted elements of the guidance below, including the use of the PIA report (see Clause 7) to treat the privacy risks it identifies.

In this document, the term "conducting a PIA" is used to cover both an initial PIA where the necessary steps and actions are selected to match the particular PIA requirement and an update to an existing PIA where only the steps and actions necessary for the update are carried out.

Annex C provides further guidance on the understanding of terms used in this document.

To support SMEs in the PIA process, industry associations or bodies of SMEs should be encouraged to draw up codes of conduct providing valuable guidelines, and SMEs should be encouraged to take part in these activities. Reasonable codes of conduct would have to respect the values set forth in this document and could be endorsed by data protection authorities.

6.2 Determine whether a PIA is necessary (threshold analysis)

Objective: To determine whether a new or updated PIA is necessary.

Input: Information about the programme, information system or process under assessment.

Expected output: Threshold analysis result, and mandate to prepare a new or updated PIA if required, terms of reference and scope of the PIA decided.

Actions:

The organization's management should decide if a new or updated PIA is required.

If a new or updated PIA is required, the organization's management, in conjunction with the assessor to be, should define the terms of reference and determine the boundaries and applicability of the PIA to establish its scope. The organization should also decide on and document the scale of the PIA, the process to be used to perform the PIA, and on the target audiences, hence the nature and contents of the PIA reports to be produced.

Output of this process in terms of the threshold analysis result and the PIA scope and terms of reference should be documented in the PIA report (see 7.2).

Implementation Guidance:

An organization should conduct a new or updated PIA if it perceives impacts on privacy from

— a new or prospective technology, service or other initiative where PII is, or is to be, processed,

— a decision that sensitive PII (see ISO/IEC 29100:2011, 2.26) is going to be processed,

— changes in applicable privacy related laws and regulations, internal policy and standards, information system operation, purposes and means for processing data, new or changed data flows, etc., and

— business expansion or acquisitions.

An organization may wish to establish a policy setting out thresholds for triggering a new or updated PIA and initial technical and organizational measures to apply. Such a policy should take account of any applicable issues from those listed above, setting boundaries within which processing of PII may be developed and operated without triggering a new PIA.

6.3 Preparation of the PIA

6.3.1 Set up the PIA team and provide it with direction

Objective: To determine the scope of the PIA and the needed expertise and to formulate the terms of reference for conducting the PIA.

Input: Mandate to prepare a PIA (see 6.2).

Expected output: Responsible person appointed, risk criteria.

Actions:

A person responsible for conducting a PIA (the assessor) should be identified and appointed by the organization. The organization should also appoint the person accountable for signing off the PIA report.

The assessor should define the risk criteria and ensure that senior management agrees with the risk criteria to be used to evaluate the significance of risk. These criteria may be based on those shown in Annex A, or they may be defined separately by the organization, together with the criteria on how to estimate the level of impact and the risk with their respective scales. The assessor should also identify the criteria for risk acceptance and ensure that senior management agrees with these criteria.

Output of this process in terms of the risk criteria should be documented in the PIA report (see 7.3.2) and resources (see 7.3.3).

Implementation Guidance:

The criteria should reflect the organization's values, objectives and resources. When defining risk criteria, the assessor should consider the following factors:

— legal and regulatory factors that impact the safeguarding of the natural person's privacy and the protection of their PII;

— external factors such as industry guidelines, professional standards, company policies and customer agreements;

— factors predetermined by a specific application or in a specific use case context;

— other factors that can affect the design of information systems and the associated privacy safeguarding requirements.

The organization's management should examine separately privacy risks from a PII principal's point of view and privacy risks from the organization's point of view.

These criteria should be used later for privacy risk assessment and treatment. The person responsible for conducting a PIA should propose the terms of reference and the scope of the PIA.

In order to define the rules that have been used to evaluate the significance of the privacy risks, the assessor should address the following questions:

— What are the criteria used to estimate the level of impact for both the PII principal as well as the organization? (For example, the level of identification, sensitivity of the PII breached, numbers of PII principals affected and level of organizational impact.)

— What are the criteria used to estimate the likelihood? (For example, vulnerabilities of the supporting assets and capabilities of the risk sources to exploit the vulnerabilities.)

— What is(are) the scale(s) used to estimate the level of impact?

— What is(are) the scale(s) used to estimate the likelihood?

— What is the significance of each combination (level of impact and likelihood) used to evaluate the risks? In particular, what are the criteria for risk acceptance?

— What is the applicable strategy to treat each of them? In particular, what is the strategy for the risks that can be accepted?

— How is the strategy modified by the benefits of the processing of PII?

NOTE 1 These criteria will be consistent with the other risk criteria used within the organization.

NOTE 2 The opportunity to improve these criteria will be considered each time they are used.

The definition of the risk criteria should be based on the following:

— harm to users of the product, service or system. Harm may include physical, financial, reputational harm, embarrassment and invasion of domestic life. Further, when considering the impacts on an individual of privacy risks to their PII, the organization should consider different types of privacy such as bodily privacy, location and space privacy, behavioural privacy, privacy of communications, privacy of data and image, privacy of thoughts and feelings and privacy of association;

— legal and regulatory requirements, and contractual obligations;

— stakeholder expectations and perceptions, and negative consequences for goodwill and reputation;

— operational importance of availability, confidentiality and integrity of PII;

— the strategic value of the information process;

— the present value and future opportunity made by the information process, aka “strategic value”.

The terms of reference should spell out whether public consultations are to be held, to whom the PIA report is to be submitted, the nominal budget and timescale for the PIA, and whether the PIA report or a summary is to be published. The minimum requirements for a PIA should depend either on legal or regulatory constraints or on how significant an organization deems the privacy risks to be.

The assessor should conduct the PIA and, if necessary, obtain support from a team comprising, for example, of representatives from the ICT department, relevant business units and the legal department.

Conducting a PIA in an organization requires strong and sustained commitment by management of the organization. Management should ensure that the necessary resources are allocated to the PIA team.

6.3.2 Prepare a PIA plan and determine the necessary resources for conducting the PIA

Objective: To create a plan for the PIA and allocate human resources and budget for conducting the planned PIA.

Input: Terms of reference and scope for the PIA.

Expected output: Plan for the PIA to be conducted, business case and allocated resources.

Actions:

Select and plan the steps of the PIA and select the actions to be conducted, in terms of tasks and needed time and resources.

Estimate costs and level of efforts, check availability of team members and decide on the allocation of budget and resources.

Output of this process in terms of resources should be documented in the PIA report (see 7.3.3).

