
Banking and related financial services — Information security guidelines

*Banque et services financiers liés aux opérations bancaires — Lignes
directrices pour la sécurité de l'information*



Contents

1 INTRODUCTION	1	6.9 Cryptographic operations	10
2 REFERENCES	1	6.10 Privacy	10
3 EXECUTIVE SUMMARY	1	7 CONTROL OBJECTIVES AND SUGGESTED SOLUTIONS	11
NOTE ON SECOND EDITION	2	7.1 Information classification	12
4 HOW TO USE THIS TECHNICAL REPORT	2	7.2 Logical access control	12
5 ENSURING SECURITY	3	7.2.1 Identification of users	13
6 INFORMATION SECURITY PROGRAM COMPONENTS	4	7.2.2 Authentication of users	13
6.1 General duties	4	7.2.3 Limiting sign-on attempts	14
6.1.1 Directors	4	7.2.4 Unattended terminals	14
6.1.2 Chief Executive Officer	4	7.2.5 Operating system access control features	14
6.1.3 Managers	4	7.2.6 Warning	15
6.1.4 Employees, vendors, and contractors should:	5	7.2.7 External Users	15
6.1.5 Legal function	5	7.3 Audit trails	15
6.1.6 Information Security Officers	5	7.4 Change control	15
6.1.7 Information Systems Security Administration	6	7.4.1 Emergency problems	16
6.2 Risk acceptance	6	7.5 Computers	16
6.3 Insurance	7	7.5.1 Physical protection	16
6.4 Audit	7	7.5.2 Logical access control	17
6.5 Regulatory compliance	7	7.5.3 Change	17
6.6 Disaster recovery planning	7	7.5.4 Equipment maintenance	17
6.7 Information security awareness	8	7.5.5 Casual viewing	17
6.8 External Service Providers	8	7.5.6 Emulation concerns	17
6.8.1 Internet Service Providers	9	7.5.7 Business continuity	17
6.8.2 Red-Teams	9	7.5.8 Audit trails	17
6.8.3 Electronic Money	10	7.5.9 Disposal of equipment	17
		7.6 Networks	17
		7.6.1 Network integrity	18
		7.6.2 Access control	18
		7.6.3 Dial-in	18
		7.6.4 Network equipment	18
		7.6.5 Change	18
		7.6.6 Connection with other networks	18
		7.6.7 Network monitoring	18
		7.6.8 Protection during transmission	19
		7.6.9 Network availability	19
		7.6.10 Audit trails	19
		7.6.11 Firewalls	19

© ISO 1997

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet central@iso.ch
X.400 c=ch; a=400net; p=iso; o=isocs; s=central

Printed in Switzerland

7.7 Software	20	7.12 Paper documents	29
7.7.1 Applications	20	7.12.1 Modification	29
7.7.2 Databases	21	7.12.2 Viewing	30
7.7.3 Artificial Intelligence(AI)	21	7.12.3 Storage facilities	30
7.7.4 System software	21	7.12.4 Destruction	30
7.7.5 Application testing	21	7.12.5 Business continuity	30
7.7.6 Defective software	22	7.12.6 Preservation of evidence	30
7.7.7 Change	22	7.12.7 Labelling	30
7.7.8 Availability of software code	22	7.12.8 Forged documents	30
7.7.9 Unlicensed software	22	7.12.9 Output distribution schemes	30
7.7.10 Property rights	22		
7.7.11 Viruses	22	7.13 Microform and other media storage	30
7.7.12 Memory resident programs	23	7.13.1 Disclosure	30
7.7.13 Telecommuting	23	7.13.2 Destruction	31
7.7.14 Software provided to customers	23	7.13.3 Business continuity	31
7.7.15 Software used to contact customers	23	7.13.4 Environmental	31
7.7.16 Applets, JAVA, and Software from External Sources	24		
		7.14 Financial transaction cards	31
7.8 Human factors	24	7.14.1 Physical security	31
7.8.1 Awareness	24	7.14.2 Insider abuse	31
7.8.2 Management	24	7.14.3 Transportation of PINs	31
7.8.3 Unauthorized use of information resources	25	7.14.4 Personnel	31
7.8.4 Hiring practices	25	7.14.5 Audit	31
7.8.5 Ethics policy	25	7.14.6 Enforcement	31
7.8.6 Disciplinary Policy	25	7.14.7 Counterfeit card prevention	32
7.8.7 Fraud detection	25		
7.8.8 Know your employee	25	7.15 Automated Teller Machines	32
7.8.9 Former employees	25	7.15.1 User identification	32
7.8.10 Telecommuting	25	7.15.2 Authenticity of information	32
		7.15.3 Disclosure of information	32
		7.15.4 Fraud prevention	32
		7.15.5 Maintenance and service	32
7.9 Voice, telephone, and related equipment	26		
7.9.1 Access to VoiceMail system	26	7.16 Electronic Fund Transfers	33
7.9.2 Private Branch Exchange (PBX)	26	7.16.1 Unauthorized source	33
7.9.3 Spoken word	26	7.16.2 Unauthorized changes	33
7.9.4 Intercept	27	7.16.3 Replay of messages	33
7.9.5 Business continuity	27	7.16.4 Record retention	33
7.9.6 Documentation	27	7.16.5 Legal basis for payments	33
7.9.7 Voice Response Units (VRU)	27		
		7.17 Checks	33
7.10 Facsimile and image	27		
7.10.1 Modification	27	7.18 Electronic Commerce	33
7.10.2 Repudiation	28	7.18.1 New Customers	33
7.10.3 Misdirection of messages	28	7.18.2 Integrity Issues	33
7.10.4 Disclosure	28		
7.10.5 Business continuity	28	7.19 Electronic Money	34
7.10.6 Denial of service	28	7.19.1 Duplication of Devices	34
7.10.7 Retention of documents	28	7.19.2 Alteration or duplication of data or software	34
		7.19.3 Alteration of messages	35
7.11 Electronic Mail	28	7.19.4 Replay or duplication of transactions	35
7.11.1 Authorized users	28	7.19.5 Theft of devices	35
7.11.2 Physical protection	29	7.19.6 Repudiation	35
7.11.3 Integrity of transactions	29	7.19.7 Malfunction	35
7.11.4 Disclosure	29	7.19.8 Cryptographic Issues	35
7.11.5 Business continuity	29	7.19.9 Criminal Activity	35
7.11.6 Message retention	29		
7.11.7 Message Reception	29	7.20 Miscellaneous	36
		7.20.1 Year 2000	36
		7.20.2 Steganography - Covert Channels	36

8 IMPLEMENTING CRYPTOGRAPHIC CONTROLS	36	GLOSSARY OF TERMS	44
8.1 Applying Encryption	37	ANNEX A	49
8.1.1 What To Encrypt	37	Sample Documents	49
8.1.2 How To Encrypt	37	A.1 Sample Board of Directors Resolution on Information Security	49
8.2 Implementing Message Authentication Codes (MAC)	38	A.2 Sample Information Security Policy (High Level)	50
8.2.2 Control of MAC	38	A.3 Sample Employee Awareness Form	51
8.2.3 When to Apply MAC	38	A.4 Sample Sign-On Warning Screens	52
8.2.4 Selection of Algorithm	38	A.5 Sample Facsimile Warnings	53
8.3 Implementing Digital Signatures	38	A.6 Sample Information Security Bulletin	54
8.3.1 How to generate digital signatures	39	A.7 Sample Risk Acceptance Form	56
8.3.2 Certification	39	A.8 Telecommuter Agreement & Work Assignment	58
8.3.3 Legal standing of digital signatures	39	ANNEX B	63
8.3.4 Certificate (Key) management	39	Basic Principles For Data Protection	63
8.3.5 Choice of algorithm	40	ANNEX C	66
8.4 Key Management	40	Names and Addresses of National Organisations	66
8.4.1 Generation	40	ANNEX D	76
8.4.2 Distribution	40	Other security standards	76
8.4.3 Storage	40	Cryptographic Standards	76
8.4.4 Public Key Certification And Standards	40	Secure Session Protocols	76
8.5 Trusted Third Parties	41	Secure Message Formats	77
8.5.1 Assurance	41	Key Management	78
8.5.2 Services of a TTP	41	Payment Protocols	78
8.5.3 Network of TTPs	41	ANNEX E	80
8.5.4 Legal Issues	41	Information Security Risk Assessment	80
8.6. Disaster Cryptography and Cryptographic Disasters	42	INDEX	96
8.6.1 Disaster cryptography	42		
8.6.2 Cryptographic disasters	42		
9 SOURCES OF FURTHER ASSISTANCE	42		
9.1 Financial Services institutions	42		
9.2 Standards bodies	42		
9.3 Building, fire, and electrical codes.	43		
9.4 Government regulators	43		

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.

The main task of technical committees is to prepare International Standards, but in exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;
- type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/TR 13569, which is a Technical Report of type 3, was prepared by ISO Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO/TR 13569:1996), of which it constitutes a technical revision.

Banking and related financial services — Information security guidelines

1 INTRODUCTION

Financial institutions increasingly rely on Information Technology (IT) for the efficient conduct of business.

Management of risk is central to the financial service sector. Financial institutions manage risk through prudent business practice, careful contracting, insurance, and use of appropriate security mechanisms.

There is a need to manage information security within financial institutions in a comprehensive manner.

This Technical Report is not intended to provide a generic solution for all situations. Each case must be examined on its own merits and appropriate actions selected. This Technical Report is to provide guidance, not solutions.

The objectives of this Technical Report are:

- to present an information security programme structure.
- to present a selection guide to security controls that represent accepted prudent business practice.
- to be consistent with existing standards, as well as emerging work in objective and accreditable security criteria.

This Technical Report is intended for use by financial institutions of all sizes and types that wish to employ a prudent and commercially reasonable information security programme. It is also useful to providers of service to financial institutions. This Technical Report may also serve as a source document for educators and publishers serving the financial industry.

