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.

The PIA plan shall identify the competent expertise needed to perform the PIA. The competent expertise shall at a minimum include:

— legal expertise familiar with all relevant financial community privacy-related laws, policies and international privacy principles (e.g. OECD);

— financial systems expertise familiar with the PFS and, if applicable, all relevant existing systems and their supporting infrastructures;

— business process, transaction and data flow expertise of the PFS and any other relevant business systems.

Annex A provides guidance on achieving a level of competent expertise for PIAs. The variety of skills required may not be possessed by one individual, so a PIA coordinator may draw on the skills of others. The coordinator may be a generalist. However, experts hired for the process should not be expected to handle areas with which they are not familiar, for example, it would not be appropriate for an external lawyer to deal with technical issues, nor for a technologist to explain the law.

5.3.5 Degree of independence and public aspects

The PIA process shall have a degree of independence built into it, as determined by the financial service. This process shall include an editing process for the PIA report which protects the security of the financial services institution and its customers. An example of independence and public aspects includes making the PIA reports available to supervision by independent auditors and government-directed financial services regulatory compliance authorities. Annex A provides guidance on achieving a level of independence for a PIA.

Annex A
(informative)

Frequently asked questions related to PIA

A.1 General

The two sets of frequently asked questions (FAQs) contained in this annex are intended to encourage the use of PIAs and this International Standard. These FAQs are informative: users are encouraged to tailor these FAQs such that they are aligned with the privacy programmes and policies associated with implementing this International Standard.

A.2 FAQs about PIAs

A.2.1 What is a PIA?

The PIA is a vehicle for addressing privacy issues in a system under development. To be effective, a PIA needs to be conducted as part of a formalized process. The PIA provides a way to ensure that a proposed new system under development complies with applicable laws and regulations governing customer and consumer privacy.

All PIA processes have the following six elements in common:

— PIA plan;

— assessment;

— PIA report;

— competent expertise;

— degree of independence and public aspects;

— use in PFS decision-making.

A.2.2 What is the difference between a PIA and a privacy compliance audit?

A privacy compliance audit differs from a PIA, in that the compliance audit tries to determine a particular business system's current level of compliance with the law and identify steps to avoid non-compliance with the law in the future. While there are similarities between PIAs and privacy compliance audits, in that they use some of the same skills and seek to avoid privacy breaches, compliance audits are primarily directed towards existing systems in order to validate their compliance with required policies, standards and law. By contrast, a PIA is used at an early stage in the development of a PFS and is useful in identifying optimum privacy options and solutions. If a PFS introduces a change to an existing system, the most recent privacy compliance audit provides very useful information for assessing the impact of the PFS.

A.2.3 When is a PIA a useful tool to ensure data protection?

A PIA is useful in the following situations:

— to determine whether or not the proposed system development complies with applicable laws and regulations governing customer and consumer privacy;

— to develop part of a data protection strategy; while a data protection strategy includes sensitive information that is not personally identifiable information, consideration of risks to personal information requires specific attention, of which privacy policy compliance is just one area;

— to ensure that privacy policy compliance risks associated with the proposed use of new technology, or with the new application of existing technologies, are mitigated.

A.2.4 My system changes frequently: do I need to repeat a PIA for each system change, or can I perform a PIA simply to address the new changes?

Depending on the scope of the changes and the adopted system development life-cycle practices, the PIA may be limited in scope. If there are no known risks associated with the proposed changes, the PIA process may be reported as concluded. If it is not certain that there are privacy issues, the PIA process can be performed within the scope of the proposed changes.

A.2.5 What are the potential consequences of invading the privacy of my current and future clients?

The competent legal and privacy expert required for a PIA will be able to answer this question, including its impact for business systems, especially in cross-jurisdiction transactions.

A.2.6 What are some of the problems that may be identified by performing the PIA process?

The following are examples of problems that may be identified by performing the PIA process:

— unintended instances of personal information used in a manner that creates privacy policy compliance risks;

— misunderstandings of privacy compliance requirements;

— misunderstandings of strategic business plans and technology directions that are, or have the potential to become, privacy policy compliance risks.

A.2.7 How can a PIA help when a “privacy crisis” erupts for my business?

A PIA can help in the following ways:

— by providing an authoritative document of system privacy compliance and actions planned to mitigate compliance risks;

— by providing a record that management exercised due diligence.

A.2.8 What are the benefits of the PIA process?