Implementation Guidance:

The plan should take into account the scope of the assessment being undertaken, allowing for iterations if necessary. This should include iterations of the PIA report. This is particularly useful when the assessment involves large-scale resources, but may not be necessary for smaller, less complex initiatives. The plan should also allow for situations where the initiative under assessment is discontinued.

The plan should spell out what is to be done to complete the PIA, who on the PIA team will do what, the PIA schedule and especially how the consultations, if any, will be carried out. It should specify why it is important to consult stakeholders in this specific instance, who will be consulted, and how they will be consulted (e.g. via public opinion survey, workshops, focus groups, public hearings, online experience, etc.).

Once the assessor has prepared the PIA plan, they should estimate the costs of undertaking the PIA and seek the budgetary and human resources necessary from the organization's senior management. The plan may require an increase in the nominal budget initially set by the senior management, or the person responsible for conducting a PIA may need to revise the PIA plan based on the budget available.

The organization should develop practical means to allocate appropriate resources for the PIA.

Consideration should be given to the following:

— people, skills, experience and competences;

— the time needed for any task;

— resources needed for each step of the PIA.

6.3.3 Describe what is being assessed

Objective: To describe the programme, process, or information system to be assessed.

Input: System requirement information, system design information, operational plans and procedures information, external and internal factors.

Expected output: Description of the business process and information system to be assessed.

Actions:

Create an appropriate description of the programme, process, or information system to be addressed.

Output of this process in terms of system requirements, design and operational plans and procedures should be documented in the PIA report (see 7.3.1).

Implementation Guidance:

By establishing the context, the organization defines the relevant internal and external parameters to be taken into account when managing privacy risk and setting the scope and privacy risk criteria for the remaining process.

The description of the programme, process or information system to be assessed should be organized under the three headings of 7.3.1.2 (System requirement information), 7.3.1.3 (System design information) and 7.3.1.4 (Operational plans and procedures information).

In order to gain a clear view of the scope under consideration, the assessor should seek answers to at least the following set of non-exhaustive questions:

— What are the PII that are processed?

— What is(are) the purpose(s) of the processing?

— What are the main benefits offered by the processing(s) of PII to the PII principals or to the society as a whole?

— Who are the PII recipients and how will they treat PII?

— What business process(es) is(are) executed by this(these) processing(s) of PII?

— Which PII principals are affected by this(these) processing(s) of PII?

— How will the privacy processes be implemented (notice, consent, opposition, access, correction, deletion, etc.)?

— How will PII principals be notified and their consent sought? Will the process be aligned with its context?

— What are the supporting assets (on which the PII rely) within the scope?

For each PII, the organization should identify the supporting assets (on which the PII rely) that will be used or that are being used. It should identify the location of those supporting assets. For example:

— user hardware and software (such as an organization-provided application on a user-provided smartphone);

— which kinds of hardware (computers, routers, electronic media, etc.);

— which kinds of software (operating systems, messaging systems, databases, business applications, etc.);

— what kinds of computer communications networks (cables, Wi-Fi, fibre optics, etc.);

— which kinds of supporting paper assets (printouts, photocopies, etc.);

— which paper transmission channels (mail, work-flow, etc.).

For the information system and supporting assets identified, the assessor should consult the commonly used operational plans and procedures with their underlying concepts. For example:

— how identity and user management is done;

— if operations are done on site or externally;

— the use of sub-contractors and their degree of access to locations and to PII;

— use of metadata, logging, backup and recovery;

— data retention, deletion and media disposal;

— system decommissioning.

The description can be used in at least three ways — it helps provide necessary contextual inputs to the assessor, the person who conducts the PIA, it can be included in the PIA report and it can be used as a briefing paper for consulting stakeholders. The description of the project should provide some contextual information (e.g. why the project is being undertaken, who comprises the target market, how the technology, service, system or other initiative described might impact privacy, what PII will be processed and what platforms will be used for processing PII). The project description should state who is responsible for the project. It should indicate important milestones and especially when decisions are to be made that could affect the project's design.

6.3.4 Stakeholder engagement

6.3.4.1 Identify stakeholders

Objective: To identify the individuals who may process PII or be impacted by the processing of their PII.

Input: Description of the business process and information system to be assessed, scope of the PIA.

Expected output: Identified privacy stakeholders.

Actions:

The organization should identify all the stakeholders (including PII principals) who might process PII or who might be impacted by the processing of their PII.

Output of this process in terms of a stakeholder list should be used in the PIA report (see 7.3.4).

Implementation Guidance:

Examples of stakeholders may include:

— employees, such as human resources, legal, information security, finance, business operational functions, communications and internal audit (especially in a regulated environment);

— PII principals;

— worker and consumer representatives;

— sub-contractors;

— business partners;

— application and database administrators;

— computer or network administrators;

— application operators;

— computer or network operators;

— maintenance people;

— people from other organizations who have appropriate concerns relevant to PIA.

In order to make the PIA process transparent and achieve goals of the PIA for addressing the privacy risks, the person responsible for conducting a PIA should identify in detail the internal or external stakeholders who may have an interest in or be affected by either the process subject to a PIA or in the protection of their PII under this process. Stakeholders could be all individuals or parties including end-users who might have or might obtain access to PII.

The person responsible for conducting a PIA should identify these different categories and then identify specific individuals from within each of the categories, preferably as representative as possible.

The scope and scale of the PII will be important in determining the appropriate stakeholders. Where a large government project is being undertaken, there may be many stakeholders. In this case, societal interest groups such as consumer representatives may need to be identified as well as stakeholders who process PII and who are PII principals. In contrast, smaller commercial processing operations may not need to identify such a wide stakeholder list.

6.3.4.2 Establish a consultation plan

Objective: To give structure to the consultation and communication with stakeholders.

Input: Identified privacy stakeholders, plan for the PIA to be conducted.

Expected output: Consultation and communication plan.

Actions:

The assessor should develop a plan to communicate and consult with both internal and external stakeholders at an early stage.

Output of this process in terms of the consultation and communication plan should be used in the PIA report (see 7.3.4).

Implementation Guidance:

This plan should address issues relating to the impact on the various privacy stakeholders, their consequences (if known), and the measures being taken to manage them. The plan should also include the scale and the schedule for the consultation.

The plan should cover two aspects:

— working with relevant stakeholders to identify and assess privacy risks;

— consulting with stakeholders over the draft PIA report to check if it adequately captures their concerns.

The range and number of stakeholders to be consulted should be a function of the privacy risks and the assumptions about the frequency and level of impact of those risks and the numbers of citizen-consumers who could be impacted.

