American National Standard for Financial Services

X9.99-2009
Identical to
ISO 22307-2008

Financial services — Privacy impact assessment

Accredited Standards Committee X9, Incorporated

Financial Industry Standards

Date Approved: August 17, 2009

American National Standards Institute

Contents

Page

Foreword

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretation should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by:

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
1212 West Street, Suite 200
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

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