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

iTeh STANDARD PREVIEW

(standards.iteh.ai)

iTeh STANDARD PREVIEW

(standards.iteh.ai)

Contents   Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC FDIS 29134
https://standards.iteh.ai/catalog/standards/sist/949a3aa4-6890-4ffb-838a-8315b7491cc6/iso-
iec-fdis-29134

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 document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directiveswww.iso.org/directives or www.iec.ch/members_experts/refdocs).

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. 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/patentswww.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation onof 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.htmlwww.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition incorporates cancels and replaces the first edition (ISO/IEC 29134:2017/DAmd 1), which has been technically revised.

The main changes are as follows:

— minor editorial changes have been made.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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~~);

— taking necessary actions, in consultation with stakeholders, ~~for taking actions as necessary in order~~ to treat privacy risk.

A PIA report ~~may~~can 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~~circumstances.

A PII controller ~~may~~can have a responsibility to conduct a PIA and ~~may~~can request a PII processor to assist in doing this, acting on the PII controller's behalf. A PII processor or a supplier ~~may~~can 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~~can be necessary for suppliers of such devices to provide privacy-relevant design information to those undertaking the PIA. ~~When~~It is possible that 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 such circumstances, in order to enable it to undertake minimal PIA activity, the device supplier ~~may~~can 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 regarding PIA can apply.

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 an 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~~cannot be implemented directly and, therefore, <u>it is presupposed that</u> this treatment plan ~~should become~~becomes 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~~can 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~~can be defined by the person responsible for conducting the PIA, independently of any other control set.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC FDIS 29134
https://standards.iteh.ai/catalog/standards/sist/949a3aa4-6890-4ffb-838a-8315b7491cc6/iso-
iec-fdis-29134

Content

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC FDIS 29134
https://standards.iteh.ai/catalog/standards/sist/949a3aa4-6890-4ffb-838a-8315b7491cc6/iso-
iec-fdis-29134

Information technology — Security techniques — Privacy impact assessment — Guidelines

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~~2018, *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~~terminology 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~~https://www.iso.org/obp

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

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

3.2

asset

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

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

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

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

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

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

[SOURCE: ISO/IEC ~~Directives, Part 1, Consolidated ISO Supplement:2014~~ 27000:2018, 3.~~12~~54]

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~~can 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~~[SOURCE: ISO/IEC 29100:2011, 2.20~~.~~, modified — Note 1 to entry has been deleted.]

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 27000:2018, 3.0150]

3.12
severity

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

3.13
system
information system

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

[SOURCE: ISO/IEC 27000:2016, 2.39]2018, 3.36, modified — "system" added as a preferred term.]

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 PIIpersonally identifiable information principals, management, regulators and customers.

Note— 2 to entry: Consultation with stakeholders is integral to a PIAprivacy impact assessment.

[SOURCE: ISO*/IEC Directives, Part 1, Consolidated ISO Supplement:*2014 37000:2021, 3.02 3.1, modified — The preferred term "interested party" has— Note 1 and Note 2 to entry have been removed from this entrymodified.]

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

IPMA   International Project Management Association

ISMS   information security management system

PII   personally identifiable information

PRINCE   PRojects IN controlled environments

SME   small and medium-sized enterprises

5 Preparing the grounds for PIA

5.1 Benefits of carrying out a PIA

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

— identifying privacy impacts, privacy risks and responsibilities;

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

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

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

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

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

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

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

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

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

A PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions on privacy issues about the project. A PIA is a tool to undertake the systematic analysis of

privacy issues arising from a project in order to inform decision makers. A PIA can be a credible source of information.

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

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

Trust is built on transparency, and a PIA is a disciplined process that promotes open communications, common understanding and transparency. An organization that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them tothat they do so too. A PIA is a way of educating employees about privacy and making them alert to privacy problems that mightcan damage the organization. It is a way to affirm the organization's values. A PIA can be used as an indication of due diligence and maycan reduce the number of customer audits.

5.2 Objectives of PIA reporting

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

The following are typical examples of stakeholders and their expectations.

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

— Management—: Several viewpoints apply with:

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

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

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

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

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

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

PIA reporting should fulfil two basic functions. The first (Inventoryinventory) keeps the specific stakeholders informed of identified affected entities, affected environment and privacy risks about the life cycle of the affected entities, whether it is inherent or mitigated. The second (Actionaction items) is a