For example, if the risks are likely to impact only the employees of a single organization, then the consultation could be limited to employees and/or their representatives. If, however, the risks are expected to impact everyone in the country, then the organization should consult widely with external stakeholders. If, at the outset, the organization thinks only a small number of stakeholders might be impacted, but subsequently comes to appreciate that the numbers of people impacted are likely to be much greater and the risks much greater, then the organization should revise its consultation plan accordingly and make efforts to involve a correspondingly larger number of relevant stakeholders.

6.3.4.3 Consult with stakeholders

Objective: To conduct consultations with stakeholders, where appropriate and feasible.

Input: Identified privacy stakeholders, communication plan.

Expected output: Stakeholder feedback.

Actions:

The organization should seek to understand the perspectives of other stakeholders.

Output of this process in terms of the stakeholder feedback should be used in the PIA report (see 7.3.4).

Implementation Guidance:

Feedback from stakeholders may identify issues that are perceptions of risk rather than actual risks. These should not be discarded but treated under wider stakeholder management issues to aid communications activity.

The potentially significant impact of a consultation with stakeholders for many separate but very similar projects may be minimized if consultation results may be re-used. Where many projects with similar privacy issues are expected, then re-use of applicable consultation results should inform the design of a consultation. Consultations should not be over-broad but good judgement may permit such re-use. Consultation on an incremental basis for new issues in newer projects may also help to avoid undue impacts.

Stakeholder alignments can be conducted per market sector based on the sector-specific guideline. Organizations serving the same market sectors may use sector-specific guidelines as a baseline for the assessment and treatment of privacy and security risks. Such guidelines should adhere to the principles of this document, and specify risks and controls based on the common business processes and services of the particular market sector.

For SMEs, the involvement of stakeholders may be associated with disproportionate time and expense. For them, the concept of sector-specific guidelines could improve the completeness and quality of the PIA when they can refer to available guidelines.

6.4 Perform the PIA

6.4.1 Identify information flows of PII

Objective: To identify information flows of PII under assessment.

Input: Description of the process and information system to be assessed.

Expected output: Summary of findings on the information flow of PII within the process.

Actions:

The person responsible for conducting a PIA should consult with others in the organization and perhaps external to the organization to describe the PII flows and specifically:

— how PII is collected and the related source;

— who is accountable and who is responsible within the organization for the PII processing;

— for what purpose PII is processed;

— how PII will be processed;

— PII retention and disposal policy;

— how PII will be managed and modified;

— how will PII processors and application developers protect PII;

— identify any PII transferred to jurisdictions where lower levels of PII protection apply;

— whether applicable, notify the relevant authorities of any new PII processing and seek the necessary approvals.

Output of this process in terms of the information flow of PII should be documented in the PIA report (see 7.3.1).

Implementation Guidance:

Use of PII (or transfer of PII) may include approved data sharing flows of PII to other parties. D.1 shows an example of how the information flow of PII can be visualized in a work flow diagram on PII processing.

As an input to the PIA, the organization should describe the information flow in as detailed a manner as possible to help identify potential privacy risks. The assessor should consider the impacts not only on information privacy, but also compliance with privacy related regulations, e.g. telecommunications acts. The whole PII life cycle should be considered.

This step could be taken immediately after 6.3.3 and concurrently with 6.3.4.

6.4.2 Analyse the implications of the use case

Objective: To identify potential user behaviour.

Input: The type of potential PII principals and use cases, especially their use of digital devices to identify privacy risks brought about.

Expected output: Summary of findings on the users' use cases within the business process.

Actions:

Identify and describe the privacy impacts in the PIA report. Reduce privacy risks through user behaviour guided by PIA summary information with respect to risks and user mitigation action.

Implementation Guidance:

Examples of potential user behaviour which may have unintended consequences are the following:

— inexpertly modifying operating system security settings on processing devices;

— inclination to lose mobile devices and smart cards;

— inclination to mis-operate devices or misunderstand devices and application settings in a manner that can increase privacy risks;

— susceptibility to illicit activity in the market place that utilizes features of the technology to trick users/consumers into loss of privacy/security. Examples are e-mails embedding malware or trick links in e-mails to spoof websites to elicit key personal details or security information, fake optical codes added to physical advertising routing consumer's smartphone optical code recognition apps to false websites.

Any BYOD use cases should distinguish between corporate use and use in private life.

6.4.3 Determine the relevant privacy safeguarding requirements

NOTE Privacy safeguarding requirements are described in ISO/IEC 29100:2011, 4.5.

Objective: To determine the relevant privacy safeguarding requirements for the purpose of the programme, information system or process under assessment.

Input: Description of the business process and information system to be assessed, summary of findings on the information flow of PII and on the implications of the use case within the business process.

Expected output: List of privacy safeguarding requirements (see 7.4).

Actions:

The person responsible for conducting a PIA or their legal experts should ensure the business process under scope complies with any legislative, regulatory, business factors and contractual requirements regarding privacy and/or data protection.

Output of this process in terms of the list of compliance requirements should be used in the PIA report (see 7.4).

Implementation Guidance:

When implementing the organization's framework for managing privacy risk, the organization should:

— identify relevant legislation, regulations and contracts applicable to the PIA process;

— identify relevant information security control sets (e.g. information security standards);

— identify the associated privacy requirements;

— describe the already planned or existing controls that are expected to fulfil the privacy requirements;

— use relevant information available from earlier projects.

The ISO/IEC 29100 principles can be divided into more detailed requirements and other requirements can be added.

Compliance requirements may include:

— ensure the PII principals are correctly notified concerning the purpose for processing the PII in accordance with the principle of consent and choice;

— ensure the PII principals have the ability to access and review their PII in accordance with the principle of individual participation and access.

6.4.4 Assess privacy risk

6.4.4.1 Privacy risk identification

Objective: To identify risks to relevant stakeholders arising from the programme, information system or process under assessment.

Input: Description of the programme, information system or process to be assessed.

Expected output: Identified privacy risks.

Actions:

Organizations should identify risks to be assessed.

Output of identified risks should be documented in the PIA report (see 7.5.1).

Implementation Guidance:

The organization should apply privacy risk identification tools and techniques which are suited to its objectives and capabilities, and to the risks faced. The respective legal privacy principles of the country in which the solution will be deployed should be used to support the identification of risks for privacy breach.

Privacy risks include, but are not limited to:

— unauthorized access to PII (loss of confidentiality);

— unauthorized modification of the PII (loss of integrity);

— loss, theft or unauthorized removal of the PII (loss of availability).

It is possible to consider other aspects like the following:

— excessive collection of PII (loss of operational control);

— unauthorized or inappropriate linking of PII;

— insufficient information concerning the purpose for processing the PII (lack of transparency);

— failure to consider the rights of the PII principal (e.g. loss of the right of access);

— processing of PII without the knowledge or consent of the PII principal (unless such processing is provided for in the relevant legislation or regulation);

— sharing or re-purposing PII with third parties without the consent of the PII principal;

— unnecessarily prolonged retention of PII.

