INTERNATIONAL STANDARD

ISO 22307

First edition
2008-05-01

Financial services — Privacy impact assessment

Services financiers — Évaluation de l'impact privé

Reference number
ISO 22307:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

ISO 22307 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 7, *Core banking*.

Introduction

Rapid advances in computer systems and networking allow financial institutions to record, store, and retrieve vast amounts of consumer data with more speed and efficiency than ever before. These advances enable financial services companies to acquire and process consumer data in ways that were previously out of reach to many due to the cost or to the specialized knowledge and training necessary to build and use these technologies. Advanced data processing, storage, collection, and retrieval technology is now available to all sectors of business and government.

Businesses have access to extremely powerful technology with significantly better price and performance than in the past. With these new abilities, businesses can effortlessly process information in ways that, intentionally or unintentionally, impinge on the privacy rights of their customers and partners. These capabilities raise concerns about the privacy of individuals in these large networked information technology environments. Furthermore, regulated industries such as financial services, law, and policy now place additional conditions on how personal information is collected, stored, shared and used.

The financial services community recognizes how important it is to protect and not abuse their customers' privacy, not just because it is required by law, but also because as systems are developed or updated, there is an opportunity to enhance business processes and to provide improved services to customers.

Ensuring compliance with the Organization for Economic Cooperation and Development (OECD) privacy principles means that an institution's privacy policies are consistent with established privacy principles such as having an external body establish a set of rules, guidelines or prohibitions. The presence of an external body can encourage corporations to protect financial information, either simply to comply with the letter of the law, or to enhance their privacy protection in general. New ways of using existing technology and new technologies bring new or unknown risks. It is advisable that corporations handling financial information be proactive in protecting and not abusing the privacy of their consumers and partners.

One way of proactively addressing privacy principles and practices is to follow a standardized privacy impact assessment process for a proposed financial system (PFS), such as the one recommended in this International Standard. A privacy impact assessment (PIA) is a tool that, when used effectively, can identify risks associated with privacy and help organizations plan to mitigate those risks. Recognizing that the framework for privacy protection in each country is different, the internationalization of privacy impact assessments is critical for global banking, in particular for cross-border financial transactions.

Financial services — Privacy impact assessment

1 Scope

This International Standard recognizes that a privacy impact assessment (PIA) is an important financial services and banking management tool to be used within an organization, or by “contracted” third parties, to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems. This International Standard

— describes the privacy impact assessment activity in general,

— defines the common and required components of a privacy impact assessment, regardless of business systems affecting financial institutions, and

— provides informative guidance to educate the reader on privacy impact assessments.

A privacy compliance audit differs from a privacy impact assessment in that the compliance audit determines an institution’s current level of compliance with the law and identifies steps to avoid future non-compliance with the law. While there are similarities between privacy impact assessments and privacy compliance audits in that they use some of the same skills and that they are tools used to avoid breaches of privacy, the primary concern of a compliance audit is simply to meet the requirements of the law, whereas a privacy impact assessment is intended to investigate further in order to identify ways to safeguard privacy optimally.

This International Standard recognizes that the choices of financial and banking system development and risk management procedures are business decisions and, as such, the business decision makers need to be informed in order to be able to make informed decisions for their financial institutions. This International Standard provides a privacy impact assessment structure (common PIA components, definitions and informative annexes) for institutions handling financial information that wish to use a privacy impact assessment as a tool to plan for, and manage, privacy issues within business systems that they consider to be vulnerable.

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.

OECD *Guidelines on the protection of privacy and transborder flows of personal data*, 1980

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
financial activities
activities including

— lending, exchanging, transferring, investing for others, or safeguarding money or securities,

— insuring, guaranteeing or indemnifying against loss, harm, damage, illness, disability or death,

— providing financial investment or economic advisory services,

— underwriting or dealing with securities

3.2
financial system
all services, facilities, business processes and data flows used by financial institutions to implement and perform financial activities

3.3
proposed financial system
all of the components of a financial system assessed in a privacy impact assessment

3.4
business process
process with clearly defined deliverable or outcome, which entails the execution of a sequence of one or more process steps

NOTE A business process is defined by the business event that triggers the process, the inputs and outputs, all the operational steps required to produce the output, the sequential relationship between the process steps, the business decisions that are part of the event response, and the flow of material and/or information between process steps.