2 REFERENCES

NOTE — Annex C contains references to national regulations, standards, and codes. The list below includes only those documents referenced in the main body of this Technical Report.

International Standards:

ISO 8730, *Banking - Requirements for message authentication (wholesale)*.

ISO 8732, *Banking - Key management (wholesale)*.

ISO 9564 (all parts), *Personal Identification Number (PIN) management and security*.

ISO 10126 (all parts), *Banking - Procedures for message encipherment (wholesale)*.

ISO 10202 (all parts), *Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards*.

National Standards:

ANSI X9/TG-2, *Understanding and Designing Checks (USA)*.

ANSI X9/TG-8, *Check Security Guideline (USA)*.

Regulations:

US Office of the Comptroller of the Currency, *Banking Circular BC-226 Policy Statement*.

Other documents:

Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing.

Code of Practice for Information Security Management.

Federal Information Protection Standard (FIPS) PUB 140-1, *Security Requirements for Cryptographic Modules*, National Institute for Standards and Technology (USA).

Security of Electronic Money, published by the Bank of International Settlement, Basle, August 1996.

3 EXECUTIVE SUMMARY

Financial institutions and their senior management have always been accountable for the implementation of effective controls for protecting information assets. The confidentiality, integrity, authenticity, and availability of that information are paramount to the business. As such, it is imperative that these assets be available and protected from disclosure, modification, fabrication, replication, and destruction, whether accidental or intentional. It is imperative for a financial institution to protect the transfer of its assets which are encoded in the form of trusted information.

Business depends more and more on computerized information systems. It is becoming impossible to separate technology from the business of finance. There is increasing use of personal computers and networks, and a greater need than ever for these to work together. In many institutions, more work is done on personal computers and local area networks than on the large mainframes. Security controls for these local computers are not as well developed as controls over mainframes. The security needed for all information systems is growing dramatically. Image systems, digital voice/data systems, distributed processing systems, and other new technologies, such as the Internet, are being used increasingly by financial institutions. This makes information security even more important to the commercial success or even the survival of an institution.

Security controls are required to limit the vulnerability of information and information processing systems. The level of protective control must be cost effective, i.e., consistent with the degree of exposure and the impact of loss to the institution. Exposures include financial loss, competitive disadvantage, damaged reputation, improper disclosure, lawsuit, or regulator sanctions. Well thought out security standards, policies and guidelines are the foundation for good information security.

Work is ongoing within the US, Canada and the European Community to establish a Common Criteria for the evaluation of information technology products. These criteria coupled with financial sector pre-defined functionality classes will enable financial institutions to achieve uniform, trusted, security facilities. This Technical Report should be used as an input to that process.

With the continuing expansion of distributed information there is growing interest and pressure to provide reasonable assurance that financial institutions have adequate controls in place. This interest is demonstrated in laws and regulations. Examples in the form of excerpts are as follows:

1. Office of the Comptroller of the Currency, Banking Circular BC-226 Policy Statement (Joint issuance of the Federal Financial Institutions Examination Council)

"It is the responsibility of the Board of Directors to ensure that appropriate corporate policies, which identify management responsibilities and control practices for all areas of information processing activities, have been established. The existence of such a 'corporate information security policy,' the adequacy of its standards, and the management supervision of such activities will be evaluated by the examiners during the regular supervisory reviews of the institution."

This Technical Report includes a guideline for building a comprehensive information security program.

NOTE ON SECOND EDITION

Since the publication of the first edition of this Technical Report, much has changed. Change has not simplified matters. Virtually no threat or control listed in the first edition has been made obsolete. New threats have surfaced, along with new opportunities for improving delivery of service to customers. Banking over the Internet, electronic money, revolutionary information technology discoveries and rediscoveries make these exciting times. Wherever possible this Technical Report addresses the environment as it is known. Our experience over the last four years dictate that constant vigilance is the minimum requirement for sound security.

4 HOW TO USE THIS TECHNICAL REPORT

This Technical Report was designed to serve many purposes. This clause provides a "road map" to the remainder of the Technical Report.

Clause 5: Requirements: This clause defines a starting point in building a security program. It sets out minimum requirements for an adequate information security program. It may also serve as a measure against which an institution can evaluate the state of its information security program.

Clause 6: Information security program components: This clause contains more specific information on how an Information Security Program should operate. Specific responsibilities are suggested for various officers and functions of an institution. Lines of communication between functions, that are considered helpful for sound security practice are identified. This clause can be used by senior officials to ensure that structural impediments to sound security practice are minimized. Information security personnel may also use this clause to evaluate the effectiveness of the information security program.

Clause 7: Control Objectives and Suggested Solutions: This clause is the heart of this Technical Report. It discusses threats to information in terms specific enough to enable financial personnel to ascertain if a problem exists at their institution, without educating criminals. The first four subclauses address controls common to many delivery platforms: classification, logical access control, change control, and audit trails. Subsequent subclauses address security concerns for information processing equipment, human resources, and those specific to the delivery platform used. Electronic fund transfers and check processing subclauses finish this clause.

Clause 8: Implementing Cryptographic Controls: This clause provides information helpful in assuring that cryptographic controls are implemented in an effective fashion.

Clause 9: Sources of further assistance: This clause lists the types of organizations which may be of assistance to information security professionals. It is intended that this clause be used with Annex C.

Annex A: Sample Documents: This Annex is a collection of ready-to-use sample forms for a variety of information security related purposes.

Annex B: Privacy Principles: This Annex presents a sample set of Privacy Principles.

Annex C: Names and Addresses of National Organizations: This annex lists the names and contact information for national organizations which can be of assistance to Information Security personnel.

Annex D: Security Standards Outside the Financial Community: A comprehensive list of security standards developed by standards groups other than ASC X9 (US) or ISO TC68.

Annex E: Risk and Vulnerability Assessment provides a methodology for identification of risk in an institution.

5 ENSURING SECURITY

At the highest level, the acceptance of ethical values and control imperatives must be communicated and periodically reinforced with management and staff. Information is an asset that requires a system of control, just as do other assets more readily reducible to monetary terms. Prudent control over the information assets of the institution is good business practice.

The protection of information should be centered around the protection of key business processes. The notion of information and its attributes change within the context of a business process and security requirements should be examined at each stage of that process.

Developing, maintaining, and monitoring of an information security program requires participation by multiple disciplines in the organization. Close coordination is required between the business manager and the information security staff. Disciplines such as audit, insurance, regulatory compliance, physical security, training, personnel, legal, and others should be used to support the information security program. Information security is a team effort and an individual responsibility.

The basic recommendation of this Technical Report is the establishment of an information security program that:

- a. includes an institution-wide information security policy and statement, containing:
 - i. a statement that the institution considers information in any form to be an asset of the institution,
 - ii. an identification of risks and the requirement for implementation of controls to provide assurance that information assets are protected. Clause 7 of this Technical Report discusses suitable controls,
 - iii. a definition of information security position responsibilities for each manager, employee and contractor. Clause 6 of this Technical Report lists suggested responsibilities.
 - iv. a commitment to security awareness and education.
- b. establishes one or more officer(s) responsible for the information security program,
- c. provides for the designation of individuals responsible for the protection of information assets and the specification of appropriate levels of security,
- d. includes an awareness or education program to ensure that employees and contractors are aware of their information security responsibilities,
- e. provides for the resolution and reporting of information security incidents,
- f. establishes written plans for business resumption following disasters,
- g. provides identification of, and procedures for addressing exceptions or deviations from the information security policy or derivative documents,
- h. encourages coordination with appropriate parties, such as audit, insurance, and regulatory compliance officers,
- i. establishes responsibility to measure compliance with, and soundness of, the security program,

j. provides for the review and update of the program in light of new threats and technology. For example, the emergence of IT evaluation criteria should assist security professionals in the selection and implementation of standardized security controls.

k. provides for the production of audit records where necessary and the monitoring of audit trails.

6 INFORMATION SECURITY PROGRAM COMPONENTS

Subclause 6.1 addresses the information security responsibilities within the institution. Subclauses 6.2 and beyond addresses functions related to information security. The controls suggested in this Technical Report are those which enforce or support protection of information and information processing resources. While some of these controls may address other areas of bank governance, this Technical Report should not be viewed as a complete checklist of management controls.

6.1 General duties

6.1.1 Directors

Directors of financial institutions have a duty to the institution and its shareholders to oversee the management of the institution. Effective information security practices constitute prudent business practice, and demonstrates a concern for establishing the public trust. Directors should communicate the idea that information security is an important objective and support an information security program.

6.1.2 Chief Executive Officer

The Chief Executive Officer, or Managing Director, as the most senior officer of the institution, has ultimate responsibility for the operation of the institution. The CEO should authorize the establishment of, and provide support for, an information security program consistent with recognized standards, oversee major risk assessment decisions, and participate in communicating the importance of information security.

6.1.3 Managers

Managers serve as supervisory and monitoring agents for the institution and the employees. This makes them key players in information security programs. Each manager should:

- understand, support, and abide by institution's information security policy, standards, and directives,

- ensure that employees, vendors, and contractors also understand, support and abide by information security policy, standards, and directives, for example, the Code of Practice for Information Security Management,
- implement information security controls consistent with the requirements of business and prudent business practice,
- create a positive atmosphere that encourages employees, vendors, and contractors to report information security concerns,
- report any information security concerns to the Information Security Officer immediately,
- participate in the information security communication and awareness program,
- apply sound business and security principles in preparing exception requests,
- define realistic business "need-to-know" or "need-to-restrict" criteria to implement and maintain appropriate access control,
- Identify and obtain resources necessary to implement these tasks.
- ensure that information security reviews are performed whenever required by internal policy, regulations, or information security concerns. Examples of circumstances that should trigger such a review include:
 - large loss from a security failure,
 - preparation of an annual report to the Board of Directors and Audit Committee,
 - acquisition of a financial institution,
 - purchase or upgrade of computer systems or software,
 - acquisition of new communications services,
 - introduction of a new financial product,
 - introduction of new out-source processing vendor,
 - discovery of a new threat, or a change in a threat's direction, scope, or intent.