NOTE Those possibilities of non-implementation or bad implementation of fundamental rights could only be checked and improved. Indeed, not implementing those fundamental rights is not an option.

Relevant and up-to-date information is important in identifying privacy risks. The assessor should involve people with appropriate knowledge in identifying privacy risks. After identifying what might happen, it is necessary to consider possible scenarios that show what consequences can occur. All scenarios should be considered.

Scenarios involving misuse and/or abuse, as well as technical or environmental disturbances, should also be considered as potential threats.

Wherever justifiable, the person responsible for conducting a PIA should make an effort to obtain stakeholder support when identifying the privacy risks.

6.4.4.2 Privacy risk analysis

Objective: To analyse the potential consequences and threats of the privacy risks identified, and to estimate their respective levels of impact and likelihood.

Input: Identified privacy risks.

Expected output: Analysed privacy risks (i.e. their description and estimation of the level of impact and likelihood).

Actions:

Organizations should determine the impact of a privacy risk.

Output of privacy risk analysis should be documented in the PIA report (see 7.5.2 and 7.5.3).

Implementation Guidance:

Risk analysis is based on a detailed analysis of a programme, information system or process, or changes thereto. Risk analysis includes identifying the PII and supporting assets that may be at risk, the vulnerabilities associated with those assets, the threats that might exploit those vulnerabilities, the likelihood and impact of that happening, as well as any existing controls that might influence the risk. All assumptions made during the risk analysis should be properly documented. Sources, both within and outside of the control of the organization, should be included if they have an impact on the PII principal. The organization should generate as comprehensive a list of privacy risks as it can.

Privacy risk analysis involves consideration of the causes and sources of privacy risk, their positive and negative consequences, and the likelihood those consequences can occur. The assessor should identify factors that affect consequences and likelihood. An event can have multiple consequences and can affect multiple objectives. The assessor should take into account existing controls and their effectiveness.

If a privacy risk is assessed as having a high or very high impact and/or is likely or very likely to occur, the organization should consider decomposing that risk into its sub-elements. This decomposition will allow the organization to identify which sub-element is contributing to the high impact or likelihood and analyse it separately. This should help identify more appropriate controls.

To estimate the likelihood of the threats (see ISO/IEC 27000:2016, 2.83), the organization should consider the risk sources capacities, the vulnerabilities of the supporting assets and the existing or planned controls. Annex A may be used.

For each of those risks (see 6.4.4.1), identify

— the most likely risk sources (see ISO Guide 73:2009, 3.5.1.2);

— the most likely threats;

— the most severe impacts on PII principals' privacy;

— a risk owner (see ISO Guide 73:2009, 3.5.1.5);

— the existing controls and the risk(s) they help to treat.

Then the level of impact should be estimated based on those potential consequences and the scale(s) determined in the risk criteria.

Annex B provides a list of generic threats that may assist in order not to overlook threats that are relevant.

The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk will vary according to the type of privacy risk, the level of exposure of the PII principals involved as well as the organization. In the case of a breach of privacy, the organization should use the information available and the output of the privacy risk analysis. These should all be consistent with the risk criteria.

The assessor should consider the level of confidence in the determination of privacy risks and their sensitivity to preconditions in the analysis, and communicate that to decision makers and other stakeholders if required. The assessor should state and may highlight factors such as any divergence of opinion among experts or limitations on modelling. The assessor should consult the relevant stakeholders identified at 6.3.4.1 by interview or include them in workshops as part of assessing privacy risk.

NOTE The level of confidence is defined as the percentage of instances that a set of similarly constructed tests will capture the true mean by ISO 772.

Privacy risk analysis can be undertaken with varying degrees of details depending on the privacy risk, the purpose of the analysis, and the information, data and resources available to support the analysis. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

In practice, qualitative analysis is often used first to obtain a general indication of the level of risk and to reveal the major risks. When possible and appropriate, one should also undertake more specific and quantitative analysis of the risks.

Risk estimation consists in assigning values to the potential consequences (level of impact) and the threats (likelihood) of a risk.

The organization should use privacy risk estimation tools and techniques which are suited to its objectives and capabilities, and to the risks faced.

The assessor should involve people with appropriate knowledge when estimating privacy risks.

If multiple PIAs are being conducted involving common programme, information system or process elements, coordination among the PIA teams is required to ensure risks are identified and assessed in a consistent manner, and subsequent action plans are also consistent.

6.4.4.3 Privacy risk evaluation

Objective: To prioritize the identified privacy risks.

Input: Identified privacy risks, privacy risk analysis.

Expected output: Privacy risk map.

Actions:

A privacy risk evaluation should be produced.

Output in terms of the privacy risk map should be documented in the PIA report (see 7.5.4).

Implementation Guidance:

Producing a privacy risk evaluation should involve the relative prioritization of privacy risk, based on the severity of privacy impact on PII principals as well as the overall impact to the organization.

The treatment of identified privacy risks may require more resources than are available to the organization. Prioritizing the identified risks will help the organization prioritize the allocation of resources for their treatment.

Risk decisions should take into account all relevant factors, including the risk tolerance of stakeholders, including, but not limited to, the PII principal, where feasible and appropriate. Decisions should be made in accordance with legal, regulatory and other requirements.

In some circumstances, the privacy risk evaluation can lead to a decision to undertake further analysis.

A privacy risk map should result from an assessment of the level of impact and the likelihood of the assessed risks.

Priorities should be set, based on where risks are located on the map (in order of priority) and on the risk criteria.

D.2 provides an illustrated example of a privacy risk map.

6.4.5 Prepare for treating privacy risks

6.4.5.1 Choose the privacy risk treatment options

Objective: To decide on the treatment option for any privacy risk assessed.

Input: Privacy risk map.

Expected output: List of the most appropriate treatment options for any privacy risk assessed.

Actions:

The privacy risk treatment options should be identified and the most appropriate options selected.

Output in terms of the list of treatment options for any privacy risk assessed should be reused in 6.4.5.2.

Implementation Guidance:

Risk treatment may include, but is not limited to, conducting application or process redesign, depending on the scope of the assessment, context of risk management or industry sector.

Selecting the most appropriate privacy risk treatment option involves balancing the costs and efforts of implementation against the organization's obligation for protecting the privacy of any stakeholder whose privacy might be impacted by the organization (e.g. their PII is controlled or processed by the organization).