3.5
data model
representation of the specific information requirements of a business area

3.6
information access model
model that depicts access to key process and organization information for reporting and/or security purposes

NOTE An information flow model is a model that visually depicts information flows in the business between business functions, business organizations, and applications.

3.7
preliminary privacy impact assessment
assessment conducted when the proposed financial system is at the early conception or design phase and detailed information is not known

NOTE A preliminary privacy impact assessment can be planned for a proposed financial system in defining the need and/or scope of a full privacy impact assessment for a proposed financial system.

4 Abbreviated terms

CPO Chief Privacy Officer

NPI Non-public Personal Information

OECD Organization for Economic Cooperation and Development

PIA Privacy Impact Assessment

PII Personally Identifiable Information

PFS Proposed Financial System

5 PIA requirements

5.1 Overview of PIA requirements

The objectives of a PIA include:

— ensuring that privacy protection is a core consideration in the initial considerations of a PFS and in all subsequent activities during the system development life cycle;

— ensuring that accountability for privacy issues is clearly incorporated into the responsibilities of respective system developers, administrators and any other participants, including those from other institutions, jurisdictions and sectors;

— providing decision-makers with the information necessary to make fully-informed policy, system design and procurement decisions for proposed financial systems based on an understanding of the privacy implications and risks and the options available for avoiding and/or mitigating those risks;

— reducing the risk of having to terminate or substantially modify a financial service after its implementation to comply with privacy requirements;

— providing documentation on the business processes and flow of personal information for use and review by departmental and agency staff and to serve as the basis for consultations with clients, the privacy officers and other stakeholders.

To meet these objectives, PIAs have common process elements that shall be followed to be effective. The following are minimum process requirements for a PIA which addresses the impacts of a PFS.

5.2 General PIA process requirements

The following are the six common elements that are required of any PIA process:

— PIA plan;

— assessment;

— PIA report;

— competent expertise;

— degree of independence and public aspects;

— use in the PFS decision-making.

More specific requirements of the PIA plan, PIA assessment and the PIA report are addressed in 5.3.

5.3 Specific PIA process requirements

5.3.1 PIA plan

5.3.1.1 Scope of PIA plan

The PIA process requires a plan with a scope. This scope shall guide the PIA process for a specific PFS by stating:

— the business objectives of the PFS;

— the privacy policy compliance objectives of the PIA, which, at a minimum, shall be to comply with OECD privacy principles and any financial sector agreements regarding compliance with OECD privacy principles (e.g. international standards addressing financial sector and security);

— whether the PFS is creating a new business system or a proposed change of an existing business system or its supporting system;

— whether the PIA is a preliminary PIA;

— any assumptions and constraints regarding the applicable jurisdiction(s) of the PFS and the consideration of alternative systems to the proposed financial system; the assessment of any alternative shall also be based on documented business objectives and the appropriate management shall approve the business objectives;

— the life-cycle phase of the PFS.

5.3.1.2 Documented report

The PIA process requires a plan resulting in a documented report. The PIA plan shall systematically establish the steps to be followed, questions to be answered and options to be examined for the PFS being assessed. The steps shall include obtaining the following prior to the assessment:

— a description of the PFS and, if necessary, the description of the existing financial systems relevant to the PFS;

— identification of the competent expertise needed to perform the PIA and to develop the PIA report within the defined scope;

— agreement by the identified competent expertise on the degree of independence built into the process;

— agreement on how the PIA report shall be integrated into decision-making processes for the PFS system development;

— identification of relevant privacy policies, privacy laws and standards for the processing of personal information relevant for the PFS;

— identification of known and relevant risks to personal information associated with the PFS, its business processes and any relevant existing systems.