The PIA process provides the following benefits:

— it obliges project planners to articulate the scope of the project in precise terms;

— privacy is considered at the front end of a project, so that privacy issues are known and can be addressed early in the project planning process;

— it provides an opportunity to communicate and discuss, and to increase the awareness of the various privacy policies and their compliance requirements;

— it enhances privacy programme planning and results in better policy compliance;

— it provides a disciplined approach for identifying and mitigating privacy risks, resulting in better information management practices;

— it is an excellent way to learn about privacy and privacy policy compliance;

— some departments have reported a better understanding of the relationship between compliance and both existing and strategic planning.

A.2.9 What are some of the PIA implementation strategies?

PIA implementation strategies are the overall steps taken to communicate and put into action the PIA process. The following are considered to be best practices:

— facilitate buy-in, establish a senior management committee to make decisions on the need for a PIA and who will review all PIA reports;

— develop an internal policy to integrate the PIA process requirements with other information management policy requirements;

— develop an implementation plan as a guide for the implementation of the PIA process and guidelines;

— develop a privacy process advisory committee to provide advice on the PIA implementation plan;

— ensure that all of the stakeholders are at the table at the start of the planning process;

— develop a workflow on the PIA process to act as a roadmap for users;

— develop a short template to help managers decide whether or not a PIA is required;

— appoint a senior executive to champion the implementation of the PIA process;

— develop and maintain organizational policies that address business processes, especially those that go across jurisdictions, including both sector and national boundaries;

— apply appropriate system development and life-cycle methodologies, architecture standards and industry privacy frameworks.

A.2.10 What are some of the PIA implementation challenges?

The following are examples of challenges to be faced in the course of PIA implementation:

— the breadth of the PIA process presents a challenge because it encompasses not only information technology projects, but also regulation compliance;

— managers need a one-stop shop for advice on interrelated compliance requirements, particularly cross-jurisdiction privacy policies and their compliance with OECD privacy principles;

— senior management has to actively participate in the implementation process;

— all departments need to define their roles and responsibilities in the PIA process clearly;

— the performance of the PIA process should be part of the detailed project plan;

— it is difficult to find skilled resources either internally or externally to conduct PIAs.

A.2.11 How does one prepare for a PIA?

Preparation for a PIA involves the following:

— creating or revising a repeatable process that involves the capturing and sharing of lessons learned;

— discussing the PIA process with staff in other departments who have completed PIA reports so as to gain insight from their experience;

— reviewing previously completed PIA reports obtained from the privacy office so as to gain insight into the expectations for a completed report;

— reusing documentation: the privacy office can be provided with much of the same documentation as that used by the departmental team involved in the PIA process;

— compiling the documentation in one place as the PIA process unfolds;

— organizing a kick-off meeting for the PIA team and explaining the PIA process as an introduction to the project;

— defining the scope at an early stage of the PIA process;

— focussing on the identification of privacy risks and strategies in order to manage or eliminate the risks;

— developing a checklist of potential background documentation to review as part of the PIA process;

— timing the project appropriately: this is important because it may be difficult to retrofit privacy into the project late in the planning cycle;

— establishing document data flows: without clearly documented data flows, it is difficult to identify privacy risks;

— ensuring that there is a sign-off if it is decided that a PIA will not be completed.

A.2.12 How can a corporate privacy officer (CPO) use PIA?

The CPO should review all PIA reports and offer comment on the privacy risks and mitigation measures. The CPO should be involved early in the PIA process so as to understand the overall nature of the PFS and discuss expectations. The CPO should expect, where appropriate:

— a clear description of the scope of the PIA for a PFS and the subjects to be covered in it;

— a clear and comprehensive description of all the actions to be pursued under the initiative involved;

— the architectural specifications of the PFS;

— the threat and risk assessment report pertaining to the PFS;

— a copy of whatever applicable privacy regulations are used;

— samples of third-party contracts, including contracts for the employment of persons hired to input data into the system, so as to ascertain whether they include appropriate privacy protection clauses;

— an explanation of the consent regime involved, with respect to the personal information involved with the initiative;

— copies of all rules and guidelines that have been prepared regarding the collection, use and disclosure of personal information for purposes of the PFS;

— a description of the procedures to follow with respect to complaints regarding the initiative and the supervisory body designated to receive these complaints; and

— copies of all forms and public education materials that have been created which deal with notification requirements.