An organization's decisions should also take into account risks that can warrant risk treatment actions that are not justifiable on economic grounds, e.g. severe (high negative impact) but rare (low likelihood) risks.

The privacy risk evaluation can also lead to a decision not to treat the privacy risk in any way other than maintaining existing privacy controls. This decision will be influenced by the organization's risk appetite or risk attitude and the privacy risk criteria that have been established.

Wherever appropriate, an organization and/or the assessor should seek stakeholders support in the selection of privacy risk treatment options.

A number of treatment options can be considered and applied either individually or in combination. The organization can benefit from the adoption of a combination of treatment options.

When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where privacy risk treatment options can impact on risk elsewhere in the organization, these areas should be involved in the decision. Though equally effective, some risk treatments may be more acceptable to stakeholders than others.

Since the resources for privacy risk treatment may be limited, the privacy risk treatment plan should clearly identify the priority order in which individual privacy risk treatments should be implemented.

Privacy risk treatment itself can introduce privacy risks that need to be assessed, treated, monitored and reviewed. A significant privacy risk can be the failure or ineffectiveness of the risk treatment measures. These secondary privacy risks should be incorporated into the same privacy risk treatment plan as the original privacy risk and not treated as a new privacy risk, and the link between the two privacy risks should be identified.

Decision makers and other appropriate stakeholders should be aware of the nature and extent of the residual privacy risk after privacy risk treatment. The residual privacy risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

Monitoring needs to be an integral part of the privacy risk management plan to give assurance to internal stakeholders that the measures remain effective.

There are four options available for privacy risk treatment: risk reduction, risk retention, risk avoidance and risk transfer.

a) Risk reduction

Risk reduction can be achieved through the selection of appropriate controls. If after control selection there is still some residual risk, the organization should determine whether the residual risk is unacceptable and should be further addressed through the selection of additional controls, or determined to be acceptable to the organization and to the stakeholders.

There may be occasions where risk reduction measures impact the benefits that stakeholders may derive from the processing of the information in question. In such situations, the assessor should conduct a risk/benefit analysis to determine if the risks outweigh the benefits or vice versa. If the former, the organization should adopt the risk reduction measures. If the latter, the organization should decide to accept the risks within compliance requirements.

Risk reduction controls will be varied in nature. They may involve:

— changes to the kind of PII being processed;

— changes to organizational structure, policies and/or procedures;

— changes to personnel qualifications (e.g. clearances, training, certification and so on).

Modifications to the supporting assets or to applications may be of three kinds: preventive measures, detection measures or correction measures.

b) Risk retention

If the level of risk meets the risk criteria, there is no need for implementing additional controls and the risk can be retained.

c) Risk avoidance

When the identified risks are considered too high, the organization should decide to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated.

d) Risk transfer

Risk transfer involves a decision to share certain risks with external parties. Transfer can be done by insurance that will support the consequences, or by sub-contracting a partner whose role will be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.

Risk transfer of significant or maximum risks to PII principals, such as fraud, arising from loss of PII is not good practice. Risk sharing should be between businesses and other organizations and significant risk should not be passed on to the PII principal.

Risk transfer can create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary.

It may be possible to transfer the responsibility to manage risk but it is not normally possible to transfer the liability of an impact. Stakeholders will usually attribute an adverse impact as being the fault of the organization.

If an organization has defined a special privacy rule in its privacy policy and has defined the acceptance statement, the organization should consider that only avoidance would be an acceptable option to treat the risk leading to the highest impact scale in this criteria.

NOTE The privacy policy is generally known as a set of rules that advertises which specific personal data may be collected by an organization, how it will be used and whether it will be kept inside that organization or shared with or sold to other organizations.

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

6.4.5.2 Determine controls

Objective: To identify appropriate controls to the treatment options chosen.

Input: List of the most appropriate treatment options for any privacy risk assessed.

Expected output: List of chosen controls, Statement of Applicability (in the ISMS framework).

Actions:

The appropriate controls for the selected risk treatment options as well as the legally required controls should be identified.

Output in terms of the list of privacy risks for treatment, combined with the list of chosen controls, should be re-used in 6.4.5.3 and documented in the PIA report (see 7.5.5 and 7.6).

Implementation Guidance:

Controls that are already existing or planned that met the requirement of the ISO/IEC 29100 principles should be described and evaluated.

NOTE 1 The privacy principles of ISO/IEC 29100 are consent and choice, purpose, legitimacy and specification, collection limitation, data minimization, use, retention and disclosure limitation, accuracy and quality, openness, transparency and notice, individual participation and access, accountability, information security and privacy compliance.

A good way to perform this analysis consists in using a commonly used set of controls[1)] that could be used in order to verify that no necessary controls have been omitted.

Additional controls (to the existing ones) should be added until the risk level is finally considered acceptable.

Additional controls may be selected from existing control sets defined in recognized international standards or issued by recognized institutions. They may also be developed by the organization independently of any existing control sets. If necessary, controls should be adapted to the specific context of the programme, information system or process under consideration.

This identification should consist of defining controls in the following categories:

— the PII: controls designed to prevent data breaches, to detect such breaches or to restore their security (informing PII principals, keeping personal data to a minimum, anonymization of personal data, etc.);

— if the above is insufficient, the potential impacts: controls designed to prevent the consequences of risks from occurring, to identify and limit their effects or to curb them (making of backups, integrity checks, management of personal data breaches, etc.);

— if the above is insufficient, the risk sources: controls designed to prevent risk sources from acting or making a risk real, to identify and limit their impact or to cause them to become ineffective

1) ISO/IEC 29151 or comparable national standards should be used as a reference.

(physical and logical access control, activity tracking, management of third parties, protection against malware, etc.);

— if the above is insufficient, the supporting assets: controls designed to prevent the exploitation of vulnerabilities, to detect and limit threats that do occur or to restore the normal operating condition (reducing the vulnerabilities of software, hardware, individuals, paper documents, etc.).

NOTE 2 It is worth supplementing the system with cross-organizational controls (organization, policy, monitoring, etc.) in order to improve the maturity of PII protection.

NOTE 3 The higher the capabilities of the risk sources, the more robust the controls will be in order to withstand them.

If this analysis provides sufficient information to determine actions that may be performed to modify the risk to an acceptable level, then the processing is complete for that risk.

If the information is insufficient, the assessor should conduct another iteration of the risk assessment with a revised context (e.g. risk criteria, risk acceptance criteria or impact criteria), possibly on limited parts of the total scope.

The assessor should re-estimate the level of impact and likelihood of the residual risks (i.e. risks that remain after the selected controls are implemented) by factoring in these additional controls. Then, they can be repositioned on the privacy risk map.

