



ISO/IEC JTC 1/SC 27 **N14164**

ISO/IEC JTC 1/SC 27/WG 5 **N514164**

REPLACES: N13391

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

**DOC TYPE:** working draft text

**TITLE:** Text for ISO/IEC 4th WD 29134 — Information technology — Security techniques — Privacy impact assessment — Methodology

**SOURCE:** Project editors

**DATE :** 2014-05-27

**PROJECT:** 1.27.104 (29134)

**STATUS:** In accordance with resolution 2 (see SC 27 N14199) of the 17th SC 27/WG 5 Plenary meeting held in Hong Kong (China) 7<sup>th</sup> – 11<sup>th</sup> May 2014 this document is being circulated for STUDY AND COMMENT.

Experts, liaison organizations and National Bodies are kindly requested to send their comments/contributions on the above-mentioned document by **2014-09-24**.

**PLEASE submit your comments / contributions on the hereby attached document via the SC 27 e-balloting/commenting website at:**  
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**PLEASE NOTE** For comments please use the SC 27 TEMPLATE separately attached to this document.

**ACTION:** COMM

**DUE DATE:** 2014-09-24

**DISTRIBUTION:** P-, O- and L-members  
W. Fumy, SC 27 Chairman  
M. De Soete, SC 27 Vice-Chair  
E.J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors  
M. Reinis, Heung Youl Youm, Project editor/co-editor

**MEDIUM:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**NO. OF PAGES:** 1 + 48

Reference number of working document: **ISO/IEC JTC 1/SC 27 N 14164**

Date: 2014-05-23

Reference number of document: **ISO/IEC 4<sup>th</sup> WD 29134**

Committee identification: **ISO/IEC JTC 1/SC 27/WG 5**

Secretariat: DIN

## **Information technology — Security techniques — Privacy impact assessment – Methodology** [change title to “Guidelines” is pending]

*Élément introductif — Élément principal — Partie n: Titre de la partie*

### **Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Note: According to the discussions happened in Seoul and Hong Kong sessions, there are requests to be raised in order to change the title and scope of the document. These have to be considered when request to go for CD. In the meantime, the document need to preserve the actual title and scope for formal reasons. NB/Liaisons are kindly requested to focus their comments on the new title and scope and to ignore the actual parts.

*[Editor's Note: Some kind of map (similar to Figure 1 in 29151) has been requested by NZ where a privacy risk assessment fits within the PIA or vis versa. NZ NB is requested to provide text.]*

Document type: **International standard**

Document subtype: **if applicable**

Document stage: **(20) Preparation**

Document language: **E**

C:\altes

NB\Documents\Project\_admin\29134\02\_04\_4thWD\_29134 \N14164\_ISO29134\_PIA\_4WD\_final\N14164\_ISO\_29134\_PIA\_4WD\_final\_20140527a.doc Basic template BASICEN3 2002-06-01

### Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

*Secretariat of ISO/IEC JTC 1/SC 27*

*DIN German Institute for Standardization*

*D-10772 Berlin*

*Tel. + 49 30 2601 2652*

*Fax + 49 30 2601 4 2562*

*E-mail [krystyna.passia@din.de](mailto:krystyna.passia@din.de)*

*Web <http://www.jtc1sc27.din.de/en> (public web site)*

*<http://isotc.iso.org/livelink/livelink/open/jtc1sc27> (SC 27 documents)*

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

# Contents

Page

Foreword .....	v
Introduction.....	vi
1 Scope .....	1
2 Normative references .....	2
3 Terms and definitions .....	2
4 Symbols (and abbreviated terms).....	3
5 Preparing the grounds for PIA Analysis .....	4
5.1 Why carry out a PIA? What are the benefits? .....	4
5.2 Expectations from PIA and on PIA reporting .....	5
5.3 Who should conduct a PIA? .....	5
5.4 Scale and scope of a PIA .....	6
6 Process for conducting a PIA .....	7
6.1 Preparation of the PIA.....	7
6.1.1 Determine whether a PIA is necessary (threshold analysis) .....	7
6.1.2 Identify the PIA team, define risk criteria and set the team's terms of reference .....	7
6.1.4 Determine the resources for conducting the PIA .....	9
6.1.5 Describe the proposed business process to be assessed .....	9
6.1.6 Identify stakeholders.....	10
6.1.7 Communication plan .....	10
6.1.8 Consult with stakeholders.....	11
6.2 Iterative phases .....	12
6.2.1 Analyze the information flows .....	12
6.2.2 Check the business process under scope meets the privacy safeguarding requirements .....	13
6.2.3 Assess privacy risk .....	15
6.2.3.1 Privacy risk identification .....	15
6.2.3.2 Privacy impact analysis .....	16
6.2.3.3 Privacy impact evaluation .....	17
6.2.4 Treat privacy risks .....	18
6.2.4.1 Choose the privacy risk treatment options .....	18
6.2.4.2 Determine controls.....	19
6.2.4.3 Create privacy risk treatment plans .....	20
6.3 Follow up of the PIA .....	22
6.3.1 Prepare and publish the report.....	22
6.3.2 Implement privacy risk treatment plans.....	23
6.3.3 Independent review and/or audit of the PIA .....	24
6.3.4 Re-Initiate PIA .....	24
7 Structure of PIA report.....	25
7.1 Introduction.....	25
7.2 Scope of PIA .....	25
7.2.1 Business process under evaluation.....	25
7.2.1.1 System requirement information .....	26
7.2.1.2 System design information.....	27
7.2.1.3 Operational plans and procedures information .....	27
7.2.2 Risk criteria .....	27
7.2.3 Resources - stakeholders, people involved .....	28
7.3 Privacy Requirements.....	28
7.3.1 Context, Stakes, Goals.....	29
7.3.2 Requirements to comply with .....	29
7.3.3 Compliance Analysis .....	29
7.4 Risk assessment .....	29

7.4.1	Risk Sources .....	29
7.4.2	Consequences and their level of Impact .....	29
7.4.3	Threats and their likelihood .....	30
7.4.4	Risk evaluation.....	30
7.5	Risk treatment.....	30
7.6	Conclusion and Decisions.....	30
Annex A	(informative) Scale criteria on the level of impact and on the likelihood .....	31
A.1	How to estimate the level of impact.....	31
A.2	How to estimate the likelihood .....	31
A.3	How to set objectives .....	32
A.4	Factors to be taken into account at specific sectors .....	32
Annex B	(informative) Generic threats.....	34
Annex C	(informative) Example of an Inventory tool supporting PIA.....	39
C.1	Inventory tool .....	39
Annex D	(informative) Text that needs reordering.....	41
Bibliography	.....	42

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29134 was prepared by Technical Committee ISO/TC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

## Introduction

A privacy impact assessment (PIA) is a tool for assessing the impacts on privacy of a project, technology, service or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts. A PIA is more than a tool: it is a *process* which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed.

A PIA is to be conducted to ensure that the privacy implications of the processing of PII will be appropriately identified, assessed and resolved according to legal and regulatory requirements.

This International Standard provides guidelines for the conduct of PIAs by organizations that are establishing or operating programmes, systems or processes that involve the processing of personally identifiable information (PII), or that are making significant changes to existing programmes, systems or processes that involve the processing of PII.

This International Standard provides a framework for conducting PIAs. It explains how to manage the privacy risks that are generated by the processing of PII.

This International Standard is relevant to managers and staffs responsible for or concerned with the life cycle of programmes, systems or processes that involve the processing of PII and, where appropriate, external parties supporting such activities.

This International Standard should be used when the impact to a PII principal needs consideration for processes, systems or programmes, where:

- The responsibility for the implementation and/or delivery of the process, system or programme is shared with other organizations and there is a need to ensure that each organization properly addresses the identified risks;
- a single organization is performing privacy risk management as part of its overall risk management effort in preparation for implementation or improvement of its ISMS (established in accordance with ISO 27001) or equivalent system; or a single organization is performing privacy risk management as a dedicated task for privacy impact only; or
- a legislator runs another programme, in which the final PII controller organization is not known yet, with the result that the treatment plan will be without an obligation yet and the controls proposed should become subject to a resulting legislative or other regulatory framework instead.