A.3 FAQs about this International Standard

A.3.1 Can I use this International Standard for both a PIA and a privacy compliance audit?

While different, the collected information that describes the use of personal information is common to both. It would be appropriate to claim that a PIA was conducted in compliance with this International Standard, but it would be inappropriate to claim that a compliance audit was conducted in compliance with this International Standard.

However, if the privacy compliance audit included a report, the report could serve as the starting point for a PIA of the next proposed change to the systems. In addition, the informative annexes of this International Standard may assist in preparing for a compliance audit. Consequently, it could be appropriate for a compliance audit to apply the report structure and the annexes of this International Standard when conducting the audit.

A.3.2 What constitutes competent expertise?

Competent expertise includes the following:

— knowledge of the specific PFS and its business objectives, the PFS design and the system development life-cycle methodologies applied by the financial services institution;

— knowledge of the privacy policies and compliance requirements relevant to the PFS, including legal expertise to provide advice and recommendations with respect to privacy and financial service authorities, institutional supervisory mechanisms and potential conflicts where multiple statutes or jurisdictions are involved;

— operational programme and business design skills to examine proposals in terms of business flow and context, stakeholder analysis, public/private partnerships, governance structures and feasibility in terms of mitigation strategies;

— knowledge of technologies and alternatives to be applied by the PFS, including technology and systems expertise to provide technical and systems advice on mainframe and legacy systems, Internet tools and system interfaces, information, security, technical architecture and data flows;

— information and record-keeping skills, in order to provide advice on how records are kept and the retention of information.

A.3.3 What is meant by a degree of independence and public aspects?

The degree of independence should be balanced against corporate needs in order to protect trade secrets, and it could include:

— access by a public supervisory body (e.g. government regulators);

— public availability of edited versions;

— inclusion of public.

A.3.4 How could a PIA be used in a PFS decision?

A PIA could be used in the following ways:

— the report needs to include present recommendations including alternatives and

— decisions should be documented and attached to the report.

A.3.5 How can I use this International Standard to improve my privacy compliance?

Assuming that your organization wants to take a proactive approach to privacy compliance and that it wants to anticipate privacy risks that may exist, but are outside of any current privacy policies, the following is suggested:

— use the whole document, including the annexes, as a framework to tailor internal guidance that is more specific to your business;

— use standards compliance as a basis for third-party sharing of personal information and

— consider establishing an internal PIA policy that refers to this International Standard.

A.3.6 Could your marketing strategy include a reference to the use of PIA standards?

Only to the extent that PIA standards apply, and that aspects of the annexes are used or tailored for use. The benefits of PIA are both internal and external. Allowing for some public disclosure of the PIA should be consistent with notifications.

A.3.7 Can a PIA report be reused?

Current PIA efforts, including existing PIA reports, should be considered in the earliest stages of system development in order to determine what changes are proposed. The resulting PIA may be able to leverage the previous analysis and recommendations. Even though this could reduce the effort required to produce the PIA, it should not be the primary purpose in place of conducting a proper assessment.

A.3.8 What is meant by a PFS?

A PFS involves

— a new financial system consisting of new or changed customer services and business processes,

— new use of existing technology or technologies and infrastructure support systems, particularly those technologies and infrastructure systems that support the business processes involving collection, storage or access to personal information.

A.3.9 How do I use this International Standard as part of my organization?

This International Standard specifies normative process requirements for privacy compliance programmes in order to provide supervision and governance of new financial services developments that minimize privacy compliance risks.

A.3.10 What are the benefits of using this International Standard to articulate process?

The benefits include the following:

— it is agreed to process within an organization;

— agreement is reached with parties with which personal information is shared.

A.3.11 Are there any tips on completing the PIA privacy analysis questionnaires?

The PIA privacy analysis questionnaires are a key component of the PIA process and are used to generate information on potential privacy risks. The following are considered to be best practices:

— the PIA team should go through the questionnaire as a group;

— when going through the questionnaire, it is helpful to explain why the question is being asked;

— after the completion of a number of PIAs, one department found that some of the questions could be filled out in advance.

A.3.12 Are there any tips for completing the PIA report?