The assessor should explain why residual risks may be accepted. These explanations may be based on the new level of impact and likelihood levels and on the benefits offered by the processing of PII (risk-benefit analysis).

The assessor should compare the existing and determined controls to reference lists of controls and verify that no necessary controls have been omitted:

— controls in ISO/IEC 27001:2013, Annex A;

— controls in ISO/IEC 29151;

— controls in any relevant privacy sets of controls, including national standards;

— controls from external factors;

— controls from internal factors.

If a control (or controls) is not selected to meet a compliance requirement from 6.4.3, the organization should document its rationale for not selecting a control (or controls). Reasons for not selecting a control could include the lack of a suitable control, or the controls that are available are prohibitively expensive in relation to the value of the asset to be protected.

In case the PIA is conducted in support of an ISMS, a Statement of Applicability should be produced in order to explain whether the controls from the reference lists as well as the legally required controls are implemented or not, and the justification for exclusions of controls from the reference lists.

NOTE 4 A PIA does not necessarily require an ISMS.

6.4.5.3 Create privacy risk treatment plans

Objective: To plan and to implement the risk treatment actions.

Input: List of chosen controls.

Expected output: Privacy risk treatment plan, control plan, risk owner approvals, acceptance statement.

Actions:

One or more privacy risk treatment plan(s) should be formulated.

Output in terms of the privacy risk treatment plan, control plan, risk owner approvals and an acceptance statement should be documented in the PIA report (see 7.6 and 7.7).

Implementation Guidance:

The risk treatment plan should estimate the cost of implementing each control.

A control plan should also be derived out of the risk treatment plan that should identify the factors or variables (e.g. re-assessing the new risks sources arising due to change in processing, repurposing, transfer, etc.) that need to be kept under consideration. This would help maintain the steady state of the PII processing environment (i.e. all privacy preserving controls do not wear out with time).

When planning how to facilitate the privacy risk treatment plan, the organization should determine:

— what will be done;

— what resources will be required;

— who will be responsible;

— when it will be completed;

— how the results will be evaluated.

NOTE In order to check the reliability of these controls, it may be worthwhile determining the actions taken in case these actions are ineffective (if they no longer work).

The information provided in treatment plans should include:

— what privacy safeguarding requirements protect against which risks, supported by details from threat modelling and control design activities;

— a list of PII including nature and ownership of the PII to be protected;

— performance measures and constraints;

— persons who are accountable for approving/rejecting the plan and those responsible for implementing the plan;

— proposed actions;

— reporting and monitoring requirements;

— the human resources that are necessary to implement, manage and maintain the project need to be identified;

— other resource requirements;

— timing and scheduling.

Privacy risk treatment plans should be integrated with the management processes of the organization and discussed with appropriate stakeholders.

The risk owner should approve the privacy risk treatment plan and accept the residual privacy risks. Management responsibility should also be obtained by signing the acceptance statement.

6.5 Follow up the PIA

6.5.1 Prepare the report

Objective: To configure the PIA report and sign off.

Input: Outputs from previous steps.

Expected output: Decision on the elements to be published, PIA report for publication.

Actions:

As the penultimate step of each PIA, the results of each of the previous steps should be recorded into a comprehensive report (see Clause 7). In this step, it should be decided which elements of the comprehensive report should be published and which elements should be provided to the appropriate interested parties.

The assessor should use the output in terms of the PIA report and sign off in the next step and should reflect the decision in the PIA report (see 7.7).

Implementation Guidance:

The assessor should collect the output from the previous steps in a report prepared along the structures lined out in Clause 7.

This report should be filed by the person responsible for conducting a PIA and should formally be signed off by the organization's management responsible for the programme that is controlling the processing of PII.

The report should be sent to the member of the organization who commissioned the PIA for their review and consideration. Appropriate further distribution, for example to the Board, if appropriate, or other members of the organization's management should be arranged.

The agreed elements of the PIA report should be made available to interested parties. If necessary, sensitive information should be redacted or put in a confidential annex, or the PIA report could be summarized.

6.5.2 Publication

Objective: To inform on the outcome of the PIA to the stakeholders.

Input: PIA report.

Expected output: PIA public summary and the PIA report for publication.

Actions:

In the last step, a public summary should be added and the PIA report should be published.

Output of this process should be a PIA public summary and should be used in the PIA report (see 7.8).

Implementation Guidance:

The organization should maintain a registry of PIA reports. The registry could be a simple listing of the PIAs, their titles and the dates the PIA reports were published. The registry of published PIA material should be easy to find by visitors, especially PII principals to its website, and they should be able to download a copy of any published PIA material of interest.

The registry serves several purposes. It provides organizational memory (i.e. a reference document for those in the organization who were not involved in the PIA to understand what happened and what the recommendations were). The registry provides a way of learning from others and ultimately a source of good practices. Those undertaking new PIAs can refer to any PIA antecedents conducted by the organization to see what to emulate and what to avoid. The registry also sends a message to internal and external stakeholders that the organization treats privacy seriously.

6.5.3 Implement privacy risk treatment plans

Objective: To implement the privacy risk treatment plans.

Input: Privacy risk treatment plan, risk owner approvals.

Expected output: Implementation sign-off.

Actions:

Implementing the privacy risk treatment plans should be subject to the management system planned or in place.

Implementation Guidance:

Once the PIA report has been approved by the person responsible for conducting a PIA and the management of the organization, several actions need to be performed.

Before implementing the processing of the PII (where possible),

— the organization should provide appropriate training for the people involved in the project to make sure they are sensitive to the privacy implications, the possible impacts on privacy, of what they or their colleagues do. Where necessary, record training and record any acceptable use agreements;

— the organization should provide the budget for implementing the identified controls;

— as soon as the service that is the object of the project is made available to the end-users, both the privacy policy and the privacy practice statement should also be made available to these end-users;

— the organization should implement the treatment plan.

The risk owner and/or the organization may not accept all of the PIA recommendations, but they should say and inform the organization's data protection officer and senior management which recommendations they are implementing, why they may not implement others and what are the plans for implementing the recommendations.

The organization should have a mechanism for monitoring the implementation of the recommendations.

6.5.4 Review and/or audit of the PIA

Objective: To obtain an appropriate review of the PIA conducted.

Input: PIA report.

Expected output: Review report.

Actions:

Arrange for appropriate review of the PIA report.

Implementation Guidance:

An organization may wish to establish a policy for reviews and/or audits setting out types, schedules and significance thresholds that trigger them.

Where required by privacy legislation, review and/or audit should include liaison with any relevant organization charged with the administration of the privacy legislation, such as data protection authorities or privacy commissioners.