Additionally, managers who are "owners" of information should:

- be responsible for the classification of information or information processing systems under their control.
- define the security requirements for his information or information processing systems.
- authorize access to information or information processing systems under his control.
- inform the Information System Security Officer of access rights and keep such access information up-to-date.

NOTE — All business information should have an identified "owner." A procedure for establishing ownership is required to ensure that all business information will receive appropriate protection.

6.1.4 Employees, vendors, and contractors should:

- understand, support, and abide by organizational and business unit information security policies, standards and directives,
- be aware of the security implications of their actions,
- promptly report any suspicious behavior or circumstance that may threaten the integrity of information assets or processing resources,
- keep each institution's information confidential. This especially applies to contractors and vendors with several institutions as customers. This includes internal confidentiality requirements, e.g. compartmentalization.

NOTE — Security program components should be incorporated into service agreements and employees' employment contracts.

6.1.5 Legal function

Institutions may wish to include the following responsibilities for the legal department or function:

- monitor changes in the law through legislation, regulation and court cases that may affect the information security program of the institution.
- review contracts concerning employees, customers, service providers, contractors, and vendors to ensure that legal issues relating to information security are addressed adequately.
- render advice with respect to security incidents.
- develop and maintain procedures for handling follow-up to security incidents, such as preservation of evidence.

6.1.6 Information Security Officers

For the purpose of this Technical Report, we define an Information Security Officer as the senior official or group of officials charged with developing, implementing, and maintaining the program for protecting the information assets of the institution.

The Information Security Officers should:

- manage the overall information security program,
- have responsibility for developing Information Security Policies and Standards for use throughout the organization. These policies and standards should be kept up-to-date, reflecting changes in technology, business direction, and potential threats, whether accidental or intentional,
- assist business units in the development of specific standards or guidelines that meet information security policies for specific products within the business unit. This includes working with business managers to ensure that an effective process for implementing and maintaining controls is in place,
- ensure that when exceptions to policy are required, the risk acceptance process is completed, and the exception is reviewed and reassessed periodically,
- remain current on threats against financial information assets. Attending information security meetings, reading trade publications, and participation in work groups are some ways of staying current with new developments,
- understand the current information processing technologies and the most current information protection methods and controls by receiving internal education, attending information security seminars and through on-the-job training, ,
- understand the business processes of the institution, so as to provide appropriate security protection,
- apply management and organizational skills, knowledge of the business, and where appropriate, professional society recognition, in the execution of their duties,
- encourage the participation of managers, auditors, insurance staff, legal staff, and other disciplines that can contribute to information protection programs,
- review audit and examination reports

dealing with information security issues, and ensure that they are understood by management. The officer should be involved in the formulation of management's response to the audit findings and follow-up periodically to ensure that controls and procedures required are implemented within the stipulated time frames,

- confirm that the key threats to information assets have been defined and understood by management,
- assume responsibility or assist in the preparation and distribution of an appropriate warning of potentially serious and imminent threats to an organization's information assets, e.g., computer virus outbreak. See clause A.6 for a sample warning,
- coordinate or assist in the investigation of threats or other attacks on information assets,
- assist in the recovery from attacks,
- assist in responding to customer security issues, including letters of assurance and questions on security. Although a letter of assurance is sent from the institution to the customer, it will often reflect the customer's desires rather than the institution's security policy.

6.1.7 Information Systems Security Administration

Each business unit and system manager must determine the need-to-know access privileges for users within their business sectors and communicate these documented privileges to the administrator. These access privileges should be reviewed periodically and changes should be made when appropriate.

Each information access control system should have one or more Information Systems Security Administrator(s) appointed to ensure that access control procedures are being monitored and enforced. Administrators should operate under dual control, especially for higher level privileges. These access control procedures are described in detail in 7.2.

The Information System Security Administration should:

- be responsible for maintaining accurate and complete access control privileges based on instructions from the information resource owner and in accordance with any applicable internal policies, directives, and standards,
- remain informed by the appropriate

manager whenever employees terminate, transfer, take a leave of absence, or when job responsibilities change,

- monitor closely users with high-level privileges and remove privileges immediately when no longer required,
- monitor daily access activity to determine if any unusual activity has taken place, such as repeated invalid access attempts, that may threaten the integrity, confidentiality, or availability of the system. These unusual activities, whether intentional or accidental in origin, must be brought to the attention of the information resource owner for investigation and resolution,
- ensure that each system user be identified by a unique identification sequence (USERID) associated only with that user. The process should require that the user identity be authenticated prior to gaining access to the information resource by utilizing a properly chosen authentication method,
- make periodic reports on access activity to the appropriate information owner,
- ensure that audit trail information is collected, protected, and available.

The activities of the ISSA should be reviewed by an independent party on a routine basis.

6.2 Risk acceptance

Business Managers are expected to follow the institution's information security policy, standards and directives whenever possible. If the manager believes that circumstances of his particular situation prevent him from operating within that guidance, he should either:

- undertake a plan to come into compliance as soon as possible, or
- seek an exception based upon a risk assessment of the special circumstances involved.

The Information Security Officer should participate in the preparation of the compliance plan or exception request for presentation to appropriate levels of management for decision.

The Information Security Officer should consider changes to the information security program whenever the exception procedure reveals situations not previously addressed.

While a complete treatment of risk management is far beyond the scope of this Technical Report,

clause A.7 provides a sample risk acceptance form that identifies relevant factors in making risk acceptance decisions.

See clause 9 for a risk evaluation methodology.

6.3 Insurance

In planning the information security program, the Information Security Officer and business manager should consult with the insurance department and, if possible, the insurance carrier. Doing so can result in a more effective information security program and better use of insurance premiums.

Insurance carriers may require that certain controls, called Conditions Prior to Liability or conditions precedent, be met before a claim is honored. Conditions Prior to Liability often deal with information security controls. Since these controls must be in place for insurance purposes, they should be incorporated into the institution's information security program. Some controls may also be required to be warranted, i.e., shown to have been in place continuously since inception of the policy.

Business Interruption coverage and Errors and Omissions coverage, in particular, should be integrated with information security planning.

6.4 Audit

The following quotation from the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing defines the auditor's role as follows:

"Internal auditing is an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization. The objective of internal auditing is to assist members of the organization in the effective discharge of their responsibilities. To this end, internal auditing furnishes them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed."

More specifically, in the area of information security, auditors should:

- evaluate and test controls over the information assets of a financial institution.
- engage in an on-going dialogue with Information Security Officers and others to bring appropriate perspectives to the identification of threats, risks, and the adequacy of controls for both existing and new products.
- provide management with objective

reports on the condition of the control environment and recommend improvements that can be justified by need and cost benefit.

- specify retention and review of audit trail information.

Where the audit review function is combined with other functions, management attention is required to minimize conflict of interest potential.

6.5 Regulatory compliance

Regulatory authorities concern themselves principally with issues of safety, soundness, and compliance with laws and regulations. One element of safety and soundness is the institution's system of control that protect information from unavailability, and unauthorized modification, disclosure, and destruction.

Regulatory Compliance Officers should work with the Information Security Officer, business managers, risk managers, and auditors to ensure that information security requirements of regulations are understood and implemented. Regulatory Compliance Officers should also remain current on new technologies or methodologies which may become subject of regulation. For example, compliance with pre-defined functionality classes for Information Technology products.

6.6 Disaster recovery planning

An important part of an Information Security Program is a plan to continue critical business in the event of a disruption. A disaster recovery plan outlines roles and responsibilities under those conditions.

Disaster recovery is that part of business resumption planning that ensures information and information processing facilities are restored as soon as possible after interruption.

The disaster recovery plan should include the following:

- listing of business activities considered critical, preferably with priority rankings, including time frames adequate to meet business commitments,
- identification of the range of disasters that must be protected against,
- identification of processing resources and locations available to replace those supporting critical activities,
- identification of personnel available to operate processing resources or to replace personnel unable to report to the institution,

- identification of information to be backed up and the location for storage, as well as the requirement that the information will be saved for back-up on a stated schedule,
- information back-up systems capable of locating and retrieving critical information in a timely fashion,
- agreements with service suppliers for priority resumption of services, when possible.

The disaster recovery plan should be tested as frequently as necessary to find problems and to keep personnel trained in its operation. A periodic re-evaluation of the recovery plan to ascertain that it is still appropriate for its purposes should be undertaken periodically. A minimal frequency for both tests and reevaluations should be specified by the institution.

6.7 Information security awareness

The goal of a Security Awareness Program is to promote information security. The program is meant to influence, in a positive way, employees' attitudes towards Information Security. Security awareness should be addressed on an on-going basis.

The success of any Information Security Program is directly related to the Information Security Officer's ability to gain support and commitment from all levels of staff within the organization. Failure to gain this support reduces the program's effectiveness.

Without Management support, the information security program cannot survive. Different levels of management and staff have different concerns. These concerns should be emphasized when addressing those various levels. Furthermore, presentations must be made in such a way that people of all levels and skills will be able to understand.

Managers should be made aware of the exposure, risks and loss potential, as well as regulatory and audit requirements. This should be presented both in business terms and with examples pertinent to the manager's area of responsibility; positive messages being the most effective. Subclause 7.8 of this Technical Report examines these areas in more detail.

To function properly, the Information Security Program must achieve a balance of control and accessibility. Both staff and management must be made aware of this. Users must be given access sufficient to perform their required job functions. They should never be given unrestricted access.

The Information Security Program must support the work environment in which it exists. The Information Security staff must not operate in a vacuum. They must understand the business objectives as well as the internal operation and organization of the institution to better protect and advise the institution. By acting in concert with other groups within the organization, a cooperative spirit can evolve that will benefit everyone. In this way, security awareness will be promoted daily.