The PIA report is a policy-level discussion of a PFS that summarizes the specific privacy implications and risks together with mitigation measures, as appropriate. The following are considered to be best practices:

— defining the scope of the PIA is critical to the process;

— the person conducting the PIA really needs to understand what is being proposed in order to determine the effect on the management of personal information;

— project staff have their own time schedules, and the PIA process timing needs some flexibility in order to support the programme manager's business needs;

— the PIA report has to be managed as a work in progress because there may be a tendency to complete the report and set it aside;

— documentation has to form the basis of the PIA process in order to avoid speculation on what may or may not be involved in the proposed project;

— it is important to involve the entire PIA team during the discussion of the privacy risks and risk management plan;

— treat the executive summary as a stand-alone document that succinctly describes the PFS, the privacy risks and mitigation measures, and that is destined for a non-technical audience;

— at the start of the PIA process, it is useful to document who is accountable for which aspects in the process and the follow-up to the PIA report.

A.3.13 What internal capacity is required for completing PIA reports?

The following internal capacity is required for completing PIA reports:

— use standards to frame organizational specific implementation guides based on normative requirements;

— ensure that required PIA process skills are available and fully involved; if appropriate, use consultants to assist and advise staff on how to complete the PIA process and thereby develop in-house PIA expertise;

— when consultants are used, ensure that internal PIA skills are used at a minimum, in order to assess work that has been completed by consultants;

— ensure management involvement for decisions involving multi-departmental project conducting a PIA.

Annex B
(informative)

General questionnaire to determine when to begin a PIA

The questionnaire in Table B.1 is intended to help the user of this International Standard determine when to begin the PIA process. This questionnaire is informative. The user may wish to add questions as appropriate for the implementation of this International Standard. This questionnaire is intended to provide a starting point to assist the user in determining when to begin a PIA.

Table B.1 — General questionnaire to determine when to begin a PIA

1	Are you: — designing a new financial service or general support service? — making significant changes to an existing financial service? — converting a financial service to an electronic service delivery mode when you have outstanding privacy issues and no PIA?
2	Does the financial service require you to collect, use or disclose any personal information, such as name, address, age, identifying number, educational, medical or employment history?
3	Will the financial service require that you collect, use or disclose more or different personal information or more sensitive personal information than in the past? Are you shifting from informed consent to indirect collection of information?
4	Will it be necessary to develop mechanisms to notify individuals about their privacy rights, or to obtain the consent of individuals to collect, use and/or disclose their personal information?
5	Will the financial service require you to collect personal information from other financial services within your institution, other institutions, or the government?
6	Will the personal information generated by the financial service be used in decision-making processes that directly affect individuals, such as eligibility for financial services?
7	Will the personal information generated by the financial service be used for any other purposes, including research and statistical purposes?
8	Will the personal information be shared with any other organizations for any purposes other than for those for which it was originally collected?
9	Are you introducing new common client identifiers, or are you using them without any legal authority?
10	Do you anticipate that the public will have any privacy concerns regarding the proposed financial service?
11	Are you introducing changes to the business systems or infrastructure architecture that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information?

Annex C
(informative)

Questionnaire for PIA objectives

The questionnaire in Table C.1 is intended to assist the user of this International Standard when preparing the PIA plan as required in this International Standard. This questionnaire is informative. The user may wish to add questions as appropriate for the implementation of this International Standard. This questionnaire is intended to provide a starting point to assist the user in developing PIA objectives.

Table C.1 — Questionnaire for PIA objectives

1	Will the PIA assess the impact of the PFS on the quality of a financial institution's compliance management policies and procedures for implementing the privacy regulation, specifically ensuring consistency between what the financial institution tells consumers in its notices about its policies and practices, and what it actually does?
2	Will the PIA determine the impact of the PFS on the reliance that can be placed on a financial institution's internal controls and procedures for monitoring the institution's compliance with the privacy regulation?
3	Will the PIA determine the impact of the PFS on the financial institution's compliance with the privacy regulation, specifically in meeting the following requirements: — giving customers notices of its privacy policies and practices that are timely, accurate, clear and conspicuous, and that are delivered in such a way that each customer can reasonably be expected to receive actual notice? — disclosing NPI to non-affiliated third parties, other than under an exception, after first meeting the applicable requirements for giving consumers notice and the right to opt out/opt in? — appropriately honouring consumer opt-out directions? — lawfully using or disclosing NPI received from a non-affiliated financial institution? — disclosing account numbers only in accordance with the limits in the regulations?
4	Will the PIA identify the corrective actions of the PFS when potential violations of law are identified, or when policies or internal controls are deficient for the PFS?