Independent review or audit of the PIA is a way of ensuring the PIA has been conducted appropriately and the organization has implemented the risk treatment plan or, if it has not implemented some recommendations, then it can say why it has not done so (e.g. the residual risk may be deemed to be of lesser consequence than the perceived benefits).

Third-party review or audit, where possible, is a way of giving credibility to the PIA report, of improving transparency, of learning from experience and raising the quality of PIA practices. If the PIA is conducted by a third party, then the review and/or audit of the PIA should not be carried out by the same third party.

6.5.5 Reflect changes to the process

Objective: To deal with changes in a process formerly assessed.

Input: Significant change within the process or information system.

Expected output: Decision on another iteration of the PIA.

Actions:

The organization should have a mechanism for updating in the PIA report, as necessary, notably if there are significant changes in the business process affecting the processing of PII or the way in which the business process was previously presented to stakeholders.

Output of this process should be used in the PIA report (see 7.2).

Implementation Guidance:

The organization should explain why changes are being made in the business process and how these changes might affect the processing and/or disposition of PII.

The organization should verify that the processing of PII meets privacy safeguarding requirements by periodically conducting an internal audit or a trusted third-party audit.

A renewed PIA should be conducted, not only if the business process changes, but also after some previously defined time (in a certain interval).

An organization should decide if it is preferable to update the PIA (e.g. a simple audit can be carried out, which only checks whether basic conditions have changed).

7 PIA report

7.1 General

Clause 7 gives guidance on the content of the PIA report.

The PIA report's contents will depend strongly on the type and sensitivity of PII being processed, its nature and the scope and objectives of the PIA being conducted. Thus, this guidance should be interpreted within the context of the specific project.

Some of the PIA report's details may be confidential. They may address business issues that should not be made public. They may address treatment options that may reveal sufficient details about residual risks to increase the risk of system compromise.

The organization should determine the appropriate audience for and contents of the PIA report and its degree of confidentiality. A report provided in confidence to an independent auditor or to a data protection authority may contain more details than one provided to stakeholders or to the public.

The organization should consider addressing the following issues and consider the guidance provided for each:

— the report structure (7.2);

— the scope of the assessment (7.3);

— the privacy requirements (7.4);

— the risk assessment (7.5);

— the risk treatment plan (7.6);

— the conclusion and decisions taken on the basis of the outcome of the PIA (7.7);

— a PIA public summary to inform PII principals about the level of risk associated with the programme, information system, and the process implemented in which their PII will be involved (7.8).

7.2 Report structure

The PIA report should be adapted to specific circumstances. Those circumstances should be as determined through consideration of the guidance in Clause 6. It should normally state on its cover page at least the name of the process, information system or programme, name and address of the PII controller and of the organization which conducts the PIA, contact person along with contact details, its version number for document control, the date of the PIA report, and it should also name those to whom one can address any queries if different from the person who conducted the PIA.

The Introduction should indicate why a PIA has been conducted, when it was conducted, who was involved in the conduct of the PIA and the terms of reference of the PIA. It should provide some information about the process, information system or programme assessed. It should introduce the guidelines employed in the PIA (e.g. the decision whether to engage stakeholders). The Introduction should provide any contextual information about the organization and its environment that might be necessary in order to understand the rationale for the PIA. The Introduction could also refer to the organization's privacy policy and/or code of conduct as well as the organization's obligations to its stakeholders (and shareholders, if relevant) as well as its compliance with relevant legislation.

If the PIA report is long, it should include an executive summary stating the main findings and recommendations of the PIA and which stakeholders were consulted. The executive summary should state why the PIA was undertaken, who initiated the PIA, and who conducted it. The executive summary should provide a brief description of the programme, information system, process or other initiative, which was the subject of the PIA. It should identify the principle privacy impacts and the alternatives for minimizing or avoiding negative impacts.

Input comes from 6.2, 6.3.1 and 6.5.5.

7.3 Scope of PIA

7.3.1 Process under evaluation

7.3.1.1 General

The PIA report should clearly define the scope for the PIA conducted.

The management should make some statement regarding the boundaries of assessment and what was considered to be out of the scope.

Any assessment can only be as good as the description of the scope allows. Therefore, the organization should provide the most complete description possible of the process, programme, information system or other initiative that will be the subject of the PIA.

The PIA report should state how individuals are notified that the organization is collecting information about them, and what role individual consent plays in the process, information system or programme. It should also state whether the information collected is combined or "matched" with information from other sources and, if so, under what legal authority.

The organization should say how it intends to delete the PII once it is no longer needed. It should say what procedures it will put in place to allow individuals to see their PII and to rectify it if necessary or to request its deletion. It should state what appeal procedures exist if the organization refuses to delete the information or allow access to it. The organization should also specify the costs, if any, of allowing individual access to their PII and how much time it takes the organization to respond to requests.

The PIA report should describe at least system requirements, the system design and the operational plans and procedures as described in 7.3.1.2, 7.3.1.3 and 7.3.1.4.

Input comes from 6.3.3 and 6.4.1.

7.3.1.2 System requirement information

The system requirement information should contain:

— the purpose of processing;

— a description of the business process that is, or will be, supported by the information system;

— the list of functional requirements defined for the information system and their level of obligation or implementation;

— the information security objectives;

— a description of how data will be gathered and from whom and why. The description should state who will have access to the PII, including the parameters regarding PII principal access;

— if the information system or its PII is intended to be shared with third parties, details or advice about with whom the information system or PII will be shared and for which purpose(s);

— a statement on the justification for processing the PII involved in this information system.

7.3.1.3 System design information

The system design information should contain:

— an overview of the functional (or logical) architecture;

— an overview of the physical architecture;

— the structure and list of information system databases, tables and fields that could contain PII;

— the data flow diagram by entities as well as by interfaces;

— a data flow diagram through the life cycle of PII, e.g. generation, use, transfer, and disposal of PII;

— a work flow diagram that describes when to notify and get consent from PII principals;

— a list of interfaces, defining the parties connected and the data fields transferred;

— details of ports, protocols, APIs, and encryption details.

7.3.1.4 Operational plans and procedures information

The operational plans and procedures information should contain:

— the identity and user management concept for the information system;

— the operational concept, including if the information system or parts of it are operated on site or externally hosted, or cloud sourced and where;

— the support concept, especially listing third parties by name who are involved in supporting the information system, the degree to which they will have access to PII and locations from where the PII can be accessed;

— the logging concept and the respective retention plans for the logged information;

— the backup and recovery plans;

— the protection and management of metadata;

— the data retention and deletion plans and media disposal;

— the decommissioning concept.