Controls determined to fulfill the ISO/IEC 29100 principles or those determined to treat the privacy risks can be derived from different sets of controls, such as ISO/IEC 27002 for information security and ISO/IEC 29151 for privacy, or being defined from nothing by the PII controller.

Whether an ISMS according to ISO/IEC 27001 is used or not, the controls used for comparison should be privacy focused. ISO/IEC 29151 should be used to that extent.

Once it has been determined that a PIA is required, perhaps through a threshold analysis or as a result of a legal requirement, it is recommended that the PIA be conducted in accordance with this standard. It is also recommended that PIAs be reviewed and/or conducted by an independent authority (i.e., an authority independent of the organization, or department/function/unit that conducted the PIA ).

# Information technology — Security techniques — Privacy impact assessment – Methodology [change title to “Guidelines” is pending]

## 1 Scope

*[Editor's note: The following is the scope defined up to 2nd WD. This is already decided to become subject for a scope change before CD stage.]*

~~This International Standard establishes guidelines for the conduct of privacy impact assessments that are used for the protection of personally identifiable information (PII).~~

~~It should be used by organizations that are establishing, operating or significantly changing programmes, systems or business processes that involve the processing of PII. This International Standard also provides guidance on privacy risk treatment options. Privacy Impact Assessments can be conducted at various stages in the life cycle of a programme, system or business process ranging from the requirement analysis phase to decommissioning. In order to support Privacy by Design, the results of privacy impact assessments have to be considered in the specification of the system.~~

~~In particular, it will provide a specific method for privacy impact assessment.~~

~~It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations. This standard is relevant to any staff involved in designing or implementing projects, including operating data processing systems and services, which will have an impact on privacy within an organization and, where appropriate, external parties are supporting such activities.~~

~~This Standard describes privacy risk assessment as introduced by ISO/IEC 29100:2011. For the basic elements of the privacy framework and the privacy principles, reference is made to ISO/IEC 29100:2011.~~

*[Editor's note: The following is the scope defined at 2013 Incheon sessions. It is the proposal that is foreseen as the scope to be requested with the scope change.]*

This International Standard:

- gives guidelines for a process on privacy impact assessments;
- describes 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 International Standard is relevant to those involved in designing or implementing projects, including operating data processing systems and services, that use PII that may have an impact on privacy within an organization and, where appropriate, external parties are supporting such activities.

*[Editors Note: Suggesting a last discussion on the new scope text before requesting scope change - Focus: Does the “project” term also covers PIA supporting operational changes on releases and changes of stage of system life cycles? Option: Substitute “project” with “business process” like request at other places of the document.]*



## 2 Normative references

The following referenced documents are indispensable for the application 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/IEC 29100, Information technology – Security techniques – Privacy framework

ISO/IEC 27000, Information security management systems -- Overview and vocabulary

ISO 31000, Risk management – Principles and guidelines on implementation

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100:2011, ISO/IEC 27000:2013 and the following apply.

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

**3.2  
asset**  
[based on ISO/IEC 27001:2005]  
anything that has value to the organization

NOTE In the context of privacy risk management process, an asset is either a PII or a supporting asset.

**3.3  
privacy supporting asset**  
components of the information system – hardware, software, networks, personnel, paper, sites... – on which the PII rely

**3.4  
impact**  
[from ISO 15392:2008]  
any change that may be adverse or beneficial

NOTE 1 In terms of privacy, the impact is the adverse change to the privacy of the PII principal.

NOTE 2 impact is defined in ISO/IEC 27000:2009 as “adverse change to the level of business objectives achieved”.

NOTE 3 The “impact of an organization” is defined in ISO 26000:2010 as “positive or negative change to society, economy or the environment, wholly or partially resulting from an organization's past and present decisions and activities”.

NOTE 4 The main impact is to perform non-legal activities.

**3.5  
privacy impact assessment**  
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing privacy risk

*[Editor's note: With the work on ISO 29134 it seems as if it will become necessary to request a change in ISO/IEC 29100 terminology later on.]*

### 3.6

#### **privacy risk treatment**

[on the basis of risk treatment from ISO-Guide 73:2009]

process to modify privacy risk

NOTE 1 Privacy risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- removing the risk source;
- transferring the risk to another party or parties (e.g., by obtaining insurance)
- mitigating the risk by changing the nature and magnitude of likelihood or changing the consequences;
- accepting the risk by informed decision.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.

### 3.7

#### **risk**

effect of uncertainty on objectives

NOTE 1 In a privacy context, a risk can be more precisely defined as the impacts of potential events on PII principals' privacy, and is characterized by its level of impact and its likelihood

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

### 3.8

#### **stakeholder**

alias: interested party

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

## **4 Symbols (and abbreviated terms)**

The following abbreviations are common to ISO/IEC 29134:

CEO	Chief Executive Officer
DPO	Data Protection Officer
IEC	International Electrotechnical Commission
ICT	Information and Communication Technologies
ISMS	Information Security Management System
ISO	International Organization for Standardization

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

## 5 Preparing the grounds for PIA Analysis

### 5.1 Why carry out a PIA? What are the benefits?

A PIA can be carried out for the purpose to

- identify the risks to privacy;
- design for privacy protection (Privacy by Design/Privacy by Default) where possible;
- plan a response for privacy impacts where not;
- aid in stakeholder management where privacy may be a sensitive issue; or
- show compliance, where compliance is required.

A privacy impact assessment PIA has often been described as an early warning system. It provides a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organization makes heavy investments. The costs of fixing a project at the planning stage will be a fraction of those incurred later on. If the privacy impacts are unacceptable, the project may even have to be canceled altogether. Thus, a PIA helps reduce costs in management time, legal expenses and potential media or public concern by considering privacy issues early. It helps an organization to avoid costly or embarrassing privacy mistakes.

Although a PIA should be more than simply a compliance check, it does nevertheless enable an organization to demonstrate its compliance with privacy policy in the context of a subsequent complaint, privacy audit or compliance investigation. In the event of an unavoidable 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.

A PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions 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.

This PIA enables an organization to learn about the privacy pitfalls of a process, system or programme directly, 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 to gain the public's trust and confidence that privacy has been built into the design of a project, technology or service. 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 appropriately demonstrates that the privacy of individuals is a priority for their organization. It affirms that an organization has addressed privacy issues and has taken reasonable steps to provide an adequate level of privacy protection. 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 evidence in due diligence and may reduce the number of customer audits.

A proper 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.

## 5.2 Expectations from PIA and on PIA reporting

Expectations from PIA exist from multiple perspectives - regulator, management, PII principal, client (in case of data processor), privacy function, business function. For e.g.:

Regulator – PIA as an instrument to enable compliance to applicable legal requirements. Also, an exercise which can be presented as due diligence taken by the organization in case of breach, non-compliance, complaint, etc.

Management – PIA as an instrument to manage privacy risks, create awareness and establish accountability; Visibility over PII processing within organization and possible risks and impacts of the same; Inputs to business or product strategy.

Business Function – PIA as an opportunity to better understand privacy requirements and assess activities against these requirements; inputs for product or service design and delivery.

Privacy Function – 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.

Client – PIA to assess how the data processor is handling PII and meeting the contractual obligations.

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

The organization and stakeholders will expect a PIA report to identify the perceived benefits of a new system, technology, service as well as possible risks. The report should recommend measures that can be taken to address the risk(s). The report should say who might be affected by or interested in the new system, technology or service and to what extent the stakeholders have been engaged in the PIA process.

The organization should publish the PIA report or create a summary. The PIA report should be available for the data protection authority.

The PIA reporting objective is to communicate assessment result to stakeholders. It should be clear, objective, free of bias (and more characteristics).

## 5.3 Who should conduct a PIA?

Responsibility for the conduct of a PIA should lie, in the first instance, with a person responsible of conduct a PIA assisting the project manager who intends to develop a new technology, service or other initiative which may have impacts on privacy. Alternatively, the organization's data protection officer (DPO) may act as the person responsible of conduct a PIA or the organization may decide to engage an external consultant to lead the PIA process. More generally, the organization's chief executive officer (CEO) is responsible to the board for ensuring that risks to the organization are managed effectively. The person responsible of conduct a PIA can conduct the PIA or delegate an external independent authority to conduct the PIA, by engaging other stakeholders, internal and/or external, to the organization. The person responsible of conduct a PIA may delegate the conduct (but not the responsibility) to a senior staff member. While there are advantages and disadvantages to each of these options, generally, it is desirable that sensitivity to potential privacy impacts be embedded in the organization and that the DPO acts as an advisor to the person responsible of conduct a PIA.