Lastly, to promote goodwill and support for the program, Information Security staff members must be available to assist at all times.

6.8 External Service Providers

Financial institutions require that externally provided critical services, such as data processing, transaction handling, network service, and software generation, receive the same levels of control and information protection as those activities processed within the institution itself. The contract should include the elements necessary to satisfy the financial institution that:

- external service provider should in all cases abide by the security policies and standards of the financial institution.
- third party reports, i.e., the reports prepared by the service provider's own public accounting firm are made available.
- internal auditors from the financial institution be accorded the right to conduct an audit at the service provider relating to procedures and controls specific to the financial institution.
- the external service provider should be subject to Escrow agreements of delivered systems, products or services.

In addition to the above, an independent financial review of the provider should be conducted by specialists within the financial institution before engaging in a contract with a service provider.

No business should be transacted with a service provider unless a letter of assurance is obtained stating information security controls are in place. The Information Security Officer should examine the service provider's security program to determine if it is in concert with the institution's. Any shortfall should be resolved either by negotiations with the provider or by the risk acceptance process within the institution.

In addition to information security requirements, contracts with service providers should include a non-disclosure clause and clear assignment of liability for losses resulting from information security lapses.

6.8.1 Internet Service Providers

A new emerging networking environment is rapidly introducing new risks to the financial world. The Internet is the world-wide collection of interconnected networks that use the Internet Protocol (IP) to link the various physical networks into a single logical network. This new environment will introduce many new risks never before faced.

The Internet was originally designed as an open network with the emphasis on sharing research information. Security was of little concern to anyone. As the network grew through the years it began to be used by more than a few universities who needed an electronic mail system.

Private companies soon discovered that they could communicate with their peers in other companies which allowed them to escape the boundaries of their internal electronic mail systems. Realizing the vast numbers of people connected to the Internet could have potential for commerce, companies soon began advertising and conducting limited business transactions. They realized that the Internet was virtually free and could reach millions of people for little or no investment.

The Internet was still in its' infancy with little or no tools to make it user friendly. Then new formatting languages were developed which made the Internet easy to access goods and services in human readable form (pictures, color, motion and sound).

The risks of an open network such as the Internet are many because security was never a design consideration and therefore has to be retrofitted. Security that is part of the operating system provides better protection than one that is added on later. Some of the major risks that exist in many of the operating systems are the following:

- **Address spoofing** which allows someone to impersonate another thereby making EMAIL messages untrustworthy.
- **Message integrity** threatened by the ability to change the contents of a message after it has been sent to the recipient.
- **Information theft** where the original message is left unaltered but information such as credit card numbers are stolen.
- **Denial of service attacks** where persons are able to flood an Internet node with automated mail messages which may eventually shut the system down.

There are several ways that one can connect to the Internet. The first is to have a direct connection to the Internet from a computer via serial line Internet protocol (SLIP) connection or a point to point protocol (PPP) connection. Both of these methods

provide the greatest risk to your internal networks because they provide a peer to peer connection. In other words, they are now part of the institution's network and have access to any of the institution's network resources. For more information on how to protect these connections see 7.6 Firewalls.

The second method is to purchase a connection from an Internet service provider that will provide access to the Internet except an outsider is now connecting directly to the service provider's computer, not the institution's.

When selecting a service provider, one must look beyond the price and features and understand what safe guards they are employing to keep outsiders from accessing the system. Some Internet service providers offer complete turnkey operations where all of the security equipment resides on their premises and they manage it all. In this scenario, they monitor all security violations and alert the institution to the incidents that are serious based upon an agreed set of rules.

Insist on conducting a thorough review of the service provider to include who has access to their computer and firewall which is the gateway to the institution's internal networks. Ensure that only the barest minimum of their staff have access to those computer resources and that those access privileges are monitored on a regular basis. If one does not possess the necessary in-house skills to conduct a thorough review, hire a private company not related to the Internet service provider to conduct a security review. Usually this results in a written report which can be used to negotiate changes prior to contract signing.

The Internet can provide a cost effective, relatively safe environment if you are careful in the implementation and ongoing management of this resource.

6.8.2 Red-Teams

The use of a Red-Team, usually a contractor, to test system security by attempting system penetration with the knowledge and consent of an appropriate official of the institution, is a method of deriving assurance for the security program.

As computer systems become more and more complex, security will become increasingly harder to maintain. Use of red-teams can help in finding specific points of weakness in an institutions system. However, some issues must be considered.

- The contractor should be adequately bonded or of sufficient strength to meet any liabilities arising from their efforts.
- The institution should not rely solely on red-team reports to monitor its security program.

- Non-disclosure of results should be addressed in the contract with the red-team. Any disclosure of security problem should be at the discretion of the institution.

6.8.3 Electronic Money

Recent advancements in smart-card technology and cryptography has led to the ability of financial and non-financial institutions to issue tokens which are capable of storing and exchanging value. While the regulatory environment differs from country to country, several issues seem to be common to all. Some of the following issues illustrate the questions that may impact an institution's decision to participate in an electronic money program.

Disclosure: How much information is to be made available to customers and how? Who decides? Customer advocates will pressure governments to require a certain amount of disclosure on issues of liability, refund policy in case of lost, malfunction, or theft, fees, privacy expectations, and other issues.

Issuers: Who should be allowed to issue stored value cards? Should banks be treated differently from other issuers?

Capacity: How much can be stored in a token? Can the token be refilled? How are limits to be enforced.

Privacy: What restrictions should be placed on collection of customer purchase information for marketing purposes.

Law Enforcement Concerns. Money laundering would be greatly facilitated if an unlimited value, refillable, untraceable, anonymous electronic cash system were available.

Record Keeping: To what degree does an institution keep records? For what purpose? If electronic money is to be refundable, transactions need to be capable of being traced. How is privacy, accountability and law enforcement issues to be balanced?

How these questions are addressed will have a great impact on the security of electronic money systems. Subclause 7.19 provides some control assistance, but the institution must address these broader questions first.

6.9 Cryptographic operations

Threats against confidentiality and integrity of information can be countered by appropriate cryptographic controls. Cryptographic controls such as encryption and authentication require that certain material, e.g., cryptographic keys, remain secret.

One or more facilities that generate, distribute, and account for cryptographic material may be required to support cryptographic controls. ISO standards on banking key management should be used wherever possible.

The facilities providing cryptographic material management should be subject to the highest level of physical protection and access control. Key management must be performed under split knowledge to preserve the security of the system.

Sound cryptographic practices and effective disaster recovery planning foster conflicting objectives. Close consultation between those responsible for disaster recovery and cryptographic support is imperative to ensure that neither function compromises the other.

Supply of cryptographic materials to customers should be done in a manner that minimizes the possibility of compromise. The customer should be made aware of the importance of security measures for cryptographic material. Interoperation with a customer's, correspondent's or service provider's cryptographic system should only be allowed under a fully documented letter of assurance.

The quality of security delivered by cryptographic products depends on the continued integrity of those products. Both hardware and software cryptographic products require integrity protection consistent with the level of security they are intended to provide. Use of appropriately certified integrated circuits, and anti-tamper enclosures, and key zeroizing make hardware systems somewhat easier to protect than software. When circumstances allow, software cryptographic products may be used. Features that enhance system integrity, such as self-testing, should be employed to the maximum degree feasible.

Cryptographic products are subject to varying governmental regulations as to use, import, and export. Local regulations on the use, manufacture, sale, export, and import of cryptographic devices vary widely. Consultation with local counsel or authorities is advised.

Clause 8 provides guidelines for successful implementation of cryptographic controls.

6.10 Privacy

Financial institutions possess some of the most sensitive information about individuals and organizations. Laws and regulations require that this information be processed and retained under certain security and privacy rules. Certain technical and business developments, such as networks, document imaging, target marketing, and cross-

departmental information sharing, have led to concerns about the adequacy of banks' privacy protection.

Financial institutions should review all privacy laws and regulations, such as those involving credit information. Consideration should also be given to keeping current on emerging national privacy legislation, either through bank law offices, bank industry sources, or other independent information sources. In addition, banks that have international operations need to be aware of regional and international and other privacy laws and regulations that apply.

Financial institutions should review their operations to determine whether information on their customers and employees are adequately protected. Specific policies and procedures should be developed concerning how information is gathered, used, and protected. These policies and procedures should be made known to relevant employees. Privacy policies and procedures should address:

- collection of information to ensure that only information which is relevant to an identified business need, and accurate is collected;
- processing of information to provide appropriate restrictions over access, including determinations of who should have access to information, quality control to avoid errors in data entry or processing, and protection against inadvertent unauthorized access;
- sharing of information, so that it occurs only through pre-determined procedures, that information is used for purposes relevant to the reasons for its original collection, and that such sharing does not lead to new opportunities for unauthorized privacy invasion by other parties;
- storage of information to ensure that it occurs in protected fashion to disallow unauthorized access;
- notification of information use and the availability of procedures that allow the person whose information is being held, to correct errors and to raise objections over the use of this information; and
- secure destruction of information when no longer needed.

In addition, electronic and other forms of employee monitoring must meet legal requirements that vary by jurisdiction. Worker monitoring is increasingly being viewed as a privacy issue and is undergoing court and legislative review. Privacy protection

and due process rights need to be considered in addition to employer rights.

Financial institutions might consider developing a privacy audit. This audit evaluates how well the institution is achieving privacy protection and considers ways by which information technology can address privacy problems.

See Annex B for Basic Principles for Data Protection from the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

7 CONTROL OBJECTIVES AND SUGGESTED SOLUTIONS

The controls listed in this clause are measures to ensure the availability of information and information processing resources, and to prevent unauthorized modification, disclosure, or destruction of information, whether intentional or accidental.