Annex D
(informative)

Questionnaire on PIA initial procedures

The questionnaire in Table D.1 is intended to assist the user of this International Standard when preparing the PIA plan as required by this International Standard. This questionnaire is informative. The user may wish to add questions as appropriate for the implementation of this International Standard. This questionnaire is intended to provide a starting point to assist the user with PIA initial procedures.

Table D.1 — Questionnaire on PIA initial procedures

1	Have you identified the institution's information-sharing practices with affiliates and non-affiliated third parties, its treatment of NPI and its administration of opt-outs? Have the following been considered, as appropriate: — notices (initial, annual, revised, opt-out, short-form, and simplified)? — institutional privacy policies and procedures, including those to: — process requests for NPI, including requests for aggregated data; deliver notices to consumers? — manage consumer opt-out directions (e.g. designating files, allowing a reasonable time to opt out/opt in, providing new opt-out/opt-in and privacy notices when necessary, receiving opt-out/opt-in directions, handling joint account holders)? — prevent the unlawful disclosure and use of the information received from non-affiliated financial institutions? — prevent the unlawful disclosure of account numbers?
2	Have you acquired information-sharing agreements between the institution and affiliates, and service agreements or contracts between the institution and non-affiliated third parties, either to obtain or provide information or services?
3	Have you acquired the complaint logs, telemarketing scripts and any other information obtained from non-affiliated third parties? NOTE Review telemarketing scripts to determine whether the contractual terms are met and whether the institution is disclosing account number information in violation of any relevant privacy policies or law.
4	Have you acquired the categories of NPI collected from or about consumers in obtaining a financial product or service (e.g. in the application process for deposit, loan or investment products; for an over-the-counter purchase of a bank check; from e-banking products or services, including the data collected electronically through Internet cookies; or through ATM transactions)?
5	Have you acquired categories of NPI shared with, or received from, each non-affiliated third party?
6	Have you acquired consumer complaints regarding the treatment of NPI, including those received electronically?

Annex E
(informative)

Questionnaire on the adequacy of internal controls and procedures

The questionnaire in Table E.1 is intended to help the user of this International Standard meet the PIA plan requirement by collecting important information that describes the PFS that will be the subject of the PIA. This questionnaire is informative. The user may wish to add questions as appropriate for the implementation of this International Standard. This questionnaire is intended to provide a starting point to assist the user in determining the adequacy of internal controls procedures.

When determining the impact of the PFS on the adequacy of the financial institution's internal controls and procedures in order to ensure compliance with the privacy regulation as applicable, consider the following questionnaire in light of a new PFS.

Table E.1 — Questionnaire on the adequacy of internal controls and procedures

1	Does the PFS address the sufficiency of internal policies, procedures and controls, including the review of new products, services and controls over servicing arrangements and marketing arrangements?
2	Does the PFS address the effectiveness of management information systems, including the use of technology for monitoring, exception reports and standardization of forms and procedures?
3	Does the PFS address the frequency and effectiveness of current monitoring procedures?
4	Does the PFS address the adequacy and regularity of the institution's privacy training programme?
5	Does the PFS address the suitability of the institution's compliance audit programme for ensuring that: — the procedures address all applicable regulatory provisions? — the work is accurate and comprehensive with respect to the institution's information-sharing practices? — the appropriateness of audit compliance frequency? — conclusions from the compliance audit programme will be appropriately reached and presented to responsible parties? — steps will be taken to correct deficiencies and to follow up on previously identified deficiencies?
6	Does the PFS consider the knowledge level of management and personnel to support new PFS?

Annex F
(informative)

PIA questionnaire for assessing privacy impacts for retail financial systems

F.1 General

The questionnaire in Table F.1 is intended to assist the user of this International Standard when preparing for the PIA analysis requirement of this International Standard. This questionnaire is informative. The user may wish to add questions as appropriate for the implementation of this International Standard. This questionnaire is intended to provide a general set of questions to assist the user in assessing the privacy impacts of proposed financial systems.

F.2 Basic areas of PIA for a financial institution

Does the PFS impact the requirement for and implementation of the following:

— initial privacy notices;

— annual privacy notices;

— content of privacy notices;

— opt-out/opt-in policies or notices;

— revised notices;

— delivery methods;

— limits of disclosure to non-affiliated third parties;

— limits on redisclosure and reuse of information;

— exceptions to opt-out/opt-in requirements for service providers and joint marketing;

— exceptions to notice and opt-out/opt-in requirements for processing and servicing transactions;

— other exceptions to notice and opt-out/opt-in requirements.