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

Where carried out, the PIA can be combined, or carried out in alignment with, project business impact assessments.

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;

- specifying risk owners for implementing privacy risk treatment, maintaining privacy controls and reporting of relevant privacy risk information;
- establishing performance measurement and internal and/or external reporting and escalation processes;
- provide regular training and ongoing awareness communications; and
- ensuring appropriate levels of recognition, reward, approval and sanction.

#### **5.4 Scale and scope of a PIA**

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

Organizations should determine whether or not PIA should be conducted depending on compliance requirements from laws and regulations, degree of sensitivity of PII or the size of units of PII to be processed, which it needs to process.

## 6 Process for conducting a PIA

### 6.1 Preparation of the PIA

#### 6.1.1 Determine whether a PIA is necessary (threshold analysis)

Goal: This step aims at determining whether a PIA is necessary or not

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

Actions:

Find decision, if a PIA is needed or not.

Implementation Guidance:

A PIA should be made if an organization is establishing or operating programmes, systems or processes that involve the processing of personally identifiable information (PII), or that is making significant changes to existing programmes, systems or processes that involve the processing of PII or that poses risks to other types of privacy.

*[Editor's note: NBS and Liaisons are requested to provide an example when a change should be seen as significant.]*

NOTE PII should include de-identified data which could re-identify a specific person.

By default, a PIA should be made if sensitive PII (see definition 2.26 in ISO/IEC 29100:2011) is about to be processed.

A PIA should be carried out whenever an organization perceives that

- ⌘ a new or prospective technology, service or other initiative may have impacts on privacy;
- ⌘ Changes apply in applicable privacy related laws and regulations;
- ⌘ Transfer of PII to outside the organization is intended;
- ⌘ Business expansion in a new geography is planned;
- ⌘ Change apply in organizational policies –( privacy policy, information security, human resources, etc) or
- ⌘ Change applies in data access.

A PIA is furthermore required when stipulated in law or sector specific regulations.

Output: Mandate to prepare for a PIA

#### 6.1.2 Identify the PIA team, define risk criteria and set the team's terms of reference

Goal: This step aims to identify needed expertise and to formulate the terms of reference for conducting the PIA

Input: Mandate to prepare for a PIA

Actions:

A person responsible for the conduct of a PIA should be identified and appointed by the organization's management.

The organization should define the terms of reference and scope

The management should also define the risk criteria, based on the followings:

- legal and regulatory requirements, and contractual obligations;
- stakeholders expectations and perceptions, and negative consequences for goodwill and reputation;
- operational and business importance of availability, confidentiality and integrity;
- the strategic value of the business information process.

The risk criteria should be established separately for risks that affect PII from a PII principal's point of view and for risks that affect PII from the organization point of view.

These criteria will be used later on during the privacy risk treatment. The person responsible of conduct a PIA should propose the terms of reference and the scope for the PIA. Management should mandate the person responsible of conduct a PIA to prepare a PIA plan, based on this scope and terms of reference.

#### Implementation Guidance:

The person responsible for the conduct of a PIA may need some additional expertise or the organization's senior management delegate the external independent authority to be responsible for the conduct of a PIA.

The person responsible of conduct a PIA and/or the organization's senior management should decide on the terms of reference and scope for the PIA team.

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 time frame for the PIA, and whether the PIA report is to be published. The minimum requirements for a PIA will depend on how significant an organization deems the privacy risks to be.

The PIA team should consist of, for example, senior management such as the Chief Privacy Officer, employees from the ICT department, employees from relevant business units, and a legal advisor.

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 privacy impact team.

Output: Person responsible appointed, terms of reference and scope of the PIA

### **6.1.3 Prepare a PIA plan**

Goal: This step aims to plan for the PIA

Input: Terms of reference and scope for the PIA

Actions:

Plan the steps of the PIA to be conducted in terms of tasks and needed time and resources

#### Implementation Guidance:

Plan should take into account scope for conducting assessment in multiple iterations, and reporting the same. This is particularly useful when the assessment involves large scale resources, but may not be necessary to proceed if based on the preliminary analysis the initiative need to be abandoned. This also helps the

organization to discontinue resource allocation into the project early in life cycle and instead adopt an alternative approach to meet the intended objectives.

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 consultation 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, on line experience, etc.).

*[Editor's note: With commenting on WD3, a sample plan was requested. NB are invited to provide samples]*

Output: Plan for the PIA to be conducted

#### **6.1.4 Determine the resources for conducting the PIA**

Goal: This step aims to allocate human resources and budget for the conduct of the PIA planned

Input: Plan for the PIA to be conducted

Actions:

Calculate costs and efforts, check availability of team members and decide on the allocation of budget and resources

Implementation Guidance:

Once the person responsible of conduct a PIA has prepared a PIA plan, they can estimate better 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 senior management or the person responsible of conduct 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 PIA.

Consideration should be given to the following:

- people, skills, experience and competences;
- estimation on the time needed for any task;
- resources needed for each step of the PIA.

Output: Business case, allocated resources

#### **6.1.5 Describe the proposed business process to be assessed**

Goal: This step aims at gaining a clear view of what should be taken into consideration in the PIA (e.g.: external and internal factors, scope and risk criteria).

Input: System requirement information, system design information, operational plans and procedures information (see clauses 7.2.1.1 to 7.2.1.3), external and internal factors

Actions:

Create an appropriate description of the business process and system that the PIA is intended for

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 can be used in at least three ways — it helps provide necessary contextual inputs to the person who would do 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 it might impact the privacy, what PII will be collected and what are the platforms used for handling 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.

Output: Description of the business process and system to be assessed

### 6.1.6 Identify stakeholders

Goal: This step aims to identify the individuals or groups of persons that may have interests either in the business process subject to PIA, or in the protection of their PII under this business process.

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

Actions:

The organization should identify all the stakeholders (including end-users) that might have or might obtain an access to PII. As example:

- employees from the organization, including commercials people,
- sub-contractors,
- application administrators,
- computer or network administrators,
- application operators,
- computer or network operators,
- maintenance people,
- people from others organizations.

Implementation Guidance:

Output: Privacy stakeholders identified

### 6.1.7 Communication plan

Goal: This step aims to give structure to the consultation and communication with stakeholders

Input: Privacy stakeholders identified, plan for the PIA to be conducted

Actions:

A plan to communicate and consult with both internal and external stakeholders should be developed at an early stage.

This plan should address issues relating to the impact to the various privacy stakeholders, their consequences (if known), and the measures being taken to manage them.

The plan should identify the types of stakeholders to be consulted. For example, stakeholders could include representatives from government, industry, academia, civil society organizations, consumer organizations, professional organizations, etc.

*[Editor's note: Stronger focus on internal stakeholders is desired; NB/Liaisons are requested to provide contribution]*

#### Implementation Guidance:

The person responsible of conduct a PIA should identify these different categories and then identify specific individuals from within each of the categories, preferably as representative as possible. The range and number of stakeholders to be consulted should be a function of the privacy risks and the assumptions about the frequency and consequences of those risks and the numbers of citizen-consumers who could be impacted.

The key to identifying relevant stakeholders is to determine whether the concerned stakeholders have an interest in or are impacted by the new (or modified) technology, product, service, programme, system or other initiative impacting privacy.

A PIA should seek out and engage stakeholders internal and external to the organization.

Output: Communication plan

### **6.1.8 Consult with stakeholders**

*[Editor's note: On WD3 a comment was received that perception should be treated differently from fact. Relation to stakeholder management and that consultation with stakeholders regarding privacy does not replace the need to consult with stakeholders regarding other matters relating to the project as well. NB/Liaison are requested to provide text]*

Goal: This step aims to conduct the consultation with stakeholders.

Input: Privacy stakeholders identified, Communication plan

#### Actions:

The organization should seek to understand the perspectives of other stakeholders. The organization needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered. The consultation plan should also identify relevant techniques for consulting stakeholders.

