

INTERNATIONAL STANDARD

ISO/IEC 29134

First edition
2017-06

Information technology — Security techniques — Guidelines for privacy impact assessment

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



Reference number
ISO/IEC 29134:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Preparing the grounds for PIA	4
5.1 Benefits of carrying out a PIA	4
5.2 Objectives of PIA reporting	5
5.3 Accountability to conduct a PIA	5
5.4 Scale of a PIA	6
6 Guidance on the process for conducting a PIA	6
6.1 General	6
6.2 Determine whether a PIA is necessary (threshold analysis)	7
6.3 Preparation of the PIA	7
6.3.1 Set up the PIA team and provide it with direction	7
6.3.2 Prepare a PIA plan and determine the necessary resources for conducting the PIA	9
6.3.3 Describe what is being assessed	10
6.3.4 Stakeholder engagement	11
6.4 Perform the PIA	13
6.4.1 Identify information flows of PII	13
6.4.2 Analyse the implications of the use case	14
6.4.3 Determine the relevant privacy safeguarding requirements	15
6.4.4 Assess privacy risk	16
6.4.5 Prepare for treating privacy risks	19
6.5 Follow up the PIA	23
6.5.1 Prepare the report	23
6.5.2 Publication	24
6.5.3 Implement privacy risk treatment plans	24
6.5.4 Review and/or audit of the PIA	25
6.5.5 Reflect changes to the process	26
7 PIA report	26
7.1 General	26
7.2 Report structure	27
7.3 Scope of PIA	27
7.3.1 Process under evaluation	27
7.3.2 Risk criteria	29
7.3.3 Resources and people involved	29
7.3.4 Stakeholder consultation	29
7.4 Privacy requirements	29
7.5 Risk assessment	29
7.5.1 Risk sources	29
7.5.2 Threats and their likelihood	29
7.5.3 Consequences and their level of impact	30
7.5.4 Risk evaluation	30
7.5.5 Compliance analysis	30
7.6 Risk treatment plan	30
7.7 Conclusion and decisions	30
7.8 PIA public summary	30
Annex A (informative) Scale criteria on the level of impact and on the likelihood	32

ISO/IEC 29134:2017(E)

Annex B (informative) Generic threats	34
Annex C (informative) Guidance on the understanding of terms used	38
Annex D (informative) Illustrated examples supporting the PIA process	40
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.

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

- the responsibility for the implementation and/or delivery of the process, information system or programme is shared with other organizations and it should be ensured that each organization properly addresses the identified risks;
- an organization is performing privacy risk management as part of its overall risk management effort while preparing for the implementation or improvement of its ISMS (established in accordance with ISO/IEC 27001 or equivalent management system); or an organization is performing privacy risk management as an independent function;
- an organization (e.g. government) is undertaking an initiative (e.g. a public-private-partnership programme) in which the future PII controller organization is not known yet, with the result that the treatment plan could not get implemented directly and, therefore, this treatment plan should become part of corresponding legislation, regulation or the contract instead;
- the organization wants to act responsible towards the PII principals.

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

Information technology — Security techniques — Guidelines for privacy impact assessment

1 Scope

This document gives guidelines for

- a process on privacy impact assessments, and
- a structure and content of a PIA report.

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

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

2 Normative references

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

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

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

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

3 Terms and definitions

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

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

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

acceptance statement

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

3.2

asset

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

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

ISO/IEC 29134:2017(E)**3.3****assessor**

person who leads and conducts a *privacy impact assessment* ([3.7](#))

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

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

3.4**process**

set of interrelated or interacting activities which transforms inputs into outputs

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

3.5**device**

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

3.6**privacy impact**

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

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

3.7**privacy impact assessment****PIA**

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

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

3.8**privacy risk map**

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

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

3.9**programme**

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

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

3.10**project**

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

[SOURCE: ISO 9000:2015, 3.4.2]

3.11**organization**

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

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

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

3.12**severity**

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

3.13**system****information system**

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

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

3.14**stakeholder**

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

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

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

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

3.15**technology**

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

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

4 Abbreviated terms

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