Table F.1 — PIA questionnaire for assessing privacy impacts for retail financial systems

Initial privacy notice	
1	Does the PFS impact the institution's ability to provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all customers not later than when the customer relationship is established?
2	Does the PFS impact the institution's ability to provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all consumers who are not customers before any NPI about the consumer is disclosed to a non-affiliated third party, other than under an established exception?
3	Does the PFS impact the institution's ability to provide to existing customers who obtain a new financial product or service an initial privacy notice that covers the customer's new financial product or service, if the most recent notice provided to the customer was not accurate with respect to the new financial product or service?
4	Does the PFS impact the institution's ability to provide initial notice after establishing a customer relationship only a) if the customer relationship is not established at the customer's election, or b) if to do otherwise would substantially delay the customer's transaction (e.g. in the case of a telephone application) and the customer agrees to the subsequent delivery?
5	When the subsequent delivery of a privacy notice is permitted, does PFS impact the institution's ability to provide notice after establishing a customer relationship within a reasonable time?
Annual privacy notice	
6	Does the PFS impact the institution's ability to provide a clear and conspicuous notice that accurately reflects its privacy policies and practices at least annually, or in compliance with applicable privacy policies, throughout the customer relationship?
7	Does the PFS impact the institution's ability to provide an annual privacy notice to each customer whose loan the institution owns the right to service?
Content of privacy notices	
8	Does the PFS impact the institution's initial, annual and revised privacy notices, including each of the following, as applicable: a) the categories of NPI that the institution collects? b) the categories of NPI that the institution discloses? c) the categories of affiliates and non-affiliated third parties to whom the institution discloses NPI, other than parties to whom information is disclosed under an established exception? d) the categories of NPI disclosed about former customers, and the categories of affiliates and non-affiliated third parties to whom the institution discloses that information, other than those parties to whom the institution discloses information under an established exception? e) if the PFS impacts the institution's ability to disclose NPI to a non-affiliated third party, a separate statement of the categories of information the institution discloses and the categories of third parties with whom the institution has contracted? f) an explanation of the opt-out/opt-in right, including the method(s) of opt-out/opt-in? g) any disclosures that the institution makes? h) the PFS impact on the institution's policies and practices with respect to protecting the confidentiality and security of NPI? i) a general statement (with no specific reference to the exceptions or to the third parties) that the institution makes disclosures to other non-affiliated third parties, as permitted by law?

Table F.1 (*continued*)

9	If an institution collects NPI in any of the following categories, does the PFS impact the institution's list of categories of information: a) from the consumer? b) about the consumer's transactions with the institution or its affiliates? c) about the consumer's transactions with non-affiliated third parties? d) from a consumer reporting organization?
10	If an institution collects NPI in any of the following categories, does the PFS impact the institutions whose category of information it lists, or if it does not list the categories it collects and give examples, does the PFS impact any statements that the institution reserves the right to disclose all the NPI that it collects: a) from the consumer? b) about the consumer's transactions with the institution or its affiliates? c) about the consumer's transactions with non-affiliated third parties? d) from a consumer reporting organization?
11	Does the PFS impact the institution's list of the following categories of affiliates and non-affiliated third parties to whom it discloses information, as applicable, while providing a few specific examples of the third parties in each category: a) financial service providers? b) non-financial companies? c) others?
12	Does the PFS impact the institution's ability to make the following disclosures regarding service providers and joint marketers to whom it discloses NPI: a) as applicable, the same categories and examples of NPI [see questions 8 b) and 10]? b) that the third party is a service provider that performs marketing on the institution's behalf, or on behalf of the institution and another financial institution? c) that the third party is a financial institution with which the institution has a joint marketing agreement?
13	If the institution does not disclose NPI, and does not reserve the right to do so, does the PFS impact the institution's ability to provide a simplified privacy notice that contains at a minimum: a) a statement to this effect? b) the categories of NPI it collects? c) the policies and practices the institution uses to protect the confidentiality and security of NPI? d) a general statement that the institution makes disclosures to other non-affiliated third parties, as permitted by law?
14	Does the PFS impact the institution's ability to describe the following about its policies and practices with respect to protecting the confidentiality and security of NPI: a) who is authorized to have access to the information? b) whether security practices and policies are in place to ensure the confidentiality of the information in accordance with the institution's policy?