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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

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,