#### Implementation Guidance:

The scale and scope of consultation with stakeholders should be a function of the perceived seriousness of the privacy risks and the numbers of people who could be impacted by those risks. 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.

For small and medium enterprises, particularly for small companies, the involvement of stakeholders may be associated with disproportionate time and expense.

For this purpose, alternative approaches are required, which should be defined for example in sector-specific guidelines.

Output: Stakeholder feedback

## 6.2 Iterative phases

### 6.2.1 Analyze the information flows

Goal: This step aims to make transparent how PII is used within the business process.

Input: Description of the business process and system to be assessed

Actions:

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

- who will collect what PII from whom;
- how the organization will use the collected PII;
- how the PII will be stored, secured, processed, and distributed (i.e., to whom the organization might pass on the PII);
- for what purpose;
- how well will secondary users (e.g., the organization's service providers, apps developers) protect that PII;
- whether they will pass it on to still others,
- underlying systems and platforms that handle PII,
- whether PII is likely to be transferred to a new location and if so are there any regulatory restrictions,
- whether there is need to notify the government about new data processing or collection and seek their approval.

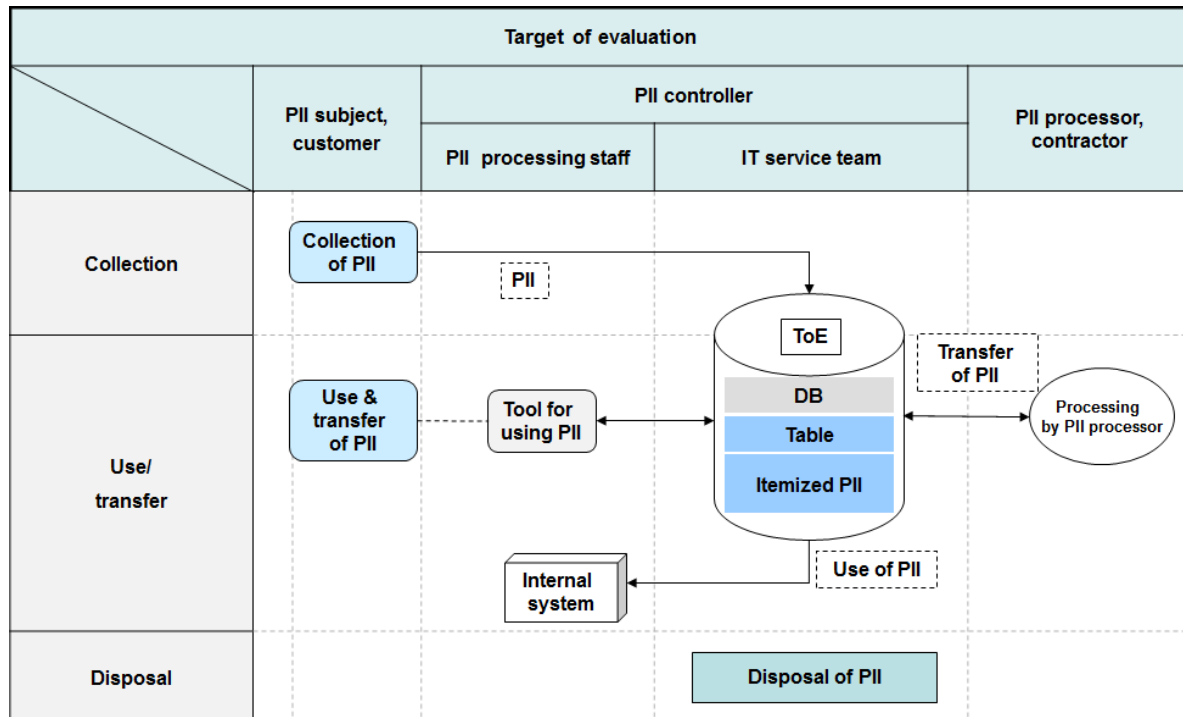


Figure 1 —Data flow diagram PII life cycle

In addition to the documented PII flows the person responsible of conduct a PIA should also focus on one-to-one interactions.

#### Implementation Guidance:

As an input to the PIA, the organization should provide a proper description of the system or other initiative that risks impacting privacy (see clause 7.2.1).

This analysis should be as detailed as possible to help to identify potential privacy risks. The person responsible of conduct a PIA should consider the impacts not only on information privacy, but other types of privacy like physical privacy, spiritual and intellectual privacy, telecommunications secrecy, postal privacy as well. The whole PII life cycle should be considered.

This step could be taken immediately after 6.1.5 and concurrently with 6.1.6.

Output: Summary of findings on the information flow of PII within the business process

### 6.2.2 Check the business process under scope meets the privacy safeguarding requirements

Goal: This step aims to do a compliance check.

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

#### Actions:

The person responsible of conduct a PIA or her legal experts should ensure that the business process under scope complies with any legislative or regulatory requirements regarding privacy and/or data protection.

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

- Identify laws and regulations for applying legal and regulatory requirements to PIA process;
- identify the privacy requirements;
- describe the controls that are expected to fulfill the privacy requirements;
- comply with legal and regulatory requirements; and
- use relevant information available from earlier projects.

The PIA should take into account the privacy principles defined in ISO/IEC 29100:2011 and other legal and regulatory requirements.

Thus, at least, controls that are already existing or planned in order to fulfil the ISO/IEC 29100 principles should be described and evaluated:

- 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;
- privacy compliance.

The controls chosen to fulfil the requirements should be described, or a justification should be brought.

#### Implementation Guidance:

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

NOTE Controls chosen to implement the “information security” principle should be proportionate to the privacy risks assessed in 6.2.3.

A good way to make this analysis consists in using a well know set of controls that could be used in order to verify that no necessary controls have been omitted. ISO/IEC 29151 should be used as a reference.

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 know 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.

Output: List of requirements to comply with (see clause 7.3.2), Compliance analysis (see clause 7.3.3)

### 6.2.3 Assess privacy risk

Goal: Privacy risk assessment is the overall process of privacy risk identification, privacy risk analysis and privacy risk evaluation.

#### 6.2.3.1 Privacy risk identification

Goal: This step aims to identify risks occurring to the PII principal by executing the business process under scope

Input: Description of the business process and system to be assessed

Actions:

Risk identification need to be based on the understanding of the proposed change, which must be documented in sufficient details. Since some of the details that are relevant from data privacy regulation perspective do not get specified in documents, it is important to list assumptions based on which the risks are being identified.

For the step of privacy risk identification, the organization should identify sources of privacy risk, areas of impacts, events and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of privacy risks based on those events that might prevent, degrade or delay the achievement of the privacy principles. Comprehensive identification is critical. Identification should include privacy risks whether or not the source of those risks is under control of the organization.

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 regions in which the solution will be deployed should be used to support the identification of risks for privacy breach.

For each processing of PII, the potential consequences on the PII principals' privacy should be identified in case of:

- an access to the PII by an unauthorized person (loss of confidentiality);
- a modification of the PII (loss of integrity);
- a disappearance of the PII (loss of availability);
- a misappropriate linking of PII (loss of linkage prevention);
- non sufficient information on the processing of PII (loss of transparency);
- non considering the rights of the PII principal (loss of intervention capability);
- collection and processing of PII without the knowledge of PII Principal (loss of control) as one of the potential consequences

for each of those risks:

- the most likely risk sources should be identified;
- the most likely threats should be identified;
- the most severe consequences on PII principals' privacy should be identified; and
- an owner should be identified.

Implementation Guidance:

Relevant and up-to-date information is important in identifying privacy risks. This should include suitable background information where possible. People with appropriate knowledge should be involved 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, it is advisable that stakeholders support the identification of privacy risks.

Output: Identified privacy risks, threats and consequences

### **6.2.3.2 Privacy impact analysis**

Goal: This step aims to determine the impact of the privacy risks identified.

Input: Identified privacy risks, threats and consequences

Actions:

The organization should provide as the results of its analysis the list of privacy risks, including their potential consequences and threats, estimated in terms of level of impact and likelihood.

For determining the impact of the privacy risk, the organization

- should consider the scale criteria given in Annex A; and
- may add its own definitions to the list of criteria.

