American National Standard for Financial Services

X9.99–2004

Privacy Impact Assessment Standard

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: September 2, 2004

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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
P.O. Box 4035
Annapolis, MD 21403 USA

X9 Online http://www.x9.org

Introduction

NOTE Compliance with this standard may require use of an invention covered by patent rights.

By publishing this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

Rapid advances in computer systems and networking allow institutions to record, store, and retrieve vast amounts of consumer data with more speed and efficiency than ever before. These advances enable businesses to acquire and process consumer data in ways that were previously out of reach to many businesses 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/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.

Privacy means an individual's interest in limiting who has access and/or can use their personal information. The public is concerned that corporations that offer financial services and use highly integrated information systems will encroach on their privacy rights. The Federal Trade Commission (FTC) has established Fair Information Practices related to corporate use and management of consumer information. The five principles of Fair Information Practices are: access, consent, enforcement, notice and security. Furthermore, criminals find these increasingly massive, complex, interconnected systems attractive targets. As a result, there has been a significant increase in identity-related fraud. To ensure the safety of personal financial data and to maintain the public's trust, institutions must commit to a proactive and aggressive approach to protect and not abuse individual's privacy.

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.

There are many ways to ensure that an institution's privacy policies are consistent with fair information practices, such as having an external body establish a set of rules, guidelines, or prohibitions. The presence of an external body may encourage corporations to protect financial information, either to simply 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. Corporations handling financial information should be proactive in protecting and not abusing the privacy of their consumers and partners.

One way of addressing privacy and fair information practices proactively is to follow a privacy impact assessment process, such as the one recommended in this standard. A privacy impact assessment (PIA) is a tool that, when used effectively, can identify risks and help organizations plan to mitigate those risks. A privacy impact assessment may be conducted multiple times during the life cycle of an information system.

Privacy issues, as with many risk issues, are best managed when systems are being developed, when issues are cheaper and easier to remedy. Thus, privacy protection and fair information practices must be integrated into

these systems during the development life cycle. As the system changes, a privacy impact assessment can ensure that the privacy risks associated with the system changes are addressed and mitigated as the system matures. Additionally, the PIA process also can provide assurance that a system complies with applicable laws and regulations governing customer and consumer privacy.

A PIA process will identify risks associated with:

- a new technology or the convergence of existing technologies (for instance, electronic road pricing, caller ID, and smart cards);
- the consolidation of business systems and databases that are ultimately used to service customer transactions
- known privacy-intrusive technology that will be used in new ways (for instance, expanding data matching or drug testing or installing more video surveillance cameras in public places);
- identity theft, pretexting, and misuse of information for denial of service;
- unauthorized disclosure of nonpublic personal information to nonaffiliated third parties;
- a major endeavor or change in practice that may have significant effects on privacy; and will identify strategies to minimize those risks.

This Privacy Impact Assessment Standard provides common requirements for the PIA Process and a number of Informative Annexes in support of common privacy impact assessment (PIA) process to help corporations that handle financial information to identify applicable privacy enhancing technologies for use with or in their systems and to consider the risks, costs, and benefits of using these technologies versus using other technologies or using none at all.

In many cases, a privacy impact assessment report that accompanies a PIA can allay privacy risk concerns associated with business systems. The reports will also assist in other endeavors that propose to use the same business systems (or a variant). In later years, this PIA report may also be used to re-evaluate the proposed financial system (PFS) and to ensure that the design and operation of the business system remains within the original guidelines intended to protect consumer privacy.

A high quality PIA can significantly help to protect privacy. However, a PIA is most beneficial when the process is undertaken by competent and credible people and the process itself demonstrates integrity throughout. This involves a systematic process carried out by a team with knowledge of the particular business system(s), and its objectives, technologies, and compliance requirements.

A PIA is not a substitute for the legal protection of privacy and the granting to individuals of enforceable entitlements. The process should fit with whatever policy or process method a control has. If there is a data protection or privacy law in place, the PIA will help to ensure that:

- individual entitlements are not undermined
- agencies are helped to comply with the law
- regulatory agencies are informed enough to make decisions
- existing and future national identification and authentication initiatives are leveraged to reduce identity theft

Suggestions for the improvement or revision of this standard are welcome. Send suggestions to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, P.O. Box 4035, Annapolis, Maryland, 21403, USA.

This standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval.

The X9 committee had the following members:

Gene Kathol, X9 Chairman

Vincent DeSantis, X9 Vice Chairman

Cynthia Fuller, Executive Director

Isabel Bailey, Managing Director

ORGANIZATION	REPRESENTATIVE
ACI Worldwide	Jim Shaffer
American Express Company	Mike Jones
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Bank One Corporation	Jacqueline Pagan
BB and T	Woody Tyner
Citigroup, Inc.	Daniel Schutzer
Deluxe Corporation	John Fitzpatrick
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Jon Mills
eFunds Corporation	Cory Surges
Federal Reserve Bank	Dexter Holt
First Data Corporation	Gene Kathol
Fiserv	Bud Beattie
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
Ingenico	John Sheets
JPMChase Bank	Robert J Blair
KPMG LLP	Alfred Van Ranst Jr.
MagTek, Inc.	Carlos Morales
MasterCard International	William Poletti
Mellon Bank, N.A.	David Taddeo
National Association of Convenience Stores	John Hervey
National Security Agency	Sheila Brand
NCR Corporation	David Norris
NEC Solutions (America)	Michael Versace
Savvis	Kevin M. Nixon
Star Systems, Inc.	Michael Wade
The Clearing House	Vincent DeSantis
Unisys Corporation	David J. Concannon
University Bank	Stephen Ranzini
VeriFone, Inc.	Brad McGuinness

VECTORsgi	Ron Schultz
VISA International	Patricia Greenhalgh
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Ruven Schwartz

Under ASC X9, Inc. procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at the time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F Privacy Impact Assessment working group that developed this standard had the following members:

J. Martin Ferris, Chairman

ORGANIZATION	REPRESENTATIVE
Ferris & Associates, Inc.	J. Martin Ferris
First Data Corporation	Lynn Wheeler
PreVal Specialist, Inc.	Peter C. Sargent
NEC Soultions (America)	Michael Versace
National Security Agency	Sheila Brand
Identrus	Brandon Brown
Diebold, Inc.	Bruce Chapa
Bank of America	Andi Coleman
ACI Worldwide	Fay Fisher
First Data Corporation	Bonnie Howard
Bank of America	Todd Inskeep
Bank of America	Joan S. (Cam) Lambert
Savvis	Shannon Myers
Savvis	Kevin M. Nixon
R Squared Academy Ltd.	Ralph Spencer Poore
TECSEC Incorporated	Pud Reaver
TECSEC Incorporated	Ed Scheidt
NCR Corporation	Steve Stevens

This document does not cancel or replace any other standards documents in whole or in part. This is the first draft of the Privacy Impact Assessment Standard produced by the Privacy Impact Assessment working group.

Privacy Impact Assessment Standard

1 Scope

This standard recognizes that a Privacy Impact Assessment (PIA) is an important management tool that should be used within an organization or by third parties to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems. This PIA Standard scope:

- provides references to educate the reader on privacy topics and financial privacy in particular
- describes the privacy impact assessment activity, in general
- defines the common components of a PIA regardless of business system affecting financial institutions, and
- explains how to improve the quality of business-system specific PIAs

A privacy impact assessment (PIA) is different than a privacy compliance audit. A 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 PIAs 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 to just meet the requirements of the law, whereas a PIA should delve much further to identify ways to optimally safeguard privacy. Note: Some laws (e.g. the Gram Leach Bliley act (GLB) address both financial privacy rules and financial security guidelines. X9.99 addresses the privacy aspects, but does not address the security aspects (e.g. the implementation of an information security program (ISP)).

This standard recognizes that the choices of system development and risk management procedures are business decisions and as such, the business decision makers must be informed in order to make educated decisions for their institutions. This standard provides a privacy impact assessment structure (e.g., common PIA components, definitions, and informative annexes) for institutions that handle financial information who are seeking to use a PIA as a tool to plan for and to manage privacy issues within business systems that they consider to be vulnerable.