

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

This is a preview of "X9 TG-5:1992". [Click here to purchase the full version from the ANSI store.](#)

# 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](mailto:Cindy.Fuller@X9.org)  
[Isabel.Bailey@X9.org](mailto:Isabel.Bailey@X9.org)  
X9 Online: <http://www.x9.org>**

Copyright © 1992 Accredited Standards Committee X9, Inc.  
All rights reserved

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher.

Printed in the United States of America

## Contents

	Page
Foreword . . . . .	vii
1 Introduction . . . . .	1
1.1 Scope and purpose . . . . .	1
1.2 Application . . . . .	1
1.3 Note on definitions . . . . .	1
2 References . . . . .	1
2.1 Standards referenced in text . . . . .	1
2.2 Regulations referenced in text . . . . .	1
2.3 Other documents referenced in text . . . . .	2
3 Executive summary . . . . .	2
4 How to use this document . . . . .	3
5 Requirements . . . . .	4
6 Information security program components . . . . .	4
6.1 General Duties . . . . .	4
6.1.1 Directors . . . . .	4
6.1.2 Chief Executive Officer . . . . .	4
6.1.3 Managers . . . . .	5
6.1.4 Employees, vendors, and contractors should . . . . .	5
6.1.5 Lawyers . . . . .	5
6.1.6 Information Security Officers . . . . .	5
6.1.7 Information Systems Security Administrator . . . . .	6
6.2 Risk acceptance . . . . .	7
6.3 Insurance . . . . .	7
6.4 Audit . . . . .	7
6.5 Regulatory compliance . . . . .	7
6.6 Disaster recovery planning . . . . .	8
6.7 Information security awareness . . . . .	8
6.8 External service providers . . . . .	9
6.9 Cryptographic operations . . . . .	9
6.10 Privacy . . . . .	10
7 Discussion of threats and controls . . . . .	11
Platform Independent	
7.1 Information classification . . . . .	11
7.1.1 Highly sensitive . . . . .	11

## Contents continued

	Page
7.1.2 Sensitive .....	11
7.1.3 Internal.....	11
7.1.4 Public.....	11
7.2 Logical access control.....	12
7.2.1 Identification of users.....	12
7.2.2 Authentication of users .....	12
7.2.3 Limiting sign-on attempts.....	13
7.2.4 Unattended terminals.....	13
7.2.5 Operating system access control.....	13
7.2.6 Warning .....	13
7.3 Audit trails.....	13
7.4 Change controls .....	14
7.4.1 Emergency problems.....	14
7.5 Computers .....	14
7.5.1 Physical protection.....	14
7.5.2 Logical access control .....	15
7.5.3 Change .....	15
7.5.4 Equipment maintenance .....	15
7.5.5 Casual viewing.....	15
7.5.6 Emulation concerns .....	15
7.5.7 Business continuity .....	15
7.5.8 Audit trails .....	15
7.6 Networks.....	15
7.6.1 Network integrity .....	15
7.6.2 Access control .....	16
7.6.3 Dial-in.....	16
7.6.4 Network equipment .....	16
7.6.5 Change .....	16
7.6.6 Connection with other networks.....	16
7.6.7 Network monitoring .....	16
7.6.8 Disclosure during transmission .....	16
7.6.9 Network availability .....	16
7.6.10 Audit trails .....	17

## Contents continued

	Page
7.7	Software . . . . . 17
7.7.1	Applications . . . . . 17
7.7.2	Databases . . . . . 17
7.7.3	Application testing . . . . . 18
7.7.4	Defective software . . . . . 18
7.7.5	Change. . . . . 18
7.7.6	Availability of software code. . . . . 18
7.7.7	Unlicensed software. . . . . 18
7.7.8	Property rights . . . . . 18
7.7.9	Viruses . . . . . 18
7.7.10	Memory resident programs . . . . . 19
7.7.11	Remote control. . . . . 19
7.7.12	Software provided to customers. . . . . 19
7.8	Human factors. . . . . 19
7.8.1	Awareness . . . . . 19
7.8.2	Management . . . . . 20
7.8.3	Unauthorized use of information resources . . . . . 20
7.8.4	Hiring practices . . . . . 20
7.8.5	Ethics policy . . . . . 20
7.8.6	Fraud detection . . . . . 20
7.8.7	Know your employee . . . . . 20
7.8.8	Former employees . . . . . 20
	Platform Dependent
7.9	Voice, telephone and related equipment. . . . . 20
7.9.1	Access to VoiceMail system. . . . . 21
7.9.2	Private Branch Exchange (PBX) . . . . . 21
7.9.3	Spoken word . . . . . 21
7.9.4	Intercept. . . . . 21
7.9.5	Business continuity . . . . . 21
7.9.6	Documentation. . . . . 21
7.9.7	Voice Response Units (VRU). . . . . 22
7.10	Facsimile and image . . . . . 22
7.10.1	Modification . . . . . 22
7.10.2	Misdirection of messages. . . . . 22