If a privacy risk is rated as having a high or very high impact and/or a likely or very likely risk, the organization should consider performing a more detailed analysis to go into further details for this privacy risk in order to split it up into serious and less serious sub-scenarios of the privacy risk. This can help the organization to better tailor the treatment activities later on and therefore can increase efficiency and economics.

The overall privacy impact should be the highest impact category determined through the impact analysis process.

For each of those risks identified (see clause 6.2.3.1 Privacy risk identification)

- the existing controls should be identified and associated to the risk(s) they help to treat;
- the level of impact should be estimated based on those potential consequences and the scale(s) determined in the risk criteria.

For each privacy risk, the organization should consider possible scenarios that show what consequences can occur. All significant scenarios should be considered.

The result of this phase is the production of a list of risks, each one associated with its risk levels expressed in a way that is compatible with the risk criteria established in clause 6.1.2.

Implementation Guidance:

Privacy risk analysis involves consideration of the causes and sources of privacy risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect

consequences and likelihood should be identified. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness should be taken into account.

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 organization in the case of a breach of privacy, the information available and the purpose for which the privacy risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different privacy risks and their sources.

The level of confidence in the determination of privacy risks and their sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and other stakeholders if required. Factors such as divergence of opinion among experts or limitations on modeling should be stated and may be highlighted.

Privacy impact 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.

People with appropriate knowledge should be involved when estimating privacy risks.

Care must be exercised to ensure that multiple PIAs are not being conducted involving common systems simultaneously, to prevent overlap and wrong identification of risks and action plans.

Output: Level of impact to any risk identified

### **6.2.3.3 Privacy impact evaluation**

Goal: This step aims to determine actions to treat the privacy risks

Input: Identified privacy risks, threats and consequences, level of impact to any risk identified

Actions:

Privacy impact evaluation involves comparing the level of privacy risk found during the analysis process with privacy risk criteria established in clause 6.1.2.

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

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

The output of this phase is a list of risks prioritized according to risk criteria in relation to the risks.

Implementation Guidance:



Decisions should take account of the wider context of the privacy impact and include consideration of the tolerance of the privacy risks by the PII principal. Decisions should be made in accordance with legal, regulatory and other requirements.

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

A privacy risk map should be done from 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.

Output: Privacy risk map

## 6.2.4 Treat privacy risks

### 6.2.4.1 Choose the privacy risk treatment options

Goal: This step aims to decide on the treatment option for any privacy risk assessed

Input: Privacy risk map

Actions:

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 could be impacted by the organization (e.g., their PII is controlled or processed by the organization).

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 impact 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, it is advisable that stakeholders support 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.

If the resources for privacy risk treatment are 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 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 that the measures remain effective.

There should be at least one applicable privacy risk treatment option applied to any privacy risk identified. If a treatment option is applicable should be retrieved from clause 6.2.3.3.

Implementation Guidance:

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

**Risk reduction**

The level of risk should be reduced through the selection of controls so that the residual risk can be re-assessed as being acceptable both for the organization and for the stakeholders (in particular the end-users).

Reducing the risks for the end-users may be conflicting with the benefits for the organization of the presence or of the use of a particular privacy related data.

These controls may concern modifications to the kind of specific personal data that is captured, to the processes, to the privacy policy, to the organizational structure, to the operating procedures, to the supporting assets, to applications or to the qualifications of the personal.

Modifications to the supporting assets or to applications may be of three kinds: preventive measures, detection measures or correction measures. When preventions controls are not possible or would be too expensive, detection and correction measures may be sufficient, in particular when the detection controls are advertised and thus may act as a deterrent.

**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.

**Risk avoidance**

When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision may be made 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.

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

It should be noted that 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.

Output: Privacy risk treatment map

**6.2.4.2 Determine controls**

Goal: This step aims to identify appropriate controls to the treatment options chosen.

Input: Privacy risk treatment map

Actions:

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

These additional controls may be created from scratch or taken from good practices issued by recognized institutions or international standards. Generally, they must be adapted to the specific context of each processing operation under consideration.

This should consist in determining additional controls that will cover:

- the primary assets: controls designed to prevent data breaches, to detect such breaches or to restore their security (informing data subjects, 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 backfire (physical and logical access control, activity tracking, management of third parties, protection against malicious codes, 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 1: It is worth supplementing the system with cross-organizational controls (organization, policy, monitoring, etc.) in order to improve the maturity of personal data protection.

NOTE 2: The higher the capabilities of the risk sources, the more robust controls should be in order to withstand them.

NOTE 3: PIA not necessarily requires to have an ISMS set up for its use.

#### Implementation Guidance:

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

Explanations about why residual risks may be accepted should be given. 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 person responsible of conduct a PIA and/or the organization may not accept all of the PIA recommendations, but they should say which recommendations they are implementing, why they may not implement others and what are the plans for implementing the recommendations.

Recommended actions not implemented by the person responsible of conduct a PIA should be brought to Privacy office for recommending alternate actions or risk acceptance by senior management.

*[Editor's Note: The term "privacy office" of above is not specified yet. NB's and liaisons are requested to provide explanations.]*

Output: List of chosen controls

#### **6.2.4.3 Create privacy risk treatment plans**

Goal: This step aims to plan and to implement the risk treatment actions.

Input: List of chosen controls

Actions:

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

When planning how to achieve its information security objectives, the organization should determine:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed; and
- 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 are protected against which risks;
- 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;
- resource requirements; and
- timing and schedule.

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

A Statement of Applicability should be produced in order to explain whether the controls from the reference lists are implemented or not, and the justification for exclusions of controls from the reference lists.

Risk owner's approval of the privacy risk treatment plan and the acceptance of the residual privacy risks should be obtained. Management responsibility should also be obtained by signing the acceptance statement.

The organization should implement the privacy risk treatment plan (see clause 6.3.2).

Implementation Guidance:

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

These additional controls may be created from scratch or taken from good practices issued by recognized institutions or international standards. Generally, they must be adapted to the specific context of each processing operation under consideration.

This should consist in determining additional controls that will cover:

- the PII: controls designed to prevent data breaches, to detect such breaches or to restore their security (informing data subjects, 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 backfire (physical and logical access control, activity tracking, management of third parties, protection against malicious codes, etc.);
- if the above is insufficient, the privacy 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 1: It is worth supplementing the system with cross-organizational controls (organization, policy, monitoring, etc.) in order to improve the maturity of personal data protection.

NOTE 2: The higher the capabilities of the risk sources, the more robust controls should be in order to withstand them.

Then, the existing and determined controls should be compared to reference lists of controls and verify that no necessary controls have been omitted:

- controls in ISO/IEC 27001 Annex A;
- controls in any relevant privacy sets of controls;
- controls from the external factors;
- controls from the internal factors.

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

Explanations about why residual risks may be accepted should be given. 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).

Output: Privacy risk treatment plan, Statement of Applicability, Risk owner approvals, acceptance statement

## 6.3 Follow up of the PIA

### 6.3.1 Prepare and publish the report

Goal: This step aims to report on the outcome of the PIA.

Input: Outputs from previous steps

Actions:

At the end of each PIA, the results of each step should be recorded into a comprehensive report (see clause 7.)

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

The PIA report should be published, where sensitive information should be redacted or put in a confidential annex or the PIA report could be summarized. The organization should maintain a registry of PIA reports on its website. The registry could be a simple listing of the PIAs, their titles and the dates the PIA reports were published. The registry should be easy to find by visitors to its website and they should be able to download a copy of any PIA of interest.

#### Implementation Guidance:

The registry serves several purposes. It provides "corporate memory" – i.e., it provides a reference document for those in the organization who were not involved in the PIA to understand what happened and what were the recommendations. 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.

At the end of each PIA, the results of each step should be recorded into a comprehensive report.

Output: PIA report

### **6.3.2 Implement privacy risk treatment plans**

Goal: This step aims to implement the controls.

