ANSI X9/TG-5-1992

Financial Services Technical Publication
Developed By Accredited
Standards Committee
X9 - Financial Services

INFORMATION SECURITY GUIDELINE

Developed by
Accredited Standards Committee
X9 - Financial Services

Information Security for Financial Institutions

Guideline to define common prudent business practices for information security, as well as to suggest an approach for financial institutions to build information security programs appropriate to their size, lines of business and circumstances.

Developed by the
Accredited Standards Committee on Financial Services, X9
operating under the procedures of the
American National Standards Institute

Published by:

Accredited Standards Committee X9, Inc.
P.O. Box 4035
Annapolis, Maryland 21403 USA
Phone: 410-267-7707 or 301-879-7988
Fax: 301-879-5124
Email: Cindy.Fuller@X9.org
Isabel.Bailey@X9.org
X9 Online: http://www.x9.org

Printed in the United States of America

Contents

Contents continued

Contents continued

Contents continued

Contents continued

Contents continued

Foreword

This Industry Guideline is a product of the Accredited Standards Committee X9 Financial Services.

This document represents an effort by the industry to define common prudent business practices for information security, as well as to suggest an approach for financial institutions to build information security programs appropriate to their size, lines of business and circumstances.

This Industry Guideline is the result of a cooperative effort of bankers, vendors and government representatives.

The members of ACS X9 at the time of approval of this document were the following:

Harold G. Deal, Chairman
Jack Kilhefner, Vice Chairman, Administration
Eileen Bell, Vice Chairman, Membership/Marketing
Cynthia L. Fuller, X9 Secretariat

Organization Represented	*Name of Representative*
American Bankers Association	Andy Ernst
American Express Company	Eileen Bell
Applied Communications	Dale Ratliff
Bank of America	John Coombs
Canadian Bankers Association	Tom Anderson
Chase Manhattan Bank	John McKessy
Chemical Bank	Francis J. Keenan
Citicorp	Seymour R. Rosen
Continental Bank, N.A.	Joseph P. O'Toole
CoreStates Bank	Kent Seinfeld
Deluxe Check Printers	James Gallup
Discover Card Services, Inc.	Bill Kabot
Federal Reserve Bank	Michael Garrett
First Interstate Bank of CA	Clarence Collins
IBAA	Viveca Ware
IBM	Dan Sundberg
MasterCard International	Alice Droogan
Mellon Bank, N.A.	David P. Taddeo
National Security Clearing Corp.	Walter Cushman
National Security Agency	Gerard A. Rainville, Jr.
NationsBank	Harold G. Deal
NCR Corporation	A.R. Daniels
New York Clearing House	Vincent DeSantis
NIST	Miles Smid
PNC Financial Corp.	Kenneth Leckey
Sears Technology Services	Lori Eisenstaedt
Union Bank	Joseph Martino
UNISYS Corporation	Karl T. Sammons
U.S. Dept. of Treasury	Martin Ferris
VISA International	Patricia Greenhalgh
Wells Fargo Bank	Jack Kilhefner
XEROX Corporation	Frank Bov

Subcommittee ACS X9F on Data and Information Security, which developed this guideline, had the following members:

Martin Ferris, Chairman

Organization Represented	*Name of Representative*
American Bankers Association	Gregg Broomfield
Applied Communications	David Phillips
Chemical Bank	Joan Reynolds
Cylink	Sherry McMahan
Deluxe Corporation	James Gallup
Federal Reserve Bank	James Berlin
Kirchman Corporation	Blair Rugh
MasterCard International	Jim Hawkins
Mellon Bank, N.A.	Richard D. Swadley
National Security Agency	Gerard A. Rainville, Jr.
NationsBank	Jan Ward
Nat'l Institute of Standards	Miles Smid
Northern Telecom Inc.	Beth Hardison
Racal-Guardata	Samuel Epstein
U.S. Dept. of Treasury	J. Martin Ferris
VISA International	Bill Chen

Working Group ASC X9F2 which developed this guideline, had the following participants:

Gerard A. Rainville Jr., Chairman
Blanche Stolkovich, Secretary

Organization Represented	*Name of Representative*
Bank of America	Lawrence Zeni
Bank of Boston	Albert Belisle
Bank of California	Leslie Chalmers
Barclays Bank	Anthony Baratta
Chase Manhattan Bank	Natalie Dengler
Chemical Bank	Peggy Bruner
Citicorp	Perry Gleason
Data Security Systems	Sanford Sherizen
Fidelity Investments	Eddie Zeitler
Independent Monitoring	Michael Baum
Manufacturers Hanover Trust	Joseph Fadell
	Henry Mandl
MasterCard International	James Hawkins
Minn. Mining & Manufacturing	John Kessler
	Gary Pearson
Northwest Technical Services	Roger Fischer
Roxbury Integrated Systems	Norman Conklin
US Trust	John Milo
Z/B Associates	Glenda Barnes

In addition, the following organizations provided substantial contributions to this document:

American Bankers Association
Board of Governors Federal Reserve System
Deluxe Data Systems
Depository Trust Company
Federal Deposit Insurance Corporation
National Institute of Standards and Technology
National Securities Clearing Corporation
Holy Rosary Credit Union, Rochester, NH
Office of the Controller of the Currency
Risks, Ltd.
Visa International

Information Security Guideline for Financial Institutions

1 Introduction

1.1 Scope and purpose

This document presents an information security program structure together with a guideline which defines accepted prudent business practice. Adoption of this guideline will result in a more uniformly secure banking system. Recognizing that information security demands can vary greatly from institution to institution, or from application to application, flexibility was built into this document. Where appropriate, this document references and is consistent with existing standards.

While many of the controls described in this document represent powerful tools for implementing information security, the ultimate strength of any information security program derives from a diligent work force. Special attention to "human issues" should be part of any information security program.

While financial institutions have many diverse security concerns, this document addresses only information security. Other security issues are discussed only when they are related to information security.

This document focuses on business practices of the financial industry. Care has been taken to balance business concerns against the requirements of sound security practice.

1.2 Application

This document is intended for use by financial institutions of all sizes and types that wish to employ a prudent and commercially reasonable information security program. It is also useful to providers of service to financial institutions.

This document may also serve as a source document for educators and publishers serving the financial industry.

1.3 Note on definitions

This document uses terms familiar to information security practitioners. However, some of these terms, such as audit and risk, may not confer the same meaning to security practitioners and financial experts. A Glossary is included in this document.

2 References

2.1 Standards referenced in text:

Personal Identification Number (PIN) Managment and Security – X9.8

Financial Services Retail Key Management – X9.24

Financial Institution Retail Message Authentication – X9.19

Guideline for *Understanding and Designing Checks* – X9/TG-2

Financial Institution Message Authentication (Wholesale) – X9.9

Financial Institution Key Management (Wholesale) – X9.17

Encryption of Wholesale Financial Messages – X9.23

Financial Institution Sign-On Authentication for Wholesale Financial Transactions – X9.26

2.2 Regulations referenced in text:

Export Administration Regulations, 15 CFR 768–799.

International Trade in Arms Regulations, 22 CFR 120, et seq. Office of the Comptroller of the Currency:

Banking Circular BC 229, subject: Information Security

Banking Circular BC 226, subject: End-User Computing

Banking Circular BC 187, subject: Financial Information on Data Processing Servicers

Banking Circular BC 177, subject: Corporate Contingency Planning

Banking Circular BC 119, subject: "Remote" or "Off-Premise" Backup for Data Processing Files.

Advisory Letter AL 91-4, subject: Unauthorized Access to Customer Accounts.

Fair Credit Reporting Act, Public Law 91–508