TECHNICAL REPORT

ISO/TR 13569

Second edition
1997-10-01

Banking and related financial services — Information security guidelines

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

Reference number
ISO/TR 13569:1997(E)

Contents

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

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 Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.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 businss 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 USERIDs 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 stactically 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 structures 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 form 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 through 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

should be made, unless it is clear that persons who are party to the conversation or meeting are aware of the sensitivity of the information.

7.9.4 Intercept

Interception of cellular and cordless telephone conversations is easy to do, and in some cases is legal.

To protect against interception of HIGHLY SENSITIVE information during telephone transmission,

- consider encrypting telephone calls in which HIGHLY SENSITIVE information will be discussed.
- prohibit use of cordless or unencrypted cellular telephones for transmission of HIGHLY SENSITIVE information, except in emergencies.

7.9.5 Business continuity

To ensure the continued availability of VoiceMail and telephone service,

- include telephone and VoiceMail service continuation as part of the contingency and disaster recovery plans.

7.9.6 Documentation

To preserve a record of transaction requests, and to prevent action on unauthenticated requests,

- verify transaction requests received from outside the institution via telephone or VoiceMail, by callback, Cryptographic Authentication, or other means approved by the Information Security Program, except as noted below.
- require that telephone transaction requests that are part of business activities traditionally conducted over telephones, such as foreign exchange or arbitrage, be conducted on recorded telephone lines. Recordings should be retained at least as long as the statute of limitations for any legal action or crime that may arise from the transactions in question.

7.9.7 Voice Response Units (VRU)

Voice Response Units are becoming increasingly popular as a means to allow customers effective and efficient telephone access to their accounts without human intervention. This access may be as simple as an account balance inquiry, or may include a wide range of capabilities such as the transfer of funds between accounts, making loan payments, or stopping payment on one or more checks.

To provide a high degree of assurance that the accounts will only be accessed by the true owners and no one else,

- require use of customer selected Personal Identification Numbers (PINs).
- notify all account owners of the PIN selection process.
- provide the ability for the owner to block the account from service.

NOTE — Normal security practice requires encryption of transmitted PINs. Transmission of PINs without encryption, or protected by masking tones, white noise, or similar techniques, may be acceptable in certain low risk applications. PINs used in an application not requiring encryption should be limited to that application.

To protect customer PINs after acquired by the VRU,

- encrypt PINs, once received by the VRU, prior to validation by the VRU or any other system to which they may be transmitted.

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

- allow callers at least two, but no more than three, consecutive attempts to enter a valid identification or authentication code or account number before either transferring the caller to a human operator or terminating the call. In addition, these entries should be logged and reviewed on a regular basis so that suspicious behavior may be identified.

7.10 Facsimile and image

An image is a pictorial representation of a physical document. The physical document may or may not exist on paper.

Image technology may be as simple as a fax machine creating a copy of a letter at a remote site or as sophisticated as a totally paperless image processing system with image files transmitted via E-Mail.

The following controls should be implemented.

7.10.1 Modification

To prevent possible payment on fraudulently altered facsimile images,

- require independent verification by prearranged method of the authenticity of source and contents of transaction requests

received via facsimile or image system prior to action being taken.

7.10.2 Repudiation

To prevent false claims of message receipt or denial of message delivery,

- apply non-repudiation controls, such as digital signatures.

7.10.3 Misdirection of messages

To reduce disclosure of SENSITIVE or HIGHLY SENSITIVE information through misdirected facsimile transmission,

- exercise care in dialing fax numbers. A check of the fax display for the identity of receiver should be done.

To detect fax messages that were misdirected, and to assist in the retrieval of information,

- display warning notices on fax coversheets similar to those found in clause A.5.

7.10.4 Disclosure

To prevent disclosure of information during transmission,

- encrypt fax and image transmissions carrying HIGHLY SENSITIVE information.

To prevent disclosure of information by unauthorized viewing of unattended facsimile equipment,

- locate facsimile machines and image processing terminals within areas under physical access control.

- prohibit fax transmissions carrying SENSITIVE or HIGHLY SENSITIVE information, unless it is determined by independent means that a properly authorized person is present at the receiving terminal. One method of doing this is to send the cover sheet only, wait for telephonic acknowledgment of its receipt, then resend the entire package using the redial button on the fax device.

- classify and label documents in image systems or received via fax using the same criteria used for paper documents. Documents should bear markings appropriate to their classification.

The use of cellular facsimile raises potential disclosure concerns.

To protect against disclosure of fax sent via cellular connections:

- prohibit transmission of cellular fax of SENSITIVE or HIGHLY SENSITIVE information unless encryption is in use.

7.10.5 Business continuity

To ensure against business interruption due to loss of image systems,

- include image systems and fax capability as part of the contingency and disaster recovery plan.

7.10.6 Denial of service

To minimize loss of service caused by junk fax or unsolicited and unwelcome messages,

- prohibit disclosure of fax numbers outside the institution except on a need-to-know basis.

NOTE — fax lines that the institution may want to establish for solicitation of business should not be used for other purposes.

7.10.7 Retention of documents

To prevent the loss of necessary business records including fax on thermal paper and stored image where source documents are not available,

- store image or fax information on media that prevent its modification if required as a source document. It should then be stored, or a separate copy made, kept off-line, and retained.

7.11 Electronic Mail

Electronic Mail (E-Mail) is a store and forward message system for transporting information between two or more parties.

Although E-Mail was originally developed to support informal communications over computer systems, E-Mail is now often integrated with word processing systems, so that a sender can compose a formal letter and have it instantly transmitted. E-Mail may also incorporate digitized voice messages and images. E-Mail may operate over public or private networks, such as INTERNET, X400, X500.

Controls that should be implemented to protect E-Mail are as follows:

7.11.1 Authorized users

To ensure that only authorized users access E-Mail,

- restrict access to E-Mail capability by logical access control as specified in 7.2.

7.11.2 Physical protection

To prevent modification, disclosure, or destruction of information, and information processing capabilities through access to equipment providing E-Mail services,

- restrict physical access to information processing resources supplying E-Mail applications to those personnel necessary for the operation of the system. A record of entry and exit to the facility should be maintained.

7.11.3 Integrity of transactions

To prevent unauthorized transactions or repudiation of transactions,

- obtain independent verification of authenticity as to source and content prior to completion of transactions requested via E-Mail.

7.11.4 Disclosure

To protect against disclosure of SENSITIVE or HIGHLY SENSITIVE information on E-Mail systems,

- label information that is SENSITIVE or HIGHLY SENSITIVE using the same criteria as used for paper documents.

- prohibit the transmission of HIGHLY SENSITIVE information over E-Mail, unless encrypted.

To minimize the chances of misdelivery, and minimize the ensuing consequences,

- require that E-Mail messages carrying SENSITIVE or HIGHLY SENSITIVE information be checked for correct addressing and routing information. Use of warning message similar to those shown for fax in clause A.5 should be considered.

- select public network providers from those who provide protection against misdelivery.

7.11.5 Business continuity

To ensure business continuation in case of loss of E-Mail service,

- include E-Mail service continuation as part of the contingency and disaster recovery plan. See 6.6.

7.11.6 Message retention

To ensure messages required for business and regulatory reasons are safely stored and easily retrievable,

- establish a record retention program appropriate to business and regulatory requirements.

- purge unread and unsaved messages after a specified time.

To ensure that messages archived can be properly reconstructed and authenticated,

- archive public key certificates or authentication keys used during processing.

7.11.7 Message Reception

To ensure all messages are received and actioned:

- require that senders ensure their messages are received and read. Consider using an automated status checking facility.

7.12 Paper documents

This subclause deals with paper documents other than checks and currency. Checks are mentioned in 7.17, and security of currency is outside the scope of this Technical Report.

Much of the information used for decision making is first captured on paper. Most legal systems forces most contracts onto a signed piece of paper. Preprinted forms are useful for a variety of financial operations such as deposit slips, loan applications, and memoranda of telephone transfer requests. Regulators require certain reports to be submitted in writing.

The following controls should be used for protection of paper resources.

7.12.1 Modification

To prevent the modification of information received or stored on paper documents,

- prohibit the use of pencils, EraserMates, or other erasable implements for the preparation of documents used as source for payments, loans, or other transactions.

- require the use of erasure detection paper for high value documents.

- reject documents as source for any transaction that contain strike outs, correction fluid marks, or typed over text unless such corrections or additions are initialed by all signers of the document.

7.12.2 Viewing
To protect against unauthorized viewing of SENSITIVE or HIGHLY SENSITIVE information on documents,

- make employees aware of the importance of information security. Leaving paperwork containing SENSITIVE or HIGHLY SENSITIVE information open to view should be pointed out as an example of an unacceptable security practice.

7.12.3 Storage facilities
To ensure the safe storage of documents containing CRITICAL, SENSITIVE, or HIGHLY SENSITIVE information,

- provide storage facilities approved by the Information Security Officer for CRITICAL, SENSITIVE, or HIGHLY SENSITIVE documents.

7.12.4 Destruction
To ensure that information is not disclosed because of improper disposal,

- require SENSITIVE or HIGHLY SENSITIVE documents be securely destroyed. Cross-shredding and incineration, for example.

- establish a policy covering destruction of records. The type of record, its sensitivity, statute of limitations, and other applicable regulations should be used to determine a destruction date. This policy should be reviewed periodically.

7.12.5 Business continuity
To ensure that vital business records not be lost through destruction or loss of paper documents,

- include paper document and media storage as part of the contingency and disaster recovery plan. See 6.6.

7.12.6 Preservation of evidence
To ensure that transaction source documents can be located when needed,

- require that documents that are necessary as source for transactions be uniquely numbered, with all parts of a multi-part form bearing the same number. A tracking system should be used that will enable appropriate personnel to locate document parts at anytime.

- consider the use of electronic article surveillance for areas containing a concentration of documents that are accessed frequently by several authorized personnel.

7.12.7 Labelling
To further identify documents with HIGHLY SENSITIVE information,

- determine a policy on labeling of documents. There is no consensus on labeling policies. The institution should decide whether the benefits of providing notice of sensitivity are outweighed by the cost or difficulty of doing so.

7.12.8 Forged documents
To prevent acceptance of forged documents,

- train personnel responsible for processing value-bearing documents or documents used as the basis of transactions to refer documents to their supervisor immediately, if any irregularity is detected or suspected.

7.12.9 Output distribution schemes
There is a trend to replace paper documents such as reports, prospectuses, and statements with on-line access to computer systems.

To protect against unavailability or unauthorized disclosure, destruction, or modification of SENSITIVE or HIGHLY SENSITIVE information via an output distribution scheme, and to prevent unauthorized modification of reports,

- consider application of all relevant controls in clause 7 to these systems.

7.13 Microform and other media storage
Microfilm, microfiche, and mass storage media pose special concerns because of the vast quantity of information they can store, and the relative inability to readily ascertain their contents. The following controls should be put in place for the protection of this media.

7.13.1 Disclosure
To provide greater security for HIGHLY SENSITIVE information stored on magnetic media,

- encrypt storage media containing HIGHLY SENSITIVE information, or physically protect the media from unauthorized access or removal.

To prevent the disclosure of SENSITIVE or HIGHLY SENSITIVE information on microfilm or microfiche,

- attach labels indicating the highest classifications of information that is stored on a microfilm or microfiche. This label should be clearly visible.

7.13.2 Destruction
To prevent destruction or disclosure of information through unauthorized removal of storage media,

- control access to areas containing a concentration of information storage media. In addition, consideration should be given to the use of electronic article surveillance security systems.

7.13.3 Business continuity
To ensure continued availability of information stored on microfilm, microfiche, or mass storage media,

- include microfilm, microfiche, and mass storage media as part of the contingency and disaster recovery plan. See 6.6.

7.13.4 Environmental
To prevent destruction of information through loss of storage media due to environmental problems,

- provide adequate fire protection and environment control for storage sites.

7.14 Financial transaction cards
Financial transaction cards are a means to access an existing account or a pre-approved line of credit. The terms debit card and credit card are used for account access and line-of-credit access respectively. They may be used in the purchase of goods from merchants who have agreed to accept the card in exchange for goods, or as a means to acquire cash.

Financial transaction cards may be magnetic stripe cards, which may store information on magnetic media or "smart cards" which may process information as well as to store it. Since smart cards have more flexibility than stripe cards, other uses for these cards may be developed in the future. ISO 10202 defines security measures for smart cards. Please refer to ISO 10202 for security concerns for smart cards.

Financial card associations maintain their own minimum security standards for financial institutions and contractors providing services to financial institutions. In addition to those security programs, institutions using financial transaction cards should employ the controls listed below.

7.14.1 Physical security
To protect against the destruction, disclosure, or modification of transaction card information while in the processing stages,

- locate facility in an area regularly patrolled by public law enforcement services and served by fire protection services. The facility should be protected by an intrusion alarm system with auxiliary power.

7.14.2 Insider abuse
To prevent fraudulent transactions being made through access to card information,

- store all media containing valid account information, including account numbers, PIN numbers, credit limits, and account balances in an area limited to selected personnel.

- keep the production and issuing function for cards physically separate from the production and issuing function for PINs.

7.14.3 Transportation of PINs
To prevent losses through the use of PINs having been intercepted by unauthorized persons,

- handle PINs in accordance with ISO 9564, Personal Identification Number (PIN) Management and Security, or ISO 10202, as appropriate.

7.14.4 Personnel
To prevent the assignment of unsuitable personnel to credit card processing duty,

- conduct credit and criminal record checks for all employees handling embossed or unembossed cards, including part-time and temporary employees, where permissible by law.

7.14.5 Audit
To ensure the integrity of control and audit information,

- require that controls and audit logs be maintained for printed plastic sheets, plates, embossing and encoding equipment, signature panel foil, holograms, magnetic tape, semifinished, and finished cards, sample cards, cardholder account numbers information, and waste disposal equipment.

7.14.6 Enforcement
To ensure continued compliance with security standards and maintenance of Audit Control Logs,

- appoint at least one person to serve as the prime security officer responsible for performing security functions.

7.14.7 Counterfeit card prevention

To prevent information disclosed on sales drafts from being used to produce counterfeit magnetic stripe cards,

- encode cryptographic check digits on the magnetic stripe, and validate these digits on as many transactions as possible.

To prevent intercepted information from being use to produce counterfeit cards,

- use physical Card Authentication Method (CAM) to validate the authenticity of cards.

7.15 Automated Teller Machines

Automated Teller Machines (ATM) are those devices that allow a customer to check account balances, make cash withdrawals, make deposits, pay bills, or perform other functions that are generally associated with tellers. These devices may be inside an institution's buildings, attached to the outside of such a building, or remote from any institution office.

Additional precautions to reduce robbery of customers and vandalism to the machines are recommended, but beyond the scope of this Technical Report. Manufacturers of these devices and ATM network providers generally publish security guidelines for the use of ATMs These documents should be consulted. Also see 7.14 on transaction cards.

7.15.1 User identification

To provide assurance that users of ATMs are authorized,

- require the use of Personal Identification Numbers (PINs) to activate the ATM.

- educate users to understand that PIN secrecy is their responsibility.

To prevent unauthorized transactions caused by guessing the PIN of a card being used by a non-authorized person,

- limit the number of tries for entry of a PIN to three attempts. Capture the card used in such an attempt and contact the owner to ascertain the nature of the problem.

7.15.2 Authenticity of information

To prevent the unauthorized modification of information transmitted to and from ATMs,

- require the use of a Message Authentication Code (MAC) for each transmission.

To prevent unauthorized modification, destruction, or disclosure of information residing in an ATM,

- require physical access control to the interior of ATMs be consistent with physical protection controls on containers of currency.

7.15.3 Disclosure of information

To prevent the unauthorized use of ATMs or Point of Sale terminals through the unauthorized disclosure of information,

- encrypt within the ATM or smart card in use any PIN introduced into the ATM prior to transmission. Consider encrypting all information transmitted from the ATM.

- manage PINs in accordance with relevant ISO standards.

7.15.4 Fraud prevention

To detect and prevent fraudulent use of ATMs, such as kiting schemes, empty envelope deposits, and disavowed transactions,

- limit the number of transactions and amount of funds withdrawn per day per account.

- balance the ATM under dual control daily.

- install video cameras if fraud experience or potential warrant.

- maintain operation of ATMs on-line whenever possible, i.e., require that the ATM have the ability to check account balances prior to completing transaction.

If on-line operation is not possible,

- establish more stringent card issuance requirements than would be used if operation were on-line.

7.15.5 Maintenance and service

To prevent unauthorized access to information during maintenance and servicing of ATMs,

- ensure that ATMs as placed "out-of-service" to customers prior to any maintenance being performed.

- establish dual control procedures for the servicing of ATMs involving opening of the vault.

7.16 Electronic Fund Transfers

Security issues surrounding Electronic Fund Transfers have been discussed under various subclauses above. This subclause reexamines threats and controls from the perspective of fund transfer applications, independent of technology used. Controls on message preparation prior to transmission and handling of messages once received are not covered.

7.16.1 Unauthorized source

To prevent loss through the acceptance of a payment request from an unauthorized source,

- authenticate the source of messages requesting funds transfer, using a security procedure specified in customer or correspondent agreement. Cryptographic Authentication is recommended whenever feasible. Cryptographic Authentication is provided by a Message Authentication Code generated under ISO 8730 with a cryptographic key distributed under ISO 8732. Alternatively, successful decryption of a message encrypted under ISO 10126 with a key distributed under ISO 8732 may be used to establish authenticity of the source of the message. Digital signature may also be used.

7.16.2 Unauthorized changes

To prevent an improper payment due to changed message contents, whether intentional or accidental,

- authenticate at least the CRITICAL contents of a message, using a security procedure specified in a customer or correspondent agreement. Full text authentication should be used whenever practical. Cryptographic Authentication is recommended.

7.16.3 Replay of messages

To prevent an unauthorized repeated payment caused by a replayed message,

- require the use and verification of unique message identification. Include this identification in any authentication performed.

7.16.4 Record retention

To preserve evidence that may be needed to prove authorization in making a payment,

- record messages requesting transfer of funds regardless of media used to transmit messages. Material necessary to prove authentication, including supporting cryptographic material, should be preserved.

7.16.5 Legal basis for payments

To ensure that payments are being made in compliance with a signed agreement,

- establish a system that will ensure that agreements underlying EFT requests are in place and current.

7.17 Checks

Checks, also known as Negotiable Orders of Withdrawal, or Share Drafts, are written orders directing a financial institution to pay money. Several new approaches to processing checks should raise security concerns to financial institutions. Check-image and other truncation schemes are examples of techniques that generate security concerns.

Subcommittee B of X9 (USA) has published standards on many aspects of check processing operations. Particular attention is drawn to ANSI X9/TG-2, Understanding and Designing Checks and ANSI X9/TG-8, Check Security Guideline To achieve consistency among financial institutions and improved processing performance, financial institutions are strongly urged to follow the recommendations of X9/TG-2 and TG-8.

7.18 Electronic Commerce

Electronic commerce, the provision of financial services over the Internet is a relatively new phenomenon. Whether these services are provided directly or with the assistance of a service provider, all usual security concerns which must be addressed. Some security areas which may be of special concern are addressed in this subclause.

7.18.1 New Customers

The requirement to "Know Your Customer" poses special challenges when your services are delivered through cyberspace. While it may be desirable to advertise services using a Homepage or other electronic medium, a personal visit to a financial institution's place of business should be a prerequisite to opening a new account until a universally recognized and enforceable electronic method of positive personal identification is discovered. Normal customer qualification procedures should be observed.

7.18.2 Integrity Issues

Each transaction should be protected to ensure identification of user, authenticity of user, authenticity of message, confidentiality of sensitive information, and non-repudiation of instructions.

Transaction requests should be digitally signed using a key authenticated by the institution's certification authority. Properly implemented, this should provide assurance that the user is identified,

the message contents unchanged, and the user is legally bound to his or her actions.

Account numbers, PINs, or other information which, if revealed, would allow unauthorized use of an account, should be protected with encryption.

7.19 Electronic Money

The following controls are taken from Security Of Electronic Money, published by the bank of International Settlement, Basle, August 1996.

To prevent against attacks on electronic money systems,

- employ devices tamper-protection against analysis and non-authorized changes,
- employ cryptographic authentication of devices and transactions,
- employ cryptographic protection for data confidentiality and integrity.

To detect attacks against an electronic money system,

- collect transaction details for verification of financial and security data,
- require connection with central system, at least periodically to collect and verify transaction logs.
- limit transferability of stored-value balances to speed detection of fraud,
- analyze payment flow statistics
- maintain suspicious card lists and make available to merchants.

To contain security risks,

- establish a limit on stored value,
- establish a limit for transaction amounts,
- set expiration dates,
- link devices to an account,
- establish a procedure to shut down the system in case of large-scale fraud is detected.

To maintain overall security,

- establish strict manufacturing and software development procedures,
- contract for third-party security evaluation of components and procedures,
- clearly define responsibilities of all participants
- strictly control initialization, personalization, and distribution of devices,
- audit the system regularly.

7.19.1 Duplication of Devices

To prevent duplication of devices,

- protect software and hardware design information,
- employ devices whose essential parts are physically protected against optical and electrical reading,
- logically protect secret data in the token through encryption or scattering.

To detect duplication of devices,

- register devices
- assign a unique identification number and cryptographic key to each device
- authenticate devices at each transaction,
- monitor devices whenever connected to central operator.

To contain losses due to duplicated devices,

- publish list of suspicious cards and make list available to merchants,
- permit blocking of devices from central system.

To provide additional protection due to duplication threats,

- separate the manufacturing process from the initialization, personalization, and distribution of devices,
- establish a separation of duties with each organization,
- contract for third-party security evaluation of devices.

7.19.2 Alteration or duplication of data or software

To protect against alteration or duplication of data or software,

- store data and software in tamper-resistant devices
- monitor tamper-evidence whenever possible
- require on-line authorization on detection of suspicious parameters
- require ability to block device from central system
- allow loading of security parameters from central system.

To detect duplication of electronic notes,

- require central verification of notes.

To prevent or detect creation of unauthorized electronic notes,

- require notes to be cryptographically certified by the issuer,
- require on-line verification.

To prevent or detect unauthorized creation of transactions,

- require transactions be digitally signed by key unique to device.
- require on-line authorization of transactions,
- require devices mutually authenticate,
- verify transaction sequence numbers,
- maintain shadow balance accounts,
- monitor for unusual payment patterns.

To protect or detect unauthorized alteration of operating system software or static data,

- store critical software and data in a physically protected memory and logically protect with encryption or scattering,
- create and verify software checksums.

To prevent or detect unauthorized alteration of electronic value balance,

- allow balance modification be performed only by authorized devices,
- maintain shadow balance.

7.19.3 Alteration of messages

To prevent unauthorized modification of messages,

- require challenge-response mechanisms to initiate transactions
- require use of derived session key to exchange messages
- verify message integrity by MAC of hash
- authenticate messages by MAC or digital signature.

To detect unauthorized modification of messages,

- verify electronic signatures
- verify transaction sequence numbers
- verify time-stamps

7.19.4 Replay or duplication of transactions

To prevent or detect replay or duplication of transactions,

- require unique session keys be used,
- require use of PIN for load and deposit truncations,
- verify transaction sequence numbers
- verify time-stamps,
- maintain shadow balances,
- monitor for unusual payment patterns.

7.19.5 Theft of devices

To prevent theft of devices and to contain losses from theft,

- require use of PIN for load transactions
- actively poll cards whenever possible
- allow users to lock cards with PIN
- allow cards to be blocked by issuer
- set transaction or card value limits

7.19.6 Repudiation

To prevent truncations from being repudiated,

- require issuer to log transactions,
- allow cardholder to check a number of transactions from card,
- time-stamp and sequence number transactions,
- require merchant and client to cryptographically sign transactions,
- employ a reputable Certification Authority.

7.19.7 Malfunction

To protect against loss due to malfunction,

- structure protocols such that transaction are either successfully carried out or canceled,
- require cards and devices log any errors detected,
- set a maximum number of errors after which the card will be forced to connect to central operator.

7.19.8 Cryptographic Issues

To prevent theft of cryptographic keys,

- employ tamper resistant devices,
- generate secret keys in secure environment,
- encrypt any secret key transported over network, or use asymmetric systems.

To protect against consequences of theft,

- maintain list of compromised keys,
- allow for periodic and emergency change of keys,
- establish expiration date for all keys
- strict key management is employed,
- employ third party evaluation of cryptosystems,
- subject system to external audit,
- use published algorithms.

7.19.9 Criminal Activity

To detect criminal activity and to contain damage from such activity,

- uniquely identify truncations,

- require digital signature of truncations,
- verify and authorize load or payment transactions on-line,
- force devices to interact with banking system,
- investigate specific payment patterns,
- set limits for transferability of value,
- set limits for truncations
- require devices holding value to be registered and linked to an account,
- know your customer,
- check criminal records of customers and merchants (where possible and relevant),
- monitor institutions participating in electronic money systems.

7.20 Miscellaneous

No matter how carefully one plans, there is always a security concern that is not obvious until it becomes a problem. Two emerging concerns in particular illustrate the variety of security concerns that may unexpectedly arise: Year 2000 and Steganography.

7.20.1 Year 2000

The current concern over Year 2000 is one example. Many institutions are relying on systems developed at a time when memory was at a premium which uses only 2 digits for the year. Exactly how the system will react after December 31, 1999 will vary from system to system.

While this may be thought of as a business problem rather than security issue, considerable risks are involved. Security planning should be part of any Year 2000 response.

7.20.2 Steganography - Covert Channels

Steganography is the hiding of information within another media. It is a practice that can be traced back in history. A classical example; using the blades of grass in a landscape picture to Morse Code encode a message. With the advent of cheap bandwidth, multimedia transfers of digitized pictures, movies, sound bites, et cetera raises the possibility of moving information of all sorts through a covert channel. Some commercial products are available which allow this to happen, and the techniques are well known in the computer community.

While many existing financial applications make efficient use of bandwidth, leaving little redundancy for covert transmission, new technologies may introduce the opportunity for steganographic activity. For example, an institution may want to display its logo, or perhaps a picture of its headquarters or CEO on its Home-Banking-On-the-Internet product. Sending images of checks or other documents as a graphic file may become feasible.

What concerns arise from Steganography? The existence of a vehicle for covert channel exposes the institution to several concerns. Among them are

Unauthorized release and transmission of business information,
Unauthorized loading of malicious code into the processing system.

To prevent the use of steganographic tools on the institution's information processing system,

Employ digital signatures wherever possible to detect changes in graphic, voice and multimedia files. Care must be taken to ensure that signatures are applied before the opportunity to apply steganographic tools.

Maintain strict configuration control on all information processing platforms.

Conduct periodic checking for the presence of steganographic tools.

Establish and maintain a policy on the use of multimedia files, or any other file with high degree of redundancy and ensure that the possibility of stenographic usage is considered in risk analysis.

8 IMPLEMENTING CRYPTOGRAPHIC CONTROLS

The growth in information technology has made the traditional methods of controlling information much more challenging. The popularization of cryptographic devices has provided the opportunity for financial institutions to recapture the level of security previously associated with banking, while also reaping the benefits of increased information processing technology.

Like any emerging technology, there is a danger of misapplying cryptographic solutions. This clause will present information to allow for institutions to make appropriate decisions on the selection, use and continuing evaluation of their cryptography-based controls.

It is assumed that the need for a cryptographic control has been identified. The controls suggested in clause 7 include encryption, MAC, and digital signature. Each of these services also require either key management or certification services. The following five subclauses will discuss each of these functions.

8.1 Applying Encryption

8.1.1 What To Encrypt

Information requiring confidentiality protection should be encrypted if

- the information will appear outside the direct control of the institution
- the information is to be stored or transported on removable media
- the information is to be transmitted over telephone, fax, or computer networks.

Information not requiring confidentiality protection should not be separately encrypted. Encrypted text that can not be recovered represents a potential catastrophe. If the institution uses link encryption (see below) it may be more cost effective to encrypt everything on a given link.

8.1.2 How To Encrypt

Several issues require resolution to determine how best to encrypt. These include: hardware versus software encryption products, end-to-end, or local encryption, placement in the OSI model, and key management issues. Since key management will be an issue for all cryptographic services, it will be dealt with in greater detail in 8.4.

8.1.2.1 Hardware Versus Software

Encryption products exist in either hardware or software form. Hardware devices can be stand-alone devices which attach to a communications port, or a microcircuit built-in electronic equipment. Software encryption products can be individual products which encrypt any file you send them, or can be integrated into other applications.

Use hardware encryption products:

- when assurance is required that the encryption product is operating as specified
- whenever possible

Use software encryption products when:

- cost is a major factor
- assurance that the encryption product is operating as specified is not a major issue and
- compensating controls can verify that the software is operating as specified. For example, customers who will not accept additional hardware in their systems may request cryptographic services within a software package. In this case, a certain amount of assurance can be achieved if these application communicate with hardware cryptographic devices.

8.1.2.2 End-to-End, Link, or Local Encryption

End-to-end encryption is the encryption of information from its source, with decryption at the destination. Protection is provided along the entire transmission path. Each potential user must have encryption capabilities, and be supplied with key management services. Link encryption operates on all traffic passing between two facilities.

Use link encryption when

- significant communications exists between facilities,
- other controls protect information within a building or campus,
- controls are in place to ensure that information in need of protection will be routed over the designated links.

Use end-to-end encryption when

- communicating between one or more central facilities and individual users,
- a small number of users are involved within a given enterprise,
- protection is required end-to-end, or
- link encryption is not warranted.

Use encryption in local mode when

- information is to be protected in storage by an individual user.
- key management prevents unauthorized use of the encryption facility.

8.1.2.3 The OSI Layer

If the institution has organized its information processing system according to the OSI interconnection model, placement of encryption services is determined by selecting a layer. The OSI model divides information processing as follows;

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Link
Layer 1	Physical

Place encryption capability at Layer 2 when

- Link encryption is specified.

Place encryption capability at Layer 4 when

- All traffic from a given terminal is to be encrypted

Place encryption capability at Layer 6 when

- Encryption is to be treated as a service to be called from multiple applications.

Place encryption capability at Layer 7 when

- Protecting an application is specified. All ISO TC-68 security standards call for Layer 7 application.

8.1.2.4 Who Controls Encryption

Institutions employing encryption must determine who can control the use of the encryption services. Encryption is a two-edged sword. It can protect the institution's information. It can also assist a dishonest employee in stealing the institution's assets or holding a database at ransom. Hardware devices can provide significant protection against encryption of a database for purposes of extortion.

To ensure that encryption is properly controlled:

- Establish corporate policies on the use and control of encryption
- Limit control of encryption services to the most trustworthy individuals in the institution
- Establish positive institutional control over all cryptographic keying material.
- Ensure that no single individual can access keys or change keys to a value chosen by that individual.
- Use ISO 8732 for key management

8.1.2.5 Physical and Logical Security of Encryption Products

Assure that proper physical and logical security controls are applied to cryptographic products. One source of such controls is Federal Information Protection Standard (FIPS) PUB 140-1, *Security Requirements for Cryptographic Modules,* published by the National Institute for Standards and Technology (USA.)

8.1.2.6 Choice of Encryption Algorithms

To ensure the highest quality of encryption

- Only algorithms contained in ISO TC68 developed standards should be considered for use by financial institutions.

8.2 Implementing Message Authentication Codes (MAC)

ISO 8730 and 8731 specify the calculation of a Message Authentication Code (MAC) in a wholesale environment. In implementing Message Authentication, ISO 8732 should be used for key management.

8.2.2 Control of MAC

To achieve the desired security from MAC service:

- ensure that keys used for MAC be restricted to those parties who are responsible for authenticating the integrity of information.
- Use the procedures defined in ISO 8732 for key management.
- select individuals who control the authentication process with the utmost care.

8.2.3 When to Apply MAC

To obtain maximum advantage of MAC, apply MAC

- after the information to be protected is assembled and edited
- before encryption or compression is applied
- to the entire information to be sent, whenever possible.

To obtain maximum advantage of MAC, verify MAC

- after decompression and decryption
- before any action is taken on the information
- if only partial fields of a message is MAC and verified, rely only on that information.

8.2.4 Selection of Algorithm

To ensure proper MAC operation

- Allow only ISO TC-68 specified algorithm to be used.

8.3 Implementing Digital Signatures

As we automate our information processing systems, we find that paper based documents are becoming stored and processed in electronic form. Having documents in electronic form permits rapid processing and transmission and thereby improves the overall efficiency of information systems. However, approval of a written document has traditionally been indicated by a written signature. There is a need for an electronic equivalent to the written signature which would be recognized to have the same legal status. Merely digitizing the written signature -converting the signature into a series of numbers - is not an acceptable alternative, since the digitized signature bears no relationship to

the data that is being signed. Paper based documents offer some resistance to alteration and forgery. To modify a paper document one has to erase and replace text in an undetected manner. To forge a written document requires a certain amount of skill and practice. An electronic document with a digitized written signature would provide no such protection. The contents of a document could be altered without changing the signature, and the digitized signature could be replicated on other documents without detection.

8.3.1 How to generate digital signatures

Security architectures are emerging, based on public key cryptography, that will result in authentication via digital signature implementation in smart cards, or PCMCIA (Personal Computer Memory Card Industry Association) cards. These cards contain the private key associated with the individual. Thus, transactions 'signed' with the private key, can be validated by anyone with access to the individual's public key. This provides a close association between a document and an individual who possesses the authority to bind the institution to the contents of a document. Furthermore, these cards can also contain secret encryption keys used in symmetric encryption operations. As with tokens, card systems should provide PIN number entry services.

To assure that digital signatures used by the institution deliver proper non-repudiation:

- limit signature authority to those individuals entrusted to bind the institution.
- use digital signature standards accepted by TC68 or by competent national authorities.
- Ensure that parameters and keying material are properly generated and used.

8.3.2 Certification

A digital signature is a value derived from the message being signed, an appropriate cryptographic algorithm, and the 'secret' key half of an asymmetric key pair. Any party who holds the 'public' half of the key pair can verify that the holder of the 'secret' half was the party signing the message. The party verifying must have some assurance that the public key half is indeed the one associated with the signing party. This assurance is provided by certification authorities, mutually trusted third parties who can cryptographically bind an individual to his public key. The binding is generally through a certificate signed in the key of the certifying authority. Certifying authorities can exist in a hierarchy. All that is required is for both parties to a transaction to have at least one common authority in its set of relationships.

At the point at which the two parties have identified a common certification authority, that authority's public key must be well known or delivered with integrity protection, to preclude system compromise.

8.3.3 Legal standing of digital signatures

The General Accounting Office (USA) has ruled that the U. S. federal government may be bound to electronically signed transactions, using either the DSS or X9.9 Mac's. Case law exists on using marks other than a signature to indicate a willingness to enter a contract. In addition, in May, 1996, the Federal Reserve modified Regulation E to allow the use of a digital signature to validate a fund transfer request. At the time of the publication of this document, the 'Shining Star' case has firmly established that a digital signature is the equivalent of a holographic signature. Most practitioners believe such a case will arise and establish digital signature as legally binding, even in absence of a written signature.

Parties conducting business under a pre-existing contract may use digital signature for non-repudiation purposes.

8.3.4 Certificate (Key) management

In implementing non-repudiation service, the generation, control, and distribution of keying material must be accomplished in a way to maintain the security desired. Digital signatures require rather long keys. These keys will normally be stored in a smart card, security token, or personnel computer. Access to these keys and access to the signing mechanism must be carefully controlled, as signatures will result in binding the institution.

In order to prove the ownership of a public key, a binding association between the owner of a public key and that function must be documented. This binding is called a "Certificate". Certificates are generated by a trusted third party called a Certification Authority (CA).

To ensure that non-repudiation service is properly used:

- address non-repudiation in the overall information security policy for the institution
- select personnel who may be authorized to sign messages in the same manner as selection of personnel who may sign paper documents of a similar nature,
- select a certification authority with extreme care, or
- establish a certification authority for the institution.

8.3.5 Choice of algorithm

To ensure proper signature operation

- Allow only ISO TC68 specified algorithms to be used.

8.4 Key Management

As with any technology, there are elements that are relatively easy to implement and segments that pose major efforts to accomplish. One such area that requires careful planning, education, and precise implementation is cryptographic key management.

Key management is that part of cryptography that provides the methods for the secure generation, exchange, use, storage, and discontinuation of the cryptographic keys used by the cryptographic mechanism. The incorporation of cryptographic techniques like encryption and authentication into computer systems and networks can achieve many security objectives. However, these techniques are of no value without the secure management of the cryptographic keys. The major functions of key management are to provide the cryptographic keys required by the cryptographic techniques, and to protect these keys from any form of compromise. The specific procedures and security requirements for key management depend on the type of cryptosystem upon which the cryptographic techniques are based, the nature of the cryptographic techniques themselves, and the characteristics and security requirements of the computer system or network being protected. The most important element is that key management must be flexible enough for efficient use within the computer system or network, but maintain the security requirements of the system.

Key management services must be available when and where they are needed, including at back-up sites. Key management must be part of an institution disaster recovery plan.

8.4.1 Generation

To ensure that cryptographic keys may not be predictable,

- generate secret keys using random or pseudo random generation techniques, such as that found in ISO 8732.
-
- Consider central generation using a single high-quality random or pseudo random source and monitor for continuing quality of output.

To assure that asymmetric keys are properly generated:

- require tests for primality or other requirements that yield low probability of error (< .000000001) See ANSI X9.30-1997, Part 1, Appendix A.2.

8.4.2 Distribution

Key distribution involves the secure movement of cryptographic keys from the point they are generated to where they are to be used. The requirements for key distribution will depend on the nature of the service to be provided and algorithms used.

8.4.2.1 Distribution of secret keys.

Key which must be kept secret included symmetric keys and the secret key in asymmetric systems. To protect cryptographic keys during distribution

- observe all the requirements of ISO 8732, for the transport of keys.

8.4.2.2 Distribution of public keys

To ensure the validity of public keys;

- Protect keys which are used for verification of a signature or to encrypt information for ultimate decryption with a recipient's secret key against unauthorized modification or substitution.
- Enforce the use of key certificates.

8.4.3 Storage

Another area of concern is the storage of backup copies of keys in use, future and discontinued keys. Both require the ability to protect these keys from disclosure or substitution, but must also be available for access and audit by authorized personnel.

To ensure safe storage and retrieval of cryptographic keys

- enforce requirements of ISO TC68 security standards for storage and archiving of keys. (See ISO 8732)

8.4.4 Public Key Certification And Standards

To ensure that asymmetric-algorithm based systems deliver the full measure of security for which they are intended:

- require the use of a certification authority which operates using ISO TC68 approved standards
- address issues of liability in service contract with external Certificate Authorities

- require reference to revocation lists periodically or before transactions involving amounts in excess of a given limit.
- incorporate certification service with data recovery services.

8.5 Trusted Third Parties

Many markets have recognized the need for enhanced security services provided by an entity mutually trusted by other entities. These services range from increasing trust or business confidence in specific transactions to providing of recovery of information for which encryption keys are not otherwise available to authorized entities. Trusted Third Parties (TTP) is the vehicle for delivery of such services.

ISO/IEC JTC1 SC27 is in the process of determining general rules for the use of TTP. The European Telecommunications Standards Institute is also working on a Technical Report on the issue.

For the financial services industry uses TTP technology offers a vehicle by which an institution can deliver assurances between its subdivision, between itself and its customers, and between itself and its corespondent institutions. An institution may choose to set up an internal TTP function or subscribe to an external provider for TTP services.

In addition to the advice which will eventually be provided in ETSI and JTC1 documents, financial institutions desiring to use TTP services should consider the following:

8.5.1 Assurance

A TTP function, whether internally or externally provided can only add value when the users of the services are assured of its quality. Before a contract is let with a provider or operations of an internal system begins, the institution must satisfy itself that the following issues are addressed.

- Trust. Is the TTP organized, controlled and regulated in such a way that its operation can be relied upon, checked and verified?
- Accreditation. Is the TTP accredited by recognized national, regional, or international groups?
- Compliance. Is the TTP operating in compliance with accepted indusrty standards and all relevant regulation?
- Contract. Is there a legally binding contract in place covering the provision of service and addressing all the issues in this list? Are there contracts with cooperating TTPs which also address these concerns?
- Liability. Is there a clear understanding as to issues of liability? Under what circumstances is the TTP liable for damages? Does the TTP have sufficient resources or insurance to meet its potential liabilities?
- Policy Statement. Does the TTP have a security policy covering technical, administrative, and organizational requirements?

8.5.2 Services of a TTP

The services which a TTP can provide include:

- Key Management for symmetric cryptosystems
- Key Management for asymmetric cryptosystems
- Key Recovery
- Authentication and Identification
- Access Control
- Non-repudiation

This Technical Report discusses these services and their usefulness for financial service institutions throughout the text, except for Key Recovery.

Key recovery is the ability of the TTP to recover, either mathematically, through secure storage, or other procedures, the proper cryptographic key used for encryption of information using the institution's information processing resources. This function would assure an institution that it can always have access to information within its information processing resources; for example, such recovery service may be essential in disaster recovery. It may also satisfy law enforcement regulations in some jurisdictions for an institution to be able to produce such a key or encrypted information in answer to a lawful court order.

8.5.3 Network of TTPs

The TTP concept is relatively new. A network of cooperating TTP must be developed before the full potential of TTPs will be realized. Competition between suppliers may reduce costs at the risk of offering reduced levels of service or assurance. During these "growing pains" financial institutions must be particularly vigilant in insisting that their TTP maintain its assurances. Confidence in the institution and the financial service sector must be preserved.

8.5.4 Legal Issues

Financial institutions generally have higher level requirements for record retrieval. The contract with a TTP should be specific issues relating to maintenance of keys used for encryption, authentication, and digital signatures, as these may need to be reproduced many years after the transactions for which they were used.

Liability for the misfeasance, malfeasance, or non-feasance of the TTP to include direct and consequential damages must also be fully

understood and agreed upon. The TTP must have adequate financial reserves or insurance to meet any liability.

Financial institutions in many jurisdictions are obliged to protect the privacy rights of individuals, especially safeguarding personal data. These obligations are sometimes at odds with the requirement of law enforcement to access information. The contract with an external TTP, or the operating procedures of an internal TTP must address both these concerns.

8.6 Disaster Cryptography and Cryptographic Disasters

Disaster recovery planning (DRP), also called business resumption planning, is an ongoing requirement in any financial institution. Its main purpose is to assure that business functions continue to function during and after disasters, such as fire, flood, power failures, etc. DRP and cryptography interact in two basic ways.

8.6.1 Disaster cryptography

First, from the DRP perspective, cryptographic facilities, such as key management centers and certificate authorities, are one class of functions which must be brought back on-line following a disruption. Ensuring that keying material remains secure while it is made available at back-up sites is just one of the complicating factors. As an example of a complicating factor, keys for MAC of funds transfer messages may be replicated and securely stored at a back-up facility. Split knowledge and dual control may be adequate. However, the back-up site for a certificate authority should use a separate certificate root since the integrity of the signature system derives from the non-disclosure of the root key outside of the certificate authority's key generation device. ANSI X9.57-1997, Certificate Management provides guidance in this area. ISO TC68/2/7 is working on an ISO version of this document.

While cryptographic functions may place special requirements on the DRP, the continued operation of cryptographic facilities must be part of the institution's DRP.

8.6.2 Cryptographic disasters

The second nexus of DRP and cryptography is planning how to deal with events caused by or complicated by cryptographic services, especially unforeseen failures. As an example, an institution may have a up-until-now-secure access control system, yet has noticed clear signs of an intruder in the system. One possibility is that cryptography failed. There should be clear instructions on how to proceed. Without such instructions, well intentioned acts may exacerbate the problem.

Another example of a cryptographic disaster is the encryption of vital information by an employee who is now offering the proper decryption key in exchange for an immediate retirement package with a large lump-sum pension. This example may be solved through technical, law-enforcement, or negotiation method. Unless the institution planned for the technical solution, the other solutions may be expensive, embarrassing, or both.

Since no complete list of threats exists, a complete list of countermeasures is impossible. However, the information security and disaster recovery programs of an institution must address cryptographic threats, at least in generic form. A written policy should cover:

- regular monitoring of the information processing system for abnormal behavior.
- procedures to be followed in determining the cause of abnormal behavior and guidelines on how to respond to a threat, intruder, compromise, etc.
- procedures for dealing with the failure of any cryptographic control.
- provision for the availability of cryptographic services, keying material, and other related service following business interruption.

ANSI X9.57-1997, Appendix D Recommended Certification Authority Audit Journal Contents And Use, should be used as a guide.
Note also that using multiply signed certificates can ameliorate the risk of compromise of the root key of a CA.

9 SOURCES OF FURTHER ASSISTANCE

This clause is intended to be used with Annex C to identify sources which may assist security professionals in the discharge of their duties. Organizations identified by member countries are listed in Annex C. The following subclauses give brief descriptions of each type of source.

9.1 Financial Services institutions

Financial services institutions or trade organizations serving the financial services sector often publish material helpful in understanding security issues, conduct training courses and conferences, and can otherwise guide the security professional to further sources of assistance.

9.2 Standards bodies

National standards organizations can provide financial and non-financial standards on security issues. Participation in these bodies can prove

useful in learning of security concerns of others. Use of standards promote interoperability as well as help secure operations.

9.3 Building, fire, and electrical codes.
Adherence to these codes promote a safer, more secure environment.

9.4 Government regulators
Regulators can often provide assistance in securing the safety and soundness of financial institutions. Some regulators mandate certain security controls. These necessary controls can often form the basis of the bank's security program.

Glossary of terms

A term is listed in this Glossary only if it is used in this Technical Report with a connotation different from normal English usage.

Access Control: Functions which limit access to information or information processing resources to those persons or applications authorized such access.

- Physical access controls are those which are based on placing physical barriers between unauthorized persons and the information resource being protected.
- Logical access controls are those which employ other means.

Alarm: Indication of an unusual or dangerous condition or security violation which may require immediate attention.

Application: Task or set of tasks to be accomplished by the information processing system. Example: electronic funds transfer.

Audit: Function which seeks to validate that controls are in place, adequate for their purposes, and reports inadequacies to appropriate levels of management.

Audit Trail: Collection of records from an information processing facility indicating the occurrence of certain actions, used to determine if unauthorized use or attempted use of facilities have taken place.

Authentication: Process which seeks to validate identity or to prove the integrity of information.

Authentication Token: Device which performs dynamic authentication.

Back-up: The saving of business information to assure business continuity in case of loss of resources.

Biometrics: Methods of authenticating the identity of a person by measurement of some physical characteristic, such as fingerprint, retinal pattern, or voice.

Call-back: Manual or automatic procedure of contacting the originator of a request to verify that the request was authentic.

Card Authentication Method: Concept which allows unique machine-readable identification of a financial transaction card, and which prevents copying of cards.

Classification: Scheme which separates information into categories so that appropriate controls may be applied. Separation may be by type of information, criticality, fraud potential, or sensitivity.

Code:

1. System of principles or rules, such as fire codes or building codes.
2. Result of cryptographic process, such as message authentication code.
3. Software computer instructions, such as, object code (the instructions the computer executes) or source code (the instructions the programmer writes).

Contingency Plan: Procedure which, when followed, allows an institution to resume operations after natural or other disasters.

Control: Measure taken to assure the integrity and quality of a process.

Criticality: Requirements that certain information or information processing resources be available to conduct business.

Cryptography: Mathematical process used for encryption or authentication of information.

Cryptographic Authentication: Authentication based on a digital signature, message authentication code as generated under ISO 8730 with a cryptographic key distributed under ISO 8732, or inferred through successful decryption of a message encrypted under ISO 10126 with a key distributed under ISO 8732.

Cryptographic Key: A value which is used to control a cryptographic process, such as, encryption or authentication. Knowledge of an appropriate key allows correct decryption or validation of a message.

Customer Agreement: Contract with a customer which sets forth the customer's responsibilities and governs which security process will be used in the conduct of business between the institution and customer.

Destruction (of information): Any condition which renders information unusable regardless of cause.

Digital Signature: Value which can serve in place of a handwritten signature. Normally, a digital signature is the function of the contents of the message, the identity of the sender, and some cryptographic information. Digital signatures may be binding if stipulated in a customer agreement. Legal recognition of digital signatures, in the absence of a signed agreement, is expected, but has not yet occurred. At the time this Technical Report was published, digital signature standards were being developed. Since these standards were not yet completed, they have not been specified in this Technical Report.

Disclosure of Information: Unauthorized viewing or potential viewing of information.

Dual Control: Method of preserving the integrity of a process by requiring that two individuals independently take some action before certain transactions are completed. Whenever dual control is required, care should be taken to assure that individuals are independent of each other. See also Split Knowledge.

Dynamic Authentication: Technique which authenticates the identity of an individual based upon something which the individual knows on a one-time basis.

Electronic Article Surveillance: Technique which controls the movement of physical objects by means of electronic tags and sensors.

Electronic Money: Any of a number of schemes which allow value to be created, stored, or transferred in an electronic form. Conceptually it is a replacement for coins and currency.

Encryption: Process of converting information so as to render it into a form unintelligible to all except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption), against unauthorized disclosure.

Firewall: A Firewall is 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.

Freeware: Software made generally available which does not require a license agreement.

Guideline: Recommendation for information security controls to be implemented against given threats. While not mandatory, guidelines should not be ignored unless sound business and security reasons exist for doing so.

Image: Representation of a document for manipulation or storage within an information processing system. Within this Technical Report, digital representations are implied.

Information: Any data, whether in an electronic form, written on paper, spoken at a meeting, or on any other medium which is used by a financial institution to make decisions, move funds, set rates, make loans, process transactions, and the like. This definition includes software components of the processing system.

Information Asset: Information or information processing resources of an institution.

Information Resources: Equipment which is used to manipulate, communicate, or store information whether they are inside or outside the institution. Telephones, facsimiles, and computers are examples of information processing resources.

Integrity: Quality of information or a process which is free from error, whether induced accidentally or intentionally.

Irreversible Encryption: Encryption process which allows text to be transformed into encrypted form but does not allow the encrypted form to be returned into the original text.

Letter of Assurance: Document setting forth the information security controls which are in place for the protection of information held on behalf of the recipient of the letter.

Key: See cryptographic key.

"Know your Customer": Phrase used by regulators to indicate a desired attitude by financial institutions with respect to knowledge of customer activities.

"Know your Employee": Attitude of an institution which demonstrates a concern for employees' attitudes toward their duties and possible problems, such as substance abuse, gambling, of financial difficulties which may lead to security concerns.

Message Authentication Code (MAC): Code, appended to a message by the sender, which is the result of processing the message through a cryptographic process. If the receiver can generate the same code, confidence is gained that the message was not modified and that it originated with the holder of the appropriate cryptographic key.

Modification of Information: The unauthorized or accidental change in information, whether detected or undetected.

Need-to-Know: Security concept which limits access to information and information processing resources to that which is required to perform one's duties.

Owner (of Information): Person or function responsible for the collection and maintenance of a given set of information.

Network: Collection of communication and information processing systems which may be shared among several users.

Password: String of characters which serves as an authenticator of the user.

Prudent Business Practice: Set of practices which have been generally accepted as necessary.

Risk: Possibility of loss due to occurrence of one or more threats to information. Not to be confused with financial or business risk.

Risk Acceptance: Identification and acceptance of risk associated with an exception to the information security policy.

Server: Computer which acts as a provider of some service to other computers, such as processing communications, interface with file storage, or printing facility.

Shareware: Software generally available and which carry a moral, though not a legal, obligation for payment.

Sign-on: Completion of identification and authentication of a user.

Software Integrity: Confidence that the software being used performs only the functions for which it was purchased or developed.

Split Knowledge: The division of CRITICAL information into multiple parts in such a way as to require a minimum number of parts to be present before an action can take place. Split knowledge is often used to enforce dual control.

Standard:

1. Definition of acceptable practices to meet a particular defined policy.
2. A document published by a standards setting body, such as the American National Standards Institute or National Institute of Standards and Technology, which provides industry wide methods of performing certain functions.

Stored Value Card: A token which is capable of storing and transferring electronic money.

Tamper Evident Packaging: Protective packaging which will preserve an indication of attempts to access its contents.

Threat: Condition which may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the institution.

Trusted Computer System: Computer system which employs hardware and software integrity measures to allow it to be used for simultaneous processing of information having a wide range of sensitivities or classification levels.

Unavailability of Service: Inability to access information or information processing resources for any reason, i.e. disaster, power failure, or malicious actions.

USERID: Character string which is used to uniquely identify each user of a system.

Voice Mail: Systems which record and retrieve voice messages.

Annex A

Sample Documents

A.1 Sample Board of Directors Resolution on Information Security

Resolved:

Information is an asset of the corporation.

As an asset, information and information processing resources of the corporation shall be protected from unauthorized or improper use.

The Chief Executive Officer is directed to establish an information security program, consistent with prudent business practice with the goal of properly securing the information assets of the corporation.

A.2 Sample Information Security Policy (High Level)

INFORMATION SECURITY POLICY

for

THE ABC FINANCIAL INSTITUTION

ABC Financial Institution considers information, in any form, to be an asset of the corporation and requires appropriate controls to be in place to protect these assets from unauthorized or improper use. Information is vital to the efficient and effective day-to-day operation of the corporation. This information must only be used for its intended purpose -- the conduct of ABC Financial Institution's business operations. It is our corporate policy to provide access to information only on a proven "business need to know" basis and deny access to all others.

The Chief Executive Officer is responsible for appointing an Information Security Officer whose responsibility is to:

- Develop and manage a corporate wide information security program;