Input: Privacy risk treatment plan, Risk owner approvals

#### Actions:

Once the PIA report has been approved by the person responsible of conduct a PIA and the managers of the organization, several actions need to be performed:

- The human resources that are necessary to implement, manage and maintain the project need to be identified.
- An appropriate training for the people involved in the project needs to be performed to make sure that all these people are sensitive to the privacy implications, the possible impacts on privacy, of what they or their colleagues do.
- The budget for implementing, managing and maintaining the project, including the implementation of the controls identified earlier, needs to be estimated and obtained from the management.
- 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.
- A periodic internal audit needs to be performed for monitoring and review. A method for the measurement of the effectiveness of controls needs to be defined. The gaps identified in the internal audit must be addressed by identifying additional preventive, audit or corrective controls.
- When there are significant changes in the project affecting the processing of privacy-related data or the way in which the project was previously presented to stakeholders, the organization should have a mechanism for updating the PIA report as necessary. The organization should explain why changes are being made in the project and how these changes might affect the processing and/or disposition of privacy-related data.

Implementation Guidance:

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

Output: none

### **6.3.3 Independent review and/or audit of the PIA**

Goal: This step aims to opt for an independent review of the PIA conducted

Input: PIA report

Actions:

Third-party review or audit of the PIA is a way of ensuring that the PIA has been conducted appropriately and that the organization has implemented the risk treatment plan or, if it has not implemented some, 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).

Implementation Guidance:

Third-party review or audit is a way of giving credibility to the PIA report, of improving transparency, of learning from experience and raising the quality of PIA practices.

Output: Review report

### **6.3.4 Re-Initiate PIA**

Goal: This step aims to deal with changes in a business process formerly assessed.

Input: Significant change within the business process or system

Actions:

The organization should have a mechanism for updating 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.

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.

Implementation Guidance:

[void section]

Output: Decision on another iteration of PIA

## 7 Structure of PIA report

This chapter gives guidance on the content of this report. The PIA report should contain at least

- the introduction (Clause 7.1);
- the scope of the assessment (Clause 7.2);
- the privacy requirements (Clause 7.3);
- the risk assessment (Clause 7.4);
- the risk treatment (Clause 7.5); and
- the conclusion and decisions taken on the basis of the outcome of the PIA (Clause 7.6).

The PIA report should state on its cover page at least the name of the project, name and address of the sponsoring organization, contact person along with contact details, and the date of the PIA report. The length of the PIA report may justify an executive summary.

### 7.1 Introduction

As a minimum, the PIA should state the name or title of the project or otherwise indicate the subject of the PIA. It should indicate the name of the person who conducted the PIA, her or his title and contact details and for whom the PIA was prepared. The cover page should also include the date of the PIA report, its version number for document control and to whom any queries can be addressed 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. It should provide some information about the project assessed. It should introduce the methodology employed in the PIA (e.g., the decision re 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. It should state why the PIA was undertaken, who initiated the PIA, who conducted it. The executive summary should provide a brief description of the project or technology or service or other initiative, which was the subject of the PIA. It should identify the principal privacy impacts and the alternatives for minimizing or avoiding negative impacts.

### 7.2 Scope of PIA

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

It is also advisable that some statement is made regarding the edge of assessment and what was considered being out of the scope.

#### 7.2.1 Business process under evaluation

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, system or other initiative that will be the subject of the PIA.



In order to gain a clear view of the scope under consideration, the following questions should be answered:

- Which processing(s) of PII is(are) concerned?
- What is its(their) purpose?
- 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...)?
- How will PII principals be informed and make consent? Will the process be aligned with its context?
- What are the PII that are processed?
- What are the supporting assets (on which the primary assets rely) within the scope?

The PIA report should state how individuals are informed that the organization is collecting information about them, and what role individual consent plays in the project. 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 data 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 data and how much time it takes the organization to respond to requests.

Therefore, the organization should provide to the PIA team detailed documentation on the system requirements, the system design and the operational plans and procedures.

#### 7.2.1.1 System requirement information

The system requirement information should contain at least:

- the purpose of processing;
- a description of the business process that is, or will be, supported by the system;
- the list of functional requirements defined for the 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 data, including the parameters regarding data subject access;
- if the system or its data are intended to be shared with third parties, information about with whom the system or data will be shared and for which purpose(s); and
- a statement on the justification for processing the PII involved in this system.

### 7.2.1.2 System design information

The system design information should contain at least:

- an overview of the functional (or logical) architecture;
- an overview of the physical architecture;
- the structure of system databases, tables and fields, especially the list of PII;
- a data flow diagram in logical and technical means;
- a data flow diagram through the life cycle of PII, e.g. generation, use, transfer, and disposal of PII;
- a work flow diagram which describe when to notify and get consent from PII principles; and
- a list of interfaces, defining the parties connected and the data fields transferred.

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

- which kinds of hardware (computers, routers, electronic media, etc.)?
- which kinds of software (operating systems, messaging systems, databases, business applications, etc.)?
- what are the 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.)?

### 7.2.1.3 Operational plans and procedures information

The operational plans and procedures information should contain at least:

- the identity and user management concept for the system;
- the operational concept, especially if the system or parts of it are operated on site, externally hosted or housed, or if they are cloud sourced and in which geographical area;
- the support concept, especially listing third parties by name that are involved in supporting the system, the degree to which they will have access to PII and locations from where the data can be accessed;
- the logging concept and the respective retention plans for the logged information;
- the backup and recovery plans;
- the data retention and deletion plans and media disposal; and
- the decommissioning concept.

### 7.2.2 Risk criteria

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

- What are the criteria used to estimate the severity? (e.g. level of identification and level of impact)
- What are the criteria used to estimate the likelihood? (e.g. 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 the strategy is modified by the benefits of the processing(s) of PII?

NOTE 1: Those criteria should be consistent with the other risk criteria used within the organization.

NOTE 2: The opportunity to improve them should be considered each time they have been used.

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

- legal and regulatory requirements, and contractual obligations;
- stakeholders expectations and perceptions, and negative consequences for goodwill and reputation;
- operational and business importance of availability, confidentiality and integrity;
- the strategic value of the business information process.

The risk criteria should be established separately for risks that affect PII from an PII principal point of view and for risks that affect PII from the organization point of view.

These criteria will be used later on during the privacy risk treatment.

### 7.2.3 Resources - stakeholders, people involved

It is necessary to understand the capabilities of the organization, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems and technologies).

In preparation to the PIA process the organization is expected to have identified the types of stakeholders to be consulted (see clause 6.1.8).

The PIA should have sought to understand the perspectives of other stakeholders. The organization needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered.

## 7.3 Privacy Requirements

ISO/IEC 29100 has defined a set of privacy principles. In addition, some national legislation and/or regulation may include other privacy principles. A PIA should refer to these various principles and pose a set of questions aimed at determining whether the new system, technology or service that is subject to the PIA respects those principles. The privacy principles in ISO/IEC 29100 refer to data protection or information privacy. However, there are other types of privacy and they too should be considered in order to determine whether the system, technology or service might have some impacts on those other types of privacy.

### 7.3.1 Context, Stakes, Goals

This part should highlight the stakes of the processing of PII (financial benefits, social benefits...).

### 7.3.2 Requirements to comply with

Early in starting the PIA process, the organization should have identified the obligations it has to comply with in order to do the processing of PII as it is under assessment.

These obligations may come from

- the organization's social responsibility, especially in terms of the privacy principles given from ISO/IEC IS 29100:2011;
- legislation; or
- organization or branch self obligations, e.g. as part of a privacy policy.

The PIA report shall list

- the sources of obligations and
- the different aspects, that will need compliance for fulfilling the respective obligation,

which the PIA team had identified for the business process under scope.

### 7.3.3 Compliance Analysis

With respect to the set of requirements given from clause 7.3.2 above, the PIA team should state 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.

## 7.4 Risk assessment

### 7.4.1 Risk Sources

The organization should identify sources of privacy risk (see clause 6.2.3)

### 7.4.2 Consequences and their level of Impact

For each processing of PII the potential consequences on the PII principals privacy should be identified in case of:

- an access to the PII by an unauthorized person (loss of confidentiality);
- a modification of the PII (loss of integrity);
- a disappearance of the PII (loss of availability);
- a misappropriate linking of PII (loss of linkage prevention);
- non-sufficient information on the processing of PII (loss of transparency); and
- non considering the rights of the PII principal (loss of intervention capability).

For each of those risks:

- the most likely risk sources should be identified;
- the existing controls should be identified and associated to the risk(s) they help to treat;
- an owner should be identified.

The severity of impact should be estimated as described in section 6.2.3.2..