5.3.1.3 Description of the PFS

The PIA plan shall include the detailed description of the PFS, as defined by the scope. The PFS may be a completely new development or a proposed change to an existing financial system. The description of the PFS shall include:

— documented business objectives of the PFS being assessed and the consideration of alternative systems to the proposed financial system; the appropriate management shall approve the business objectives;

— how a PFS shall use and process personal information;

— whether the PFS is intended to add to or modify the existing financial system described in the scope of the proposal;

— the proposed collection, generation or obtaining of personal information through its holding, storage, security, use and disclosure, using

  — business process and data flow diagrams,

  — data models, and

  — information access models;

— the proposed compliance with applicable privacy policies and mitigations to known privacy risks;

— applicable industry privacy frameworks [e.g. the International Security, Trust and Privacy Alliance (ISTPA) privacy framework] that guide the design of the system;

— the applicable security programme and its compliance with industry security standards (e.g. ISO 17799);

— use of supporting infrastructure to process personal information including (but not be limited to)

  — telecommunications,

  — helpdesk operations,

  — use or reuse of common services shared both within jurisdictions and across jurisdictions.

The business process and data flow diagrams shall identify how information flows through the organization as a result of a particular business activity or activities. At a minimum, the diagrams should identify, on a general level, the major components of the business processes and how personal information is collected, used, disclosed and retained through this process.

For architectural descriptions that map business processes and technical support mechanisms to support data protection policies and fair information practices, the ISTPA privacy framework should be considered. The purpose of the framework is to provide an analytical starting point and basis for developing products and services that support current and evolving privacy regulations and business policies, both international and domestic.

For architectural descriptions of software-intensive systems, use of IEEE 1471:2000 should be considered.

5.3.1.4 Relevant privacy policies and standards applicable to the PFS

The PIA plan shall include the privacy policies and standards applicable to the PFS for compliance purposes. These shall include (but not be limited to)

— the OECD *guidelines on the protection of privacy and transborder flows of personal data,*

— privacy policies, laws, regulations or any other directives that apply uniquely to the international financial community, or agreed-to-be-contractual relationships,

— security standards that apply uniquely to the financial sector.

5.3.1.5 Known privacy compliance risks to personal information for the PFS

The identification of known and relevant risks to personal information is required. There may be risks to personal information other than those addressed by privacy laws and regulations. These include identity theft and pretexting. Identifying all known and relevant risks to personal information shall precede any study or research, examination of alternatives to the proposed financial system and the rendering of conclusions and recommendations.

If the competent expertise participating in the PIA agrees that there are no known risks to personal information identified in association with the PFS, the PIA report may briefly conclude this position.

5.3.1.6 Objectives of the PFS

The PIA plan shall include the documented business objectives of the PFS being assessed, as well as considerations of alternative systems to the PFS. The assessment of any alternative shall also take into account documented business objectives. The appropriate management shall approve the business objectives.

5.3.2 PIA assessment

Within the defined scope of the PIA, the minimum requirements for PIA assessment for a PFS are as follows:

— assessment shall be performed within the scope defined by the PIA plan;

— assessment shall be performed using the competent expertise identified in the PIA plan;

— business process and data flow analysis shall be performed of the personal information used by the system(s);

— privacy policy compliance gap analyses shall be performed;

— infrastructure support impact analysis shall be performed;

— security programme impact analysis shall be performed;

— findings and recommendations shall be determined for the PIA report.

Annexes A to F provide questionnaires with relevant questions to assist in the assessment. However, these questionnaires are simply a starting point, and a complete or appropriate list should be devised with reference to the relevant international and national standards and the features of the technology or PFS.

5.3.3 PIA report

The financial institution can tailor the format of the PIA report. However, the PIA report shall consist, at a minimum, of the following:

— the scope of the PIA for the specific PFS;

— the summary description of the PFS and any existing business systems;

— the competent expertise that performed the PIA and developed the PIA report;

— the degree of independence built into the PIA process;

— the decision-making processes for the PFS system development, based on the PIA report;

— the relevant privacy policies, privacy laws and standards for the processing of personal information relevant for the PFS;

— assessment findings as to the privacy risks of a PFS to complying with relevant privacy policies and laws, the significance of those risks to complying with privacy regulations and meeting business objectives, and any other risks to personal information discovered during the assessment;

— recommended alternatives to mitigate the risks and achieve the stated business objectives of the PFS; and

— identification of the executive who is the recipient of the PIA report and responsible for acting on findings and recommendations.

5.3.4 Competent expertise

The PIA process for a PFS and its services shall require competent expertise as directed by the financial institution. Competent expertise shall be required throughout the PIA process, including the development of the PIA plan, the performance of the PIA assessment and the development of recommendations in the PIA report.