Subclauses 7.1 through 7.4 discuss four recurrent themes, that support many other controls:

- information classification,
- access control,
- audit trails, and
- change control.

The remaining parts of the clause discuss controls and their applicability, organized beginning with computers, networks, and software, followed by human factors, then moving to specific service platforms. A subclause on electronic fund transfers and a note on checks complete this clause.

Each control appears with a brief statement of the primary control objective. It should be noted that many controls which are intended to prevent intentional abuse, are also useful against accidental harms. When the objective is relevant to the institution's line of business, it is recommended that the control listed be implemented whenever feasible. The actual decision to implement or not implement a control listed here will depend on the size and type of the institution as well as the institution's tolerance to risk, and regulatory requirements.

The determination of which vulnerabilities are present and what risk arise from them are an integral part of any security system. The risk assessment process is a method of selecting policies and safeguards to protect information assets from security threats occurring through the vulnerabilities inherent in personnel, facilities and equipment, communications, applications, environmental software and operating systems. The risk assessment of an institution function should be done by assessing the security threats relating to the

vulnerabilities and, based on the impact of occurrence, assigning a high, moderate, or low risk to the particular vulnerability. In this way, the possibility and magnitude of monetary loss, productivity loss and embarrassment to the user can be minimized. Annex E provides a methodology for such an assessment.

It is most important that the institution address all known threats it faces. Controls, insurance, or formal acceptance of risk are all preferable to ignoring threats.

7.1 Information classification

Not all information in a financial institution requires a maximum level security control. A method of identifying which information requires good, better, or best control, should be implemented. Information can be classified by two broad concerns within the bank: Criticality and Sensitivity.

Criticality of information is the requirement that the information be available when and where required for the continuity and survival of business. The criticality of information is directly related to the criticality of the processes accessing the information. The contingency/disaster recovery program provides classification of processes. These same categories must be applied to the information. Information which is classified as CRITICAL require certain controls to ensure its availability.

While not differentiated in this Technical Report, it may be useful to an institution to classify information or applications as to its criticality. For example information may be

ESSENTIAL

Information or information processing capacity whose loss would cause severe or irreparable damage to the institution.

IMPORTANT

Information or information processing capacity whose loss would cause moderate but recoverable damage

NORMAL

Information or information processing capacity whose loss would represent minor disruption.

Information sensitivity is specified in very broad terms as a measure of how mishandling may impact the institution. The question used when categorizing sensitive information is, "What is the possible impact on the institution of unauthorized

modification, disclosure, or destruction of the information and what is the probability of that impact occurring?" The areas to consider when evaluating impact include the effect on institutional credibility, profitability, and customer confidence as well as considering regulatory and legal requirements.

There is no consensus in the industry on words describing the various levels of sensitivity of information. For the purposes of this Technical Report, the following scheme of information classification was adopted. Institutions should look to the definitions used rather than the labels chosen.

The primary reason for classifying information is to communicate management's expectation of how employees are to handle it. If a document, file, or database contains various classifications, it must be treated according to the highest classification category of information it contains.

It is important to note that the classification of information may change during its useful life. These changes should be controlled under the information security policy of the institution.

HIGHLY SENSITIVE:

Information of the highest sensitivity which, if mishandled will probably cause substantial damage to the institution. Examples include acquisition/merger information, strategic business plans, and cryptographic keys and materials.

SENSITIVE:

Information which, if mishandled, may cause significant damage to the institution. Examples include personnel information, customer information, and department budgets or staffing plans.

INTERNAL:

Information which, if mishandled, could cause some damage to the institution. Examples include internal memos, telephone books, and organization charts.

PUBLIC:

Information which has been expressly approved for release to the public. Note that public information never originates as PUBLIC but is reclassified when it is released. Examples are the annual report and new products.

7.2 Logical access control

The term "access control" will appear many times in this subclause. As used in this Technical Report, it is the collection of all controls used to ensure that only authorized persons will have access to

information or information processing facilities for which they are authorized.

NOTE — Many of the controls described in this subclause require certain parameters be fixed by the institution; The letter 'n' will indicate such a parameter, and will be followed by a suggested value, based on current prudent practice.

The following controls should be put into place to achieve effective access control.

7.2.1 Identification of users

In this subclause, identification of users focuses on individuals. In some circumstances, a group of users may be required to share an identification and password. In these circumstances, the management must assume any responsibility arising from this shared use. When such a decision is made, the term "individual user" may be interpreted to include groups of users.

To identify individual users of information processing facilities,

- assign a unique user identification sequence (USERID) to each individual user of information processing systems.
- hold each individual accountable for all activity performed under his USERID.
- require that each use of a USERID be traceable to the individual who logs on.

To ensure that unused or unneeded USERIDs are not used in an unauthorized manner,

- suspend rights associated with a USERID after n days of non-use (suggestion n= 90), and delete n days after suspension (suggestion n=30). In circumstances in which USERIDs are only used quarterly, longer time limits may be appropriate, however, rights should be suspended between scheduled actions.
- revoke privileges assigned to separated or transferred employees' USERIDs immediately.

7.2.2 Authentication of users

Users may be internal or external to the institution. 7.2.1 through 7.2.6 address primarily internal users, External users are addressed in 7.2.7

To provide authentication of a user's identity,

- require use of either static or dynamic passwords. Static passwords are those that are memorized by the user. They authenticate a person by something the person knows. Dynamic password systems use devices to

generate new passwords for each session. They authenticate a person by something the person has, something the person knows, or something the person is.

To ensure proper authentication using a static password,

- require users to report known or suspected password compromises immediately.
- require that passwords be chosen by the user.
- assign an initial password that is to be changed by the new or reinstated user on first use.

To minimize the chances that someone may acquire or guess a password,

- require a minimum password length of n characters (suggestion n=6).
- require passwords be changed, at least once in n days (suggestion n=90 or 30 days for SENSITIVE or HIGHLY SENSITIVE applications), and enforce by suspending USERID if passwords are not changed.
- make distress passwords available for sensitive operations. A distress password is a pre-arranged password, different from a user's usual password, that is used to signal that the user is being coerced to access the system under duress.
- require that passwords not be shared, available or known to others, including administrators.
- instruct users not to choose passwords easily guessed, i.e., names or part of names, phone numbers, dates, common words or numbers. Use dictionary checking to restrict selection, if available. A dictionary enhanced with organizational terminology would provide better checking.
- consider requiring that passwords include both alphabetical and numerical components.
- forbid the writing down of passwords. Alternatively, require that passwords be subject to the same handling procedures used for lock combinations.
- protect password by encryption during transmission, where possible. Use encryption mechanisms which prevent successful replay of encrypted passwords.

To ensure the continued integrity of static passwords,

- require the use of the current password prior to allowing a new password to become effective.
- prevent reuse of the user's last n passwords (suggestion $n=4$).
- prohibit change of password within n days of previous change (suggestion $n=1$).
- store passwords under irreversible encryption.
- prohibit the display of passwords on input, reports, or other media.

To ensure proper authentication using dynamic password systems,

- select authentication tokens that require either a user-changeable personal identification number (PIN) or biometric data to be activated.
- require a user's PIN to differ from the USERID.
- prohibit token PINs from being shared.
- require minimum token PIN length to be n characters (suggestion $n=4$).
- require generated password length be a minimum of n characters (suggestion $n=6$).
- require randomly generated passwords be used only once.
- require that generated passwords not be easily guessed.
- require that keys and other information CRITICAL to authentication be encrypted within the token and on the validating system.
- require security tokens be resistant to tampering and duplication.
- lock token after n invalid PIN entries (suggestion $N=3$).
- maintain an inventory control on security tokens.
- require employees to sign for security tokens on a form which details acceptable uses and consequences for misuse.
- recover dynamic tokens from the employee upon reassignment or termination.

Alternately, terminate access privileges associated with the token assigned to the employee.

- consider use of biometric features with security tokens, where feasible.

7.2.3 Limiting sign-on attempts

To assist in the discovery of unauthorized sign-on attempts,

- display to the authorized user, the date and time of last access and the number of unsuccessful access attempts.

To limit the opportunity for unauthorized attempts to sign-on to a system,

- suspend the USERID after a maximum of n repeated unsuccessful log-on attempts (suggestion $n=5$).
- set authentication time limit at n minutes (suggestion $n=5$); terminate the session if the time limit is exceeded. In both cases, users should be informed of failure, but not the reason.

7.2.4 Unattended terminals

To prevent unauthorized use of a terminal already connected to a system,

- require that the identification and authentication process be repeated after a specified period of inactivity, before work can be continued.
- recommend use of one-button lockup system, force button, or shut-off sequence be activated when terminal is left alone.

7.2.5 Operating system access control features

To ensure that information and information processing resources are protected when systems supporting multiple users are in use,

- specify the use of access control software that is capable of restricting access of each individual to only those information resources for which the individual is authorized.

NOTE — Single user computers, such as PCs, laptops, and notebooks are required to perform authentication, but when appropriate, it is assumed that the single user has total access to, and control of, the computer.

7.2.6 Warning

To warn unauthorized users of the possible consequences of their actions,

- display a warning screen, prior to completing sign-on, that warns the reader that unauthorized access may result in prosecution. Clause A.4 contains examples of warning messages.

7.2.7 External Users

In addition to the controls listed above, access granted to users outside the institution network must be closely controlled.

To protect against unauthorized access from external users,

- require that all traffic external to the institution's network pass through a firewall. (See 7.6.11.)

7.3 Audit trails

Audit trails are records of activity used to provide a means of restructuring events and establishing accountability. The audit trail information is essential for investigation of problems.

Controls useful in the audit trail process are as follows:

To deter and provide early detection of unauthorized activity,

- provide an audit trail for computer systems and manual operations when:
 - SENSITIVE or HIGHLY SENSITIVE information is accessed,
 - network services are accessed, and
 - special privileges or authorities are used, such as, security administration commands, emergency USERIDs, supervisory functions, and overrides of normal processing flow.
- include in the audit trail as much of the following as is practical:
 - user identification,
 - functions, resources, and information used or changed,
 - date and time stamp (including time zone),

- workstation address and network connectivity path, and

- specific transaction or program executed.

- provide, where practical, an additional real-time alarm of significant security-related events for all computer systems having on-line capabilities for inquiry or update, containing information such as:

- access attempts that violate the access control rules,

- attempts to access functions or information not authorized,

- concurrent log-on attempts, and

- security profile changes.

- investigate and report suspicious activity immediately.

- ensure that management reviews the audit trail information on a timely basis, usually daily.

- investigate and report security exceptions and unusual occurrences.

- retain the audit trail information for an appropriate period of time for business requirements.

- protect audit trail information from deletion, modification, fabrication or resequencing, by use of MAC or digital signature.

7.4 Change control

To protect the integrity of information processing systems, a change control procedure is needed. Change control procedures should exist for hardware changes, software changes, and manual procedure changes. To be effective, the procedure must also address emergency changes. The controls that should be used in change situations follow.

To prevent unauthorized changes from being implemented in the production environment,

- establish a change control procedure, that manages all changes, regardless of the magnitude, whether scheduled or emergency.

To ensure that the change control procedure is effective,

- establish a formal change request and authorization process.
- establish a testing and system acceptance procedure for each change.
- require that all changes be scheduled and fully documented.
- ensure all changes have viable back-up procedures defined should they fail during or immediately after the change.
- where appropriate ensure virus checks are made before and after changes.

7.4.1 Emergency problems

To maintain integrity during emergencies,

- allow emergency fixes only to resolve production problems.
- return to normal change procedures expeditiously.
- instruct emergency support personnel to document changes.
- review all emergency changes.

7.5 Computers

Computers are at the center of information security discussions. Computation power allows financial institutions more flexibility and processing capability than ever before. The complex array of computer capabilities offers both operational advantages and raises security concerns.

This subclause focuses on computers as individual components of the information processing facility of the institution. These include mainframes, minicomputers, microcomputers, laptops, notebooks, palmtops, servers, workstations, departmental, corporate, and personal Computers, among others.

The following controls should be implemented to protect the integrity of computers in use by the institution.

7.5.1 Physical protection

Physical barriers to information or information processing equipment can serve to control access. The "fortress computer center" is becoming increasingly rare. However, there may be circumstances when physical controls may be adequate.

To protect computers and central information processing centers from physical harm,

- choose the site of processing areas away from flight paths, geologic fault lines, power lines, potential terrorist targets and the like.
- define a security perimeter around central processing facilities as a basis for physical controls.
- do not identify processing areas in lobby directories and phone books.
- limit physical access strictly to authorized personnel. A record of entry and exit should be kept. Positive identification should be established prior to any entry. All staff should be instructed to challenge or report unrecognized or unauthorized persons.
- establish an inventory or property control program.
- monitor the movement of all computer equipment from institution facilities.
- build rooms or areas containing information processing equipment that conform to all building and fire codes of the local jurisdiction and to the manufacturer's specification. Note that Building codes vary widely. Check local codes.
- provide adequate air-conditioning for cooling equipment in levels specified by manufacturers under worst case conditions.
- provide clean and adequate power. The installation of an uninterruptible power supply (UPS), generators, and agreements for priority restoration of service are recommended.
- provide adequate fire and water protection.
- have engineering diagrams that have been reviewed for single-point-of-failure and evaluated for ways to eliminate those failures.
- prohibit storage of hazardous or combustible material within the perimeter.
- consider an intermediate holding area for deliveries to the processing rooms.
- escort visitors at all times.
- ensure building and equipment meet insurer's requirements.

To protect personal computers when used off-site:

- prohibit use of personal computers off-site unless virus controls are in place.
- require that personal computers not be left unattended in public places.
- require personal computers be carried as hand luggage while traveling.
- require all manufacturer's instructions regarding protection of equipment be followed.
- prohibit the use of personal computers off site unless they have adequate access protection in place commensurate with the information's classification.
- apply all other controls as appropriate, i.e. software virus protection.

7.5.2 Logical access control

To prevent unauthorized modification, disclosure, or destruction of information residing on computer systems,

- employ logical access control, as defined in 7.2, for all computers and computer systems.

7.5.3 Change

To maintain the integrity of the processing system when changes are made,

- require that change control procedures be followed. See 7.4.

7.5.4 Equipment maintenance

To ensure that the integrity of security controls is maintained during equipment maintenance,

- allow modifications to be made only by authorized personnel within established maintenance procedures.
- require the testing of controls, both before and after maintenance changes.
- maintain a record of all faults or suspected faults.
- where appropriate ensure virus checks are made.
- Tamper-protect components which store sensitive information.

7.5.5 Casual viewing

To minimize the disclosure of SENSITIVE or HIGHLY SENSITIVE information on computer terminal screens,

- position computer displays so that information is not routinely visible to unauthorized persons. Alternately, install privacy shields.

7.5.6 Emulation concerns

To ensure that all appropriate controls are implemented,

- require that controls that are normally applied to a specific transaction or process also apply to computer systems that support that transaction or process. For example, if a personal computer contains hardware and software that allow it to emulate a facsimile machine, the controls listed in 7.10, Facsimile and Image, should also apply.

7.5.7 Business continuity

To ensure that the institution can continue to function in case of major disruption caused by natural disasters, power failures, or other factors,

- include computer systems as part of the contingency and disaster recovery plan. See 6.6 for more details.

7.5.8 Audit trails

To ensure continuing quality of controls,

- maintain an audit trail as described in 7.3.

7.5.9 Disposal of equipment

To prevent disclosure of sensitive information,

- check all equipment containing storage media for sensitive information prior to disposal.
- perform a risk assessment on damaged equipment to determine if it should be destroyed, repaired or discarded.
- require storage media to go through a secure erasure procedure prior to disposal.

7.6 Networks

A network is the collection of information processing and communications resources that enable computers or individuals to access and transmit information. Networks may be as simple as two personal computers connected to each other, or as complex as a world-wide, multi-institution, funds transfer network, e.g., S.W.I.F.T. Controls for protecting the integrity of networks include the following:

7.6.1 Network integrity

To prevent the capture of a session during accidental or intentional communication line drops,

- provide network controls for the detection and reporting of dropped communications lines and timely termination of all associated computer sessions.
- require re-authentication when line drops occur.

7.6.2 Access control

To protect against modification, destruction, or disclosure of information through unauthorized access or use of communications facilities,

- grant communications access only on a need-to-use basis. Where possible and appropriate, communications access privileges should be further restricted to specific programs, information, dates/times.

7.6.3 Dial-in

Dial-in is the capability to access information processing resources via public or private networks.

To ensure that access control is not compromised through the misuse of dial-in,

- establish a policy setting out conditions under which dial-in is permissible.
- implement, where business needs dictate, additional controls such as, token-based authentication devices, security modems that can provide password and dial-back controls, or remote computing software that can provide password controls.

To ensure that dial-in by vendors does not compromise security, in addition to other controls,

- execute a written agreement with vendors identifying security roles and responsibilities.
- establish a procedure requiring the intervention of an authorized employee to enable a dial-in access session. The dial-in session must be disabled upon completion.
- review activity logs of each vendor session.

7.6.4 Network equipment

To prevent the unauthorized use or interruption of network equipment,

- control access to network equipment by

logical access controls listed in 7.2, where possible.

- locate network equipment in a physically secure environment, where appropriate.
- require wiring closets to be physically secure, with only authorized personnel permitted access.
- route cabling underground or through conduits, wherever possible.
- maintain an inventory of network equipment.

7.6.5 Change

To preserve integrity and availability of information resources during changes to the network,

- limit network changes to those made in accordance with established change management procedures. See 7.4.

7.6.6 Connection with other networks

To ensure that information security is not compromised because of security problems in networks not under the institution's control,

- require specific authorization by the Information Security Officer for connection to networks not under the institution's control.

Alternatively,

- establish written policies and procedures for connection to external networks.
- require the security policy of the external provider be verifiably as strong as the bank's own network.

7.6.7 Network monitoring

To protect against information disclosure, modification, or destruction by use of monitoring devices,

- implement use and storage controls over devices that monitor or record information being transmitted on a network (e.g., protocol analyzers and other diagnostic equipment). This equipment should not be utilized without the consent of the Information Systems Security Administrator or the Information Security Officer.

- ensure that employees are made aware as part of their condition of employment that use

of the institution's information processing assets constitute consent to monitoring.

7.6.8 Protection during transmission

To protect HIGHLY SENSITIVE information from disclosure during transmission,

- encrypt HIGHLY SENSITIVE information during electronic transmission, if feasible.
- protect passwords by encryption during transmission, where possible.

To detect corruption or modification of HIGHLY SENSITIVE information during transmission,

- authenticate information with a message authentication code (MAC) or digital signature and require checking at the destination.

7.6.9 Network availability

To protect against information loss in situations where power fluctuations or outages occur,

- protect network equipment by use of Uninterruptable Power Supplies (UPS).

To protect against destruction or modification of information residing on network resources,

- establish and enforce a periodic back-up of information on network resources.
- test the recovery of backed-up data periodically.

To protect against losses due to the unavailability of network resources,

- include network services in the Disaster Recovery Plan, when appropriate. See 6.6.

7.6.10 Audit trails

To ensure continuing quality of controls,

- maintain an audit trail as described in 7.3

7.6.11 Firewalls

The increased use of the Internet has simultaneously made computer technology more useful and more dangerous. The almost universal connectivity which is nothing short of miraculous also presents unprecedented opportunity for attack. Any person with a computer can subscribe to an Internet service provider and become a true network "node." As a result there is no control over who can be on the Internet or what they are using it for. There is therefore a need to protect systems on the Internet from both known and

unknown assaults from a vast pool of attackers. This protection generally takes the form of a Firewall.

A Firewall is defined as a collection of components placed between two networks that collectively have the following properties:

- All traffic from inside to outside, and vice-versa, must pass through the firewall.
- Only authorized traffic, as defined by local security policy, will be allowed to pass.
- The firewall is itself immune to penetration.

A well-designed firewall protects the institution's network from attacks from sources external to its network and the network to which it is connected to by the firewall. Attacks from within the institution's network, or that of its communicating partner, must be addressed by other security services.

Firewalls specified for use in a financial institution should be designed for the following considerations:

Strong Authentication and Identification

A high degree of confidence of knowing with whom an institution is dealing is required. "Know your Customer" is a regulatory requirement in many jurisdictions and must precede any authorization to conduct business. The ability of identifying who is using a system is required to prevent unauthorized use, to aid investigation of attacks.

Audit and archive requirements

Financial institutions are required by regulation to keep certain records. The activity through a firewall will often contain information which must be archived to prove transactions.

Auditable security-related events also must be properly captured.

Non-repudiation

Payment instructions should be protected sufficiently to support a collection action.

Availability

Unless a service can be reliably offered, it should not be. Customer frustration over banking systems that do not work on demand may result in lost business.

Confidentiality of records.

Confidence that bank records will remain protected is a customer assumption. Loss of this confidence will result in lost business. Embarrassing a big institution is a powerful motivator of the hacker community.

Because the Internet environment is constantly changing, it is difficult to specify exhaustively all the requirements for firewalls. However the following suggestions, where applicable, should form the basis of proper firewall selection and implementation.

Design Axioms

- Any non-Internet connection to the institution's networks must be properly controlled
- No IP packets will be exchanged between networks and the Internet through the connection established through the Firewall
- Traffic is exchanged through the firewall at the application layer only.
- Institution's hosts which support incoming service requests from the public Internet will sit "outside" any firewall.
- Firewall systems will be implemented to work within the constraints of internal network routing

Technical Features

- The firewall must enforce a protocol discontinuity at the transport layer.
- The firewall must not switch any IP packets between the protected and unprotected networks.
- The firewall must hide the structure of the protected network.
- The firewall must provide an audit trail of all communications to or through the firewall system and will generate alarms when suspicious activity is detected.
- The firewall system must use a "proxy server" to provide application gateway function through the firewall.
- Routes through the firewall must be statically defined.
- The firewall must not accept session initiation from the public Internet.
- The firewall system must defend itself from direct attack.
- The firewall must be structured so that there is no way to bypass any firewall component.
- The firewall must include an application "launch server" to support application connections from user systems to Internet services.

Proxy Server Attributes

- The proxy server acts as an application gateway.
- The proxy server hides internal details of the protected network from the public Internet.

- The proxy server does not switch any network level packets.
- The proxy server logs all activity in which it is involved.

There are no user accounts on the proxy server itself.

Launch Server Attributes

- The launch server houses only client applications.
- User logins on the launch server must be different from the user's "home account."
- Where possible, the launch server should be based on a different hardware and software platform than user "home" systems.

7.7 Software

Software used in the financial sector carries a requirement for high integrity. Since software may be somewhat intangible, i.e., not visible or capable of existing in multiple copies or in various forms, control of software poses different challenges from the control of equipment.

The following controls should be implemented for the protection of software and the information that is processed by software. In general, all access to live data or software must always be justified and authorized. Work carried out should be monitored or recorded and validated, signed off by an authorized person who understands the underlying business application. Results to be reported to or filed in the security unit.

7.7.1 Applications

Applications are specific sets of software designed to accomplish one or more functions, such as funds transfer, billing, or logical access control. An application is the reason for using the computation power.

To prevent unavailability or unauthorized modification, disclosure, or destruction of information when used in applications,

- integrate application security with the operating system access control facility, such that USERIDs and passwords are maintained by the operating system control facility, not the application system. This allows for centralized and standardized USERID and password management, as well as more efficient audit and reporting functions.
- establish an access profile structure that controls access to information and functions, if not otherwise provided. The "profile" must have the capability to restrict access such that the "least possible privilege" can be granted to an individual to perform the job.

- require consistent access controls on information that is replicated on multiple platforms.
- require that application control identify specific accountability to a user/USERID. All updates should be logged with a USERID/time/date stamp.
- incorporate information ownership into the system, where applicable. The ownership may be accountable on a group or individual level.
- consider location control methodology that applies additional restrictions at specific locations.
- include dual control capabilities for CRITICAL transactions such as money movement transactions.
- require applications not under the control of a database management system to meet requirements listed under databases.
- log and report violation messages, when they exist.

7.7.2 Databases

A database is a collection of information that may be retrieved according to one or more criteria. It is dealt with here as a special case of software application.

To protect databases from unauthorized modification or destruction, and to maintain the integrity of information stored on databases,

- require that database management systems have controls to ensure that all updating and retrieving of information preserve information integrity with respect to transaction control and system failure. Concurrency control is required for shared-used databases.
- require that all access to information be controlled as specified by an Information System Security Administrator.
- apply access control mechanisms to physical information resources to restrict access to authorized information management systems, applications, and users. This requirement is especially important where access is possible via mechanisms other than the intended primary information management agent.

7.7.3 Artificial Intelligence(AI)

Applications using AI techniques should include controls specific to that technology.

- secure all knowledge bases used by inference engines or similar AI processing techniques and ensure a regular review for accuracy and effectiveness.
- place limits of the automatic decision making ability of AI systems or AI subsystems of conventional applications to ensure that unexpected errors do not go unchecked.
- where possible, place AI systems in an interaction or control framework with human operators to ensure that vital decisions are approved.
- place controls on the information used in the training of neural networks based applications.
- monitor the stability of neural network based application for effectiveness.
- build all AI systems within programmed decision enclosures to ensure the control of decision making is kept within reasonable limits according to the information being processes or the impact of decisions made.

7.7.4 System software

System software is that set of instructions which function as the central control for the computing system. Special attention must be given to the control of this software, and the facilities which allow manipulation of this software, and consequently other security controls in the system.

To ensure the integrity of system software,

- apply the most stringent access controls to system software and their handling facilities.
- apply the highest Human Resource standards in selecting personnel for systems software operation and maintenance.

7.7.5 Application testing

Application testing is the checking of new or modified processing systems to ensure that systems are working properly.

To protect SENSITIVE or HIGHLY SENSITIVE customer information from disclosure or inappropriate processing during application testing,

either,

- establish and communicate a policy that controls the use of production information during application testing, and use access control to limit to appropriate personnel, the renaming and restoring of production files,

or,

- depersonalize production information by rearranging one or more sensitive fields, so as to render the resulting files unrelated to actual customer accounts, and use other controls to ensure that no statements or notices are generated and distributed on test information.
- dispose of production information used in testing, in either case.
- require use of physically separate environments for operational and development systems.

7.7.6 Defective software

To minimize the probability of latent defects in software,

- require the software acquisition system to select vendors with a good reputation, a proven record, and sufficient resources or insurance to cover damages resulting from their software.
- institute a quality assurance program for all software.
- require that all software be fully documented, tested, and verified.

7.7.7 Change

To maintain the integrity of software when changes are made,

- require that change control procedures be followed. See 7.4.

7.7.8 Availability of software code

To ensure that source code is available for debugging or enhancement,

- establish procedures to maintain the most current version of programs written by the institution's staff and contractors.
- consider an escrow agreement for purchased software for which source code is not available.

7.7.9 Unlicensed software

To prevent litigation or embarrassment caused by use of software that is not licensed or beyond the license granted by the vendor,

- use only licensed or authorized software.
- maintain evidence that license agreements are being fully met. This can include an inventory system, physical control of master copies, and periodic auditing of computers.

7.7.10 Property rights

To minimize concerns over intellectual property rights to software,

- establish a written policy on intellectual property rights. Employees and contractors involved in developing software should be made aware of this policy.

7.7.11 Viruses

To protect the integrity of information from modification, disclosure, or destruction by a computer virus,

- implement a virus detection and protection procedure. All software acquired by the institution should be checked by the virus detection procedure prior to installation and use.
- establish written policy on downloading, acceptance, and use of freeware and shareware. Prohibit this practice, if possible.
- authenticate software for highly CRITICAL applications using MAC or digital signature. Failure to verify indicates a potential problem and should prevent the software from being used until the source of the problem is identified and properly dealt with.
- distribute instructions on the detection of viruses to all users. Evidence such as sluggish performance or mysterious growth of files, should alert users to a problem that must be reported.
- establish a policy and procedure for the checking of diskettes brought in from outside the institution's normal purchasing program.
- seek assistance in case of suspected infection. Assistance may be sought from vendors, colleagues, and anti-virus bulletin boards.

To ensure recovery of processing capability following a virus infection,

- retain an original back-up copy of all software and hold until such time as the original software is no longer in use.
- ensure that all data is backed up regularly.

7.7.12 Memory resident programs

To prevent loss of integrity because of the presence of memory resident programs i.e., those that allow seemingly normal processing to take place but retain ultimate control over functions of the processing resource,

- perform periodic inspection of software installed to ascertain whether any unauthorized software has been inserted. Special attention should be given to the detection of memory resident programs.

7.7.13 Telecommuting

Telecommuting is generally thought to be working from home. A virtual office can be anywhere that is an extension of the workplace. Telecommuting equipment may include phone, fax and computers, usually laptops or desktops.

A number of government mandates relating to clean air, family leave, and accommodation of workers with disabilities have encouraged employers to allow telecommuting. Telecommuters have benefited from the practice through reduce commuting costs, and avoidance of stress and fatigue. The trend seems to be to allow more and more employees to telecommute.

All controls listed in this Technical Report apply to the telecommuting environment. In addition, to those controls, Human Resource issues also arise for employees who telecommute. See 7.8 and care must be taken with respect to remote access to information resources.

To prevent loss of control over personal computers and the systems to which they may be connected because of capture through remote access software,

- require remote access software not be allowed to remain resident on computer systems. It should be loaded only as required, with specific concurrence from both parties at the time, and then removed when the session is completed. At that time, a complete disk scan should be done to check for viruses, including any diskettes used in the session.

7.7.14 Software provided to customers

- Financial institutions sometimes provide software to customers for the purposes of serving that customer or will interact with a customer who uses one of a number of software banking programs available for sale. This subclause treats software provided by the institution. The next treats use of commercial packages.

To prevent unauthorized destruction or modification of software distributed to customers,

- create and secure a dedicated environment for the creation of customer diskettes. This should include physical and logical controls on the hardware, software, and diskettes used for the creation, copying, and protection of the customer software master copies. As an alternative, restore the copying hardware and software to a "diskette creation state" prior to each creation session.

- require a written statement from vendors of software being provided to customers that best efforts were made to protect the software against viruses and other unwanted code.

To protect the institution against claims of negligence due to use of institution-provided software,

- require that all software controls applicable to institution software also apply to software provided to customers. The institution should also develop control requirements and guidelines for all departments issuing software to customers. This should include software developed within the institution, third-party software that may be legally distributed to customers and a combination of both internally developed and third-party software "packages."
- execute an agreement with customers to whom software is provided that enumerates each party's responsibilities, required security duties, and limits on liability.
- maintain sufficient documentation to prove that the institution-provided software was not the cause of viruses or other malicious code, if encountered.

7.7.15 Software used to contact customers

The growth of computer banking has lead to customers communicating with financial institutions via commercial banking packages, such as INTUIT™ and QUICKEN™. Configuration management of the software product is beyond the power of financial institutions. Competitive

pressures force financial institutions into providing service in this way.

To limit liabilities or losses due to computer banking,

- ensure that liability for security breaches are clearly spelled out in service provider agreements.
- ensure that security policies of your service provider are compatible with that of the institution.

7.7.16 Applets, JAVA, and Software from External Sources

Care should be taken to preclude software being introduced into the institution's domain through software down-loaded without the specific request or the express consent of the institution. As an example, Internet service providers will often download software to their customers. America Online call this "art."

JAVA, a language specifically aimed at creating applications that can be remotely accessed and run also represents a path for software not requested by a customer to become resident in a computer.

To prevent unauthorized software from appearing in the institution's system

- limit the connectivity to the Internet to the minimum required for conduct of business.
- install a firewall between internal networks and the specific Internet sites authorized for access. (see 7.6.11)

- require that either the firewall include virus scanning, or ensure that any executable file is virus scanned before it is introduced to the institution's network.

- include liability considerations in any contract with such providers.

7.8 Human factors

The work force is one of the most important assets of a financial institution. In a service economy where total quality management is being stressed, employees are very important for the success of the institution.

Humans are essential ingredients in any successful information security program. They are the first line of defense, helping to make the technology function as it should, spotting security problems, and helping security awareness to succeed.

On the other hand, human beings also commit computer crimes. They can misuse the technology. Humans make mistakes.

At a minimum, institutions should consider ways to mobilize their human resources in order to achieve security in all areas of the institution, while developing techniques to minimize the opportunities for people to commit crimes.

Certain positions in an institution may be particularly sensitive because of exposure of sensitive information, or may be "key" because of powerful privileges or capabilities associated with the position. Personnel selection for these positions should include a very thorough background investigation.

Regulators in some countries have encouraged institutions to "Know Your Employee." The controls listed below represent controls relating to employees.

7.8.1 Awareness

To educate employees in their information security duties, and to impress them with the importance of information security,

- inform all directors, officers, managers, employees, and contractors that information in any form is an asset of the institution and shall only be used to conduct official business.
- establish, as part of the information security program, a communications and awareness program to inform employees of the importance and seriousness of information security.
- establish policies that assign and enforce responsibilities for information security issues. Employees should be made aware that security violations may lead to disciplinary measures.
- have employees acknowledge their responsibilities. Clause A.3, Sample Employee Awareness Form, is a vehicle for obtaining such as acknowledgment.

To further minimize risk of loss,

- establish a "clear desk" policy for papers and diskettes. Any material not in use should be properly stored.

7.8.2 Management

To utilize managers as a part of sound information security awareness,

- encourage managers to treat information security concerns of employees seriously, so as to encourage their participation.
- encourage managers to make employees

aware of the sensitivity of the information they use on the job. For example, customers should not overhear a discussion of whether or not a loan should be approved.

- encourage managers to be aware of unusual behavior by employees and seek assistance from human resource department.
- consider effects on employee behavior in setting employment and management policies.
- to the extent possible make managers and employees aware of downsizing, merger or acquisition plans and have a source of reliable information to counteract destructive rumors.

7.8.3 Unauthorized use of information resources

To prevent disclosure, destruction, or modification of information through unauthorized use of information resources,

- make available to all personnel policies covering the permissible non-business uses of personal computers and other information resources. This policy should clearly address removal of information or equipment from the premises.

7.8.4 Hiring practices

To ensure that hiring practices are consistent with the information security program,

- employ prudent hiring practices that include checking for possible security exposure, if legally permissible.

7.8.5 Ethics policy

To avoid conflict of interest, and to ensure ethical behavior,

- establish an ethics policy consistent with the information security program of the institution.
- monitor compliance with special attention to employees in sensitive positions.

7.8.6 Disciplinary Policy

To ensure that employees understand the consequences of any deviance from the security policy or standards,

- establish a written disciplinary policy.

7.8.7 Fraud detection

To assist in detecting on-going defalcation schemes,

- require that every employee be away from the institution for at least two consecutive weeks every calendar year, whenever leave policy allows. During this time their USERID should be suspended. Persons replacing the employee should notify management if any security-related abnormalities are noted.
- perform unannounced rotation of personnel involved in SENSITIVE or HIGHLY SENSITIVE activities from time to time.
- implement strong controls over the five end points through which embezzlers must pass to remove the proceeds of the fraud. These end points are official checks, wire transfers, credit to accounts or avoidance of debits, cash, and items of value received or delivered.

7.8.8 Know your employee

To assist employees in handling personal problems that might result in possible information security exposures,

- provide employee assistance to address concerns including substance abuse, gambling, and financial difficulties.

7.8.9 Former employees

To prevent unauthorized access by former employees,

- terminate immediately all access that an employee possessed upon dismissal, retirement, resignation, or other departure. The USERID assigned to the employee should not be reissued.
- retrieve all identification, badges, keys, access control tokens, and other security-related items, as well as institution supplied equipment.

7.8.10 Telecommuting

Telecommuting, or the policy of allowing individuals to work from their home or a location other than the traditional office, may be beneficial to both institution and employee. Care should be taken to determine if the functions performed by the employee can be properly carried out away from the traditional office.

To address security issues for telecommuters,

- Allow an employee to telecommute only after consideration is given to the employee's interpersonal skills, communication skills, and ability to work in an unsupervised environment.
- Establish and distribute a clear written policy on telecommuting. (A sample Telecommuting Agreement may be found in clause A.8)
- Require any employee who wishes to telecommute to execute a written agreement which addressed the following issues:
 - Equipment to be used: bank or employees.
 - Phone lines: separate or employee's
 - Maintenance
 - Costs and reimbursements
 - Supervision
 - Liability for personal injury, fire, etc.
 - Physical and logical security to include protection of equipment, information transmitted or stored, hardcopy, back-up of information, disposal of hardcopy and diskettes, and protection of networks.

7.9 Voice, telephone, and related equipment

Information is carried by voice so frequently that it is easy to forget that security controls apply. The first part of this subclause deals with the spoken word, the telephone, and VoiceMail. Voice Response Units, that synthesize the human voice are discussed in the second half of this subclause. This discussion is meant to cover voice related information used in the conduct of business, not purely social conversation.

Institutions utilizing Voice Mail Systems are subject to a variety of potential threats and exposures including disclosure of messages, liability for substantial long distance charges, and even loss of service due to unauthorized accesses. It is important for the Information Security Officer to be involved in the review and implementation of appropriate controls offered by the vendor in order to reduce or eliminate these exposures. Controls that should be used to protect voice and related information are as follows:

7.9.1 Access to VoiceMail system

To preserve integrity of information residing on VoiceMail, and limit expenses and liability for unauthorized use of VoiceMail services,

- control access to VoiceMail service with physical controls listed under 7.5.1, and with logical access controls listed in 7.2.

7.9.2 Private Branch Exchange (PBX)

A PBX is an internal switch for attached telephone units within an institution, that usually supports connections to outside telephone lines, and may also support electronic switching of information to attached computer devices.

To protect the PBX systems from being used to place outside calls by unauthorized sources, and

To protect the information that passes through electronic PBX systems from unauthorized disclosure, modification, or destruction,

- maintain close liaison with PBX supplier and network service providers concerning emerging frauds and other problems.
- provide physical access controls that restrict access to the PBX to authorized individuals.
- protect any maintenance or administrative ports that are accessible via remote dial-up, with passwords meeting the access control criteria in 7.2, and where practical, require secure call-back or challenge/response procedures.
- produce an audit trail of all administrative and maintenance access.
- change all default password settings immediately upon installation of a PBX.
- follow approved change control procedures, documenting all changes. See discussion of change control in 7.4.
- use call accounting software.
- prevent access to local "hot numbers" or other expensive services.
- follow least privilege on setting facilities for particular extensions, e.g. deny international access unless explicitly authorized.

7.9.3 Spoken word

To educate employees to the sensitivity of information being discussed regardless of circumstances,

- advise employees periodically and whenever necessary, to be aware of who is present during conversations involving SENSITIVE or HIGHLY SENSITIVE information. Whenever SENSITIVE or HIGHLY SENSITIVE information is to be discussed, an announcement to that effect