7.3.2 Risk criteria

This part should describe the chosen risk criteria. It should at least contain:

— the criteria to estimate level of impact;

— the criteria to estimate likelihood;

— the scales for both;

— the criteria for risk acceptance.

Input comes from 6.3.1.

7.3.3 Resources and people involved

The organization's management should provide a statement on the composition of the PIA team, the major milestones of the PIA plan and the budget and resources spent on the PIA.

Input comes from 6.3.1 and 6.3.2.

7.3.4 Stakeholder consultation

In the PIA process, the organization is expected to have identified the types of stakeholders to be consulted (see 6.3.4.3). The PIA report should specify which stakeholder groups were consulted and how they were consulted (e.g. via surveys, interviews, focus groups, workshops).

The PIA report should state the result of the stakeholder consultation. Did the consultation have any consequence for the design of the programme, process, information system or other initiative that has been the subject of the PIA?

Input comes from 6.3.4.1 to 6.3.4.3.

7.4 Privacy requirements

The PIA report should list the relevant sources for the requirements identified by the PIA team as needing to be met.

Input comes from 6.4.3.

7.5 Risk assessment

7.5.1 Risk sources

The PIA report should list the sources of privacy risk the organization has identified (see 6.4.4).

Input comes from 6.4.4.1.

7.5.2 Threats and their likelihood

For each processing of PII and each potential consequence on the PII principals' privacy, the PIA report should list the determined threats that may allow the identified risks to occur and their respective likelihood.

Input comes from 6.4.4.1 and 6.4.4.2.

7.5.3 Consequences and their level of impact

The PIA report should document the level of impacts for each risk identified.

Input comes from 6.4.4.2.

7.5.4 Risk evaluation

The PIA report should provide a privacy risks map, which shows the level of impact and the likelihood of the assessed risks.

Priorities should be set, based on where risks are located on the map (in order of priority) and on the risk criteria.

Input comes from 6.4.4.3.

7.5.5 Compliance analysis

With respect to the set of requirements given from 7.4, the PIA report should record item by item if the processing assessed is found compliant to the different aspects of the respective obligation, and if it is not found fully compliant, up to what degree.

7.6 Risk treatment plan

The PIA report should record the risk treatment plan and the stage of implementation for any of the controls contained.

Input comes from 6.4.5.3.

7.7 Conclusion and decisions

Decisions that are made during the PIA process on the acceptance of the residual privacy risks, on non-implementation of PIA recommendations with the treatment plan and on non-publishing elements of the PIA report should be recorded, together with the conclusions which have led to these decisions.

Input comes from 6.4.5.3 and 6.5.1.

7.8 PIA public summary

In order to provide privacy risk information to users, whether they are external PII principals or employees, to support consent, the assessor may need to prepare a public summary of the main PIA report.

If necessary, the summary should remove commercially sensitive information that might be present in the full PIA report and include only those key aspects relevant to PII principals.

The PIA public summary report should contain as below:

— the benefits of the programme, information system or process;

— the PII types to be processed and collected;

— legal jurisdictions under which PII processing will be undertaken;

— a summary of the compliance analysis;

— a summary of any measures to comply with the privacy requirements or to treat privacy risk that the organization intents to take or has taken;

— any measures that PII principals are recommended to take;

— the organization responsible for the PIA and programme, information system or process;

— the contact details for the PII controller responsible;

— details of any user privacy help line or support facilities put in place for the programme, information system or process.

When the PIA public summary addresses PII principals as members of the general public, they should represent all the above information and all additional information in a transparent, clear and comprehensible manner.

Input comes from 6.5.2.

Annex A
(informative)

Scale criteria on the level of impact and on the likelihood

A.1 General

Annex A contains example scales and criteria for estimating the impact and likelihood of a potential privacy breach as covered in 6.4.4.2 of this document. Annex A contains criteria any organization should consider when it is necessary to exchange information about risk with external stakeholders.

Estimations of impact and likelihood may be applied to both mitigated and unmitigated risks.

A.2 How to estimate the level of impact

The level of impact of the identified consequences should be estimated, taking into account those consequences and the planned or implemented controls. In other words, how much damage would be caused by all the potential impacts?

1) Negligible: PII principals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).

2) Limited: PII principals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).

3) Significant: PII principals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).

4) Maximum: PII principals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as unserviceable debt or inability to work, long-term psychological or physical ailments, death, etc.).

The value of the level that best matches the potential consequences identified is selected.

This level of impact can be then modified by including additional factors, e.g. directly identifying PII, significant risk sources, a large number of interconnections (especially with foreign sites) or recipients (which facilitates the correlation between originally separated personal data) might be considered as aggravating factors; conversely, poorly identifying PII, not dangerous risk sources, very few or no interconnections or recipients might lower the level of impact.

An example for the level of impact is given with Table A.1.

Table A.1 — Examples for the level of impact, based on the nature of the PII

Nature of the PII	Level of impact
PII that is **publicly** accessible (e.g. in telephone directories, address books or selection lists)	1
PII that **requires a legitimate interest** for access (e.g. restricted public files or the members of a distribution list)	2
PII whose unauthorized disclosure can **affect the reputation** of the PII principal (e.g. information about income, social welfare benefits, property tax or penalties)	3
PII whose unauthorized disclosure, modification, loss or destruction can **affect the existence** or the **health, freedom and life** of the PII principal (e.g. information about commitment to an institution, a sentence, personnel reviews, health data, unserviceable debts, or if the PII principal is at risk of becoming a victim in a criminal case)	4

A.3 How to estimate the likelihood

The likelihood of each threat being exploited should be estimated, taking into account the vulnerabilities of the supporting assets and the capabilities of risk sources to exploit them (skills, available time, financial resources, proximity to information system, motivation, feeling of impunity, etc.). In other words, to what degree can the properties of supporting assets be exploited in order to carry out a threat?

1) Negligible: Carrying out a threat by exploiting the properties of supporting assets does not appear possible for the selected risk sources (e.g. theft of paper documents stored in a room protected by a badge reader and access code).

2) Limited: Carrying out a threat by exploiting the properties of supporting assets appears to be difficult for the selected risk sources (e.g. theft of paper documents stored in a room protected by a badge reader).

3) Significant: Carrying out a threat by exploiting the properties of supporting assets appears to be possible for the selected risk sources (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at reception).

4) Maximum: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy for the selected risk sources (e.g. theft of paper documents stored in a lobby).

The value of the level that best matches the threats is selected.

This likelihood can be then modified by including additional factors, e.g. access to the Internet, exchanges of data with foreign sites, interconnections with other information systems and a high degree of system heterogeneity or variability may raise the likelihood; conversely, a homogeneous, stable system that has no interconnections and is closed off from the Internet may lower the likelihood.