## Contents continued

	Page
7.10.3 Disclosure . . . . .	22
7.10.4 Business continuity . . . . .	23
7.10.5 Denial of service . . . . .	23
7.10.6 Retention of documents . . . . .	23
7.11 Electronic Mail . . . . .	23
7.11.1 Authorized users . . . . .	23
7.11.2 Physical protection . . . . .	23
7.11.3 Integrity of transactions . . . . .	23
7.11.4 Disclosure . . . . .	23
7.11.5 Business continuity . . . . .	23
7.11.6 Message retention . . . . .	24
7.11.7 Privacy and E-Mail . . . . .	24
7.12 Paper documents . . . . .	24
7.12.1 Modification . . . . .	24
7.12.2 Viewing . . . . .	24
7.12.3 Storage facilities . . . . .	24
7.12.4 Destruction . . . . .	24
7.12.5 Business continuity . . . . .	24
7.12.6 Preservation of evidence . . . . .	24
7.12.7 Labeling . . . . .	25
7.12.8 Forged documents . . . . .	25
7.12.9 Output distribution schemes . . . . .	25
7.13 Microform and other media storage . . . . .	25
7.13.1 Disclosure . . . . .	25
7.13.2 Destruction . . . . .	25
7.13.3 Business continuity . . . . .	25
7.13.4 Environmental . . . . .	25
7.14 Financial transaction cards . . . . .	25
7.14.1 Physical security . . . . .	26
7.14.2 Insider abuse . . . . .	26
7.14.3 Transportation of PINs . . . . .	26
7.14.4 Personnel . . . . .	26
7.14.5 Audit . . . . .	26
7.14.6 Enforcement . . . . .	26



## Contents continued

	Page
7.14.7 Counterfeit card prevention . . . . .	26
7.15 Automated Teller Machines . . . . .	26
7.15.1 User identification. . . . .	26
7.15.2 Authenticity of information . . . . .	27
7.15.3 Disclosure of information . . . . .	27
7.15.4 Fraud prevention . . . . .	27
7.15.5 Maintenance and service . . . . .	27
7.16 Electronic Fund Transfers . . . . .	27
7.16.1 Unauthorized source . . . . .	27
7.16.2 Unauthorized changes . . . . .	27
7.16.3 Replay of messages. . . . .	27
7.16.4 Record retention. . . . .	28
7.16.5 Legal basis for payments . . . . .	28
7.17 Checks . . . . .	28
8 Sources of further help . . . . .	28
8.1 Financial service institutions . . . . .	28
8.2 Standards . . . . .	29
8.2.1 ASC X9 standards . . . . .	29
8.2.2 Electronic Data Interchange standards . . . . .	29
8.2.3 ANSI/IEEE software standards . . . . .	30
8.2.4 National Institute for Standards and Technology Publications . . . . .	30
8.2.5 Building, fire and electrical codes. . . . .	30
8.3 Federal regulations . . . . .	31
8.3.1 Office of the Comptroller of the Currency. . . . .	31
8.3.2 Federal Reserve System . . . . .	31
8.3.3 Fedwire security guidelines for financial institutions . . . . .	31
8.3.4 Internal Revenue Service. . . . .	31
9 Recommendations for UCC 4A security procedure . . . . .	32
9.1 Recommended security procedure under UCC-4A. . . . .	32
9.2 General . . . . .	32
9.3 Written instructions and payment limits. . . . .	32
9.4 Technical controls . . . . .	32
10 Glossary of terms . . . . .	34

## Contents continued

	Page
<b>Table</b>	
Table 1 — Controls appropriate to each source of payment orders . . . . .	33
<b>Annex</b>	
Annex A — Sample Documents . . . . .	37
A.1 Sample Board of Directors Resolution on Information Security . .	37
A.2 Sample Information Security Policy (High Level) . . . . .	38
A.3 Sample Detailed Standard (Local Area Networks) . . . . .	39
A.4 Sample Employee Awareness Form. . . . .	44
A.5 Sample Sign-on Warning Screen . . . . .	45
A.6 Sample Facsimile Warning . . . . .	46
A.7 Sample Information Security Bulletin . . . . .	47
A.8 Sample Risk Acceptance Form. . . . .	48
Annex B — European Privacy Principles. . . . .	50
B.1 The United Kingdom Data Act 1984, Schedule 1, Data Protection Principles . . . . .	50
<b>Index</b> . . . . .	51

## 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

<i>Organization Represented</i>	<i>Name of Representative</i>
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

<i>Organization Represented</i>	<i>Name of Representative</i>
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

<i>Organization Represented</i>	<i>Name of Representative</i>
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) Management 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 Services

*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