#### **7.4.3 Threats and their likelihood**

For each processing of PII and each potential consequences on the PII principals privacy:

- the threats that may allow the identified risks to occur should be determined.

The likelihood should be estimated thanks to the vulnerabilities of the supporting assets, the capabilities of the risk sources to exploit them and the scale(s) determined in the risk criteria.

#### **7.4.4 Risk evaluation**

A privacy risks map should be done from 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.

#### **7.5 Risk treatment**

*[Editor note: Content is needed for this section. NB/Liaisons are requested to provide contributions]*

#### **7.6 Conclusion and Decisions**

*[Editor note: Content is needed for this section. NB/Liaisons are requested to provide contributions]*

## Annex A (informative)

### Scale criteria on the level of impact and on the likelihood

This Annex contains the criteria for detecting the impact of a potential privacy breach as indicated in clause 6.2.3.2 of this standard. This Annex contains criteria any organization should consider.

#### A.1 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: Data subjects 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: Data subjects 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: Data subjects 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: Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial 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.: very identifying PII, dangerous 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 an aggravating factor; conversely, poorly identifying PII, not dangerous risk sources, very few or no interconnections or recipients might lower the level of impact.

**Table 1 — Impact given by the nature of the PII**

Nature of the PII		Impact scale
<b>A.2</b> The likelihood of each threat should be	PII that are publicly accessible (e.g., in telephone directories, address books or selection lists)	1
	PII that <b>require a legitimate interest</b> for access (e.g., restricted public files or the members of a distribution list)	2
	PII whose unauthorized disclosure can <b>affect the reputation</b> 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 <b>affect the existence</b> or the <b>health, freedom and life</b> of the PII principal (e.g., information about commitment to an institution, a sentence, personnel reviews, health data, debts, or if the PII principal is at risk of becoming a victim in a criminal case)	4

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 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 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.

### A.3 How to set objectives

Objectives may be set based on where risks are located on the risk map (their level of impact and likelihood):

1. Risks with a high level of impact and likelihood should not be taken. They should be avoided or reduced by implementing controls that reduce both their level of impact and their likelihood. Ideally, care should even be taken to ensure that these risks are treated by independent controls of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event).
2. Risks with a high level of impact but a low likelihood may be taken only if it is demonstrated that their severity cannot be reduced and if their likelihood is negligible. They should be avoided or reduced by implementing controls that reduce either their level of impact or their likelihood. Emphasis should be placed on preventive controls.
3. Risks with a low level of impact but a high likelihood may be taken only if it is demonstrated that their severity cannot be reduced and if their likelihood is negligible. They should be reduced by implementing controls that reduce their likelihood. Emphasis should be placed on recovery controls.
4. Risks with a low level of impact and likelihood may be taken, especially since the treatment of other risks should also lead to their treatment.

### A.4 Factors to be taken into account at specific sectors

This clause contains factors the organization should consider in the estimation of either the level of impact or of the likelihood whenever applicable.

For illustrative purpose, a four (4) categories scale scheme is used with 1 standing for “low impact/low likelihood”, 2 for “medium impact/medium likelihood”, 3 for “high impact/likely” and 4 for “very high impact/very likely”. If the organization is making use of a different scale scheme, appropriate translation should be made.

*[Editor's note: Better explanation is needed how these factors should fit into the process to estimate the level of impact or the likelihood. NB/Liaison contributions are welcome]*

**Table 2 — Impact factors by programme or activity partners and private sector involvement**

Programme or activity partners and private sector involvement	Impact factor scale
Within the institution (among one or more programmes within the same institution)	1
With other government institutions	2
With other institutions or a combination of federal, provincial or territorial, and municipal governments	3
Private sector organizations, international organizations or foreign governments	4

*[Editor's note: Should the factor above count with likelihood or impact or with both?]*

Programme population	Impact factor scale
The programme's use of PII for internal administrative purposes affects certain employees.	1
The programme's use of PII for internal administrative purposes affects all employees.	2
The programme's use of PII for external administrative purposes affects certain individuals.	3
The programme's use of PII for external administrative purposes affects all individuals.	4

**Table 3 — Impact factors by programme population****Table 4 — Likelihood factor by PII transmission**

PII transmission	Likelihood scale
The PII is used within a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled).	1
The PII is used in a system that has connections to at least one other system.	2
The PII is unencrypted and transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed.	3
The PII is transmitted using wireless technologies.	4



## **Annex B** (informative)

### **Generic threats**

The following table presents generic threats (the same systematic events on each supporting assets and the risk they are related to).

The supporting assets (on which the PII rely) are systematically the following:

- Hardware: computers, communications relay, USB drives, hard drives...
- Software: operating systems, messaging, databases, business applications...
- Computer channels: cable, wireless, fiber optic...
- Individuals: users, administrators, top management...
- Paper documents: printing, photocopying...
- Paper transmission channels: mail, work-flow...

The actions on those supporting assets (that risk sources can do, voluntary or not) are systematically the following:

- Abnormal use / function creep: supporting assets are diverted from their intended context of use without being altered or damaged;
- Damage: supporting assets are partially or completely damaged;
- Espionage: supporting assets are observed without being damaged;
- Loss: supporting assets are lost, stolen, sold or given away, so it is no longer possible to exercise property rights;
- Modification / change: supporting assets are transformed;
- Overload / exceeded limits of operation: supporting assets are overloaded, over-exploited or used under conditions not permitting them to function properly.

**Table 5 — Generic threats**

Supporting assets	Action	Privacy risk	Examples of threats
Hardware	Abnormal use	Disappearances of PII	Storage of personal files; personal use, etc.
Hardware	Abnormal use	Illegitimate accesses to the PII	Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.
Hardware	Damage	Disappearances of PII	Flooding, fire, vandalism, damage from natural wear and tear, storage device malfunction, etc.
Hardware	Espionage	Illegitimate accesses to the PII	Watching a person's screen without them knowing while on the train; taking a photo of a screen; geolocation of hardware; remote detection of electromagnetic signals, etc.
Hardware	Loss	Disappearances of PII	Theft of a laptop or cellphone; disposal of a device or hardware, etc.
Hardware	Loss	Illegitimate accesses to the PII	Theft of a laptop from a hotel room; theft of a professional cellphone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc.
Hardware	Modification	Disappearances of PII	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of the system, etc.
Hardware	Modification	Illegitimate accesses to the PII	Tracking by a hardware-based keylogger; removal of hardware components; connection of devices (such as USB flash drives) to launch an OS or retrieve data, etc.
Hardware	Modification	Unwanted changes in the PII	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of an application, etc.
Hardware	Overload	Disappearances of PII	Storage unit full; power outage; processing capacity overload; overheating; excessive temperatures, etc.
Software	Abnormal use	Disappearances of PII	Erasure of data; use of counterfeit or copied software; operator errors that delete data, etc.
Software	Abnormal use	Illegitimate accesses to the PII	Content scanning; illegitimate cross-referencing of data; raising of privileges, wiping of usage tracks; sending of <i>spam</i> via an e-mail program; misuse of network functions, etc.

Supporting assets	Action	Privacy risk	Examples of threats
Software	Abnormal use	Unwanted changes in the PII	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc.
Software	Damage	Disappearances of PII	Erasure of a running executable or source codes; logic bomb, etc.
Software	Espionage	Illegitimate accesses to the PII	Scanning of network addresses and ports; collection of configuration data; analysis of source codes in order to locate exploitable flaws; testing of how databases respond to malicious queries, etc.
Software	Loss	Disappearances of PII	Non-renewal of the license for software used to access data, etc.
Software	Modification	Disappearances of PII	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.
Software	Modification	Illegitimate accesses to the PII	Tracking by a software-based key logger; infection by malicious code; installation of a remote administration tool; substitution of components, etc.
Software	Modification	Unwanted changes in the PII	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.
Software	Overload	Disappearances of PII	Exceeding of database size; injection of data outside the normal range of values, etc.
Computer channels	Damage	Disappearances of PII	Cut wiring, poor Wi-Fi reception, etc.
Computer channels	Espionage	Illegitimate accesses to the PII	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.
Computer channels	Loss	Disappearances of PII	Theft of copper cables, etc.
Computer channels	Modification	Unwanted changes in the PII	<i>Man-in-the-middle attack</i> to modify or add data to network traffic; replay attack (resending of intercepted data), etc.
Computer channels	Overload	Disappearances of PII	Misuse of bandwidth; unauthorized downloading; loss of Internet connection, etc.
Individuals	Abnormal use	Illegitimate accesses to the PII	Influence (phishing, social engineering, bribery, etc.), pressure (blackmail, psychological harassment, etc.), etc.
Individuals	Abnormal use	Unwanted changes in the PII	Influence (rumor, disinformation, etc.), etc.

Supporting assets	Action	Privacy risk	Examples of threats
Individuals	Damage	Disappearances of PII	Occupational accident; occupational disease; other injury or disease; death; neurological, psychological or psychiatric ailment, etc.
Individuals	Espionage	Illegitimate accesses to the PII	Unintentional disclosure of information while talking; use of listening devices to eavesdrop on meetings, etc.
Individuals	Loss	Disappearances of PII	Reassignment; contract termination or dismissal; takeover of all or part of the organization, etc.
Individuals	Loss	Illegitimate accesses to the PII	Employee poaching; assignment changes; takeover of all or part of the organization, etc.
Individuals	Overload	Disappearances of PII	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc.
Individuals	Overload	Unwanted changes in the PII	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc.
Paper documents	Damage	Disappearances of PII	Aging of archived documents; burning of files during a fire, etc.
Paper documents	Espionage	Illegitimate accesses to the PII	Reading, photocopying, photographing, etc.
Paper documents	Loss	Disappearances of PII	Theft of documents; loss of files during a move; disposal, etc.
Paper documents	Loss	Illegitimate accesses to the PII	Theft of files from offices; theft of mail from mailboxes; retrieval of discarded documents, etc.
Paper documents	Modification	Unwanted changes in the PII	Changes to figures in a file; replacement of an original by a forgery, etc.
Paper documents	Overload	Disappearances of PII	Gradual erasure over time; voluntary erasure of portions of a document, etc.
Paper transmission channels	Damage	Disappearances of PII	End of workflow following a reorganization; mail delivery halted by a strike, etc.
Paper transmission channels	Espionage	Illegitimate accesses to the PII	Reading of signature books in circulation; reproduction of documents in transit, etc.

Supporting assets	Action	Privacy risk	Examples of threats
Paper transmission channels	Loss	Disappearances of PII	Elimination of a process following a reorganization; loss of a document delivery company, etc.
Paper transmission channels	Modification	Disappearances of PII	Change in how mail is shipped Reorganization of paper transmission channels; change in working language, etc.
Paper transmission channels	Modification	Unwanted changes in the PII	Changes to a memo without the author's knowledge; change from one signature book to another; sending of multiple conflicting documents, etc.
Paper transmission channels	Overload	Disappearances of PII	Mail overload; overburdened validation process, etc.

## Annex C (informative)

### Example of an Inventory tool supporting PIA

#### C.1 Inventory tool

The Data Inventory tool contains 17 columns A to Q with the column headers and comments listed in table 1 here below.

**Table 6 — Data inventory table structure**

Column	Header	Comment regarding to the Column
A	Desc of Personal Data / Data Cluster	None
B	Personal Info Category	Contact information, file (photos, videos, music, notes), location data, bookmarks, sensor data, log files (including behavior history, browser history), messages (including SMS and email), system settings, user preferences, content metadata, contextual/derived data, account information, user identifiers, device identifiers, biometric data, financial data, health data, racial data, sexual preference data, religious preference data, trade association data, political data
C	PII Classification	PII 2.0 Classification: — Not Identifiable — Possibly Identifiable — Identifiable — Sensitive
D	Source	Author: — User Generated — System Generated
E	Collected By	None
F	Collection Method	None
G	Type of Format	None
H	Used By	None
I	Purpose of Collection	Primary purpose Secondary purpose
J	Transfer to: De-Identification	Named internal interactor, Named external interactor
K	Security Classification	Security Classification: — Public — Internal Only — Confidential — Secret
L	Security Control During Data Transfer	None
M	Data Repository Format	None
N	Storage or Data Retention Site	Country location of server, Server name, IP address
O	Disclosed To	Named internal interactor,

		Named external interactor
P	Retention Policy	None
Q	Deletion Policy	None

## Annex D (informative)

### Text that needs reordering

*[Editor's note: This annex was created in order to preserve text clauses that were found to be valid keeping, but need to find a new destination within the document]*

[formerly part of 6.1.1]

It should be used when the impact to a PII principal needs consideration for processes, systems or programmes, where:

- The responsibility for the implementation and/or delivery of the process, system or programme is shared with other organizations and there is a need to ensure that each organization properly addresses the identified risks;
- a single organization is performing privacy risk management as part of its overall risk management effort in preparation for implementation or improvement of its ISMS (established in accordance with ISO 27001) or equivalent system; or a single organization is performing privacy risk management as a dedicated task for privacy impact only; or
- a legislator runs another programme, in which the final PII controller organization is not known yet, with the result that the treatment plan will be without an obligation yet and the controls proposed should become subject to a resulting legislative or other regulatory framework.

[formerly part of 6.1.5]

The context of the PIA will vary according to the needs of an organization. It can involve, but is not limited to:

- defining responsibilities for the assessment and treatment of privacy risks;
- defining the scope, as well as the depth and breadth of the privacy risk treatment activities to be carried out, including specific inclusions and exclusions;
- defining the activity, process, function, project, product, service or asset in terms of time and location as well as its goal and objectives;
- defining the relationships between a particular project or activity and other projects or activities of the organization;
- defining the way performance is evaluated in the management of privacy risk;
- identifying and specifying the decisions that have to be made to the privacy risk treatment;
- identifying the stakes of the processing;
- identifying the main external references (legal and regulatory, sectoral, etc.) to comply with;
- identifying the main internal guidelines (policies, procedures, etc.) to be considered ;
- determining the privacy risk criteria, including those that are used to evaluate the significance of the privacy risks and risk acceptance criteria.



## Bibliography

- [1] ISO 31000, Risk management – Principles and guidelines on implementation
- [2] ISO Guide 73, Risk management – Vocabulary
- [3] ISO 27005, Security techniques - information security risk management
- [4] ISO 22307, Financial Services – Privacy impact assessment
- [5] Treasury Board of Canada Secretariat Directive on Privacy Impact Assessments <http://www.tbs-sct.gc.ca/pol/inconspicuous?id=18308>
- [6] "Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada" [http://www.priv.gc.ca/information/pub/gd\\_exp\\_201103\\_e.cfm](http://www.priv.gc.ca/information/pub/gd_exp_201103_e.cfm)
- [7] PIA Framework for RFID Applications  
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180\\_annex\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf)
- [8] HIMSS Privacy Impact Assessment Guide  
[http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D87\\_HIMSS\\_PIA\\_Guide\\_FinalV2.pdf](http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D87_HIMSS_PIA_Guide_FinalV2.pdf)
- [9] The ICO PIA handbook [http://www.ico.gov.uk/upload/documents/pia\\_handbook\\_html\\_v2/index.html](http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html)
- [10] "The Privacy Office Official Guidance – June 2010 ", US Department of Homeland Security - Privacy Office [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_guidance\\_june2010.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf)
- [11] PIA Guidelines German BSI
- [12] Tancock | Pearson | Charlesworth: The Emergence of Privacy Impact Assessments  
<http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf>
- [13] DoD Privacy Impact Assessment (PIA) Guidance  
<http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf>
- [14] Privacy Impact Assessments: International Study of their Application and Effects October, 2007 Linden Consulting, Inc.
- [15] Wright, David, "The state of the art in privacy impact assessment", Computer Law & Security Review, Vol, 28, No. 1, Feb. 2012, pp. 54-61. <http://www.sciencedirect.com/science/journal/02673649>
- [16] Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al. (eds.), European data protection: coming of age?, Springer, Dordrecht, 2013.
- [17] Wright, David, and Paul de Hert (eds.), Privacy Impact Assessment, Springer, Dordrecht, 2012.
- [18] Wright, David, "Making Privacy Impact Assessment More Effective", The Information Society, Vol. 29, No. 5, 2013, pp. 307-315. <http://www.indiana.edu/~tisj/29/index.html#5>
- [19] Methodology for privacy risk management, CNIL, 2012,  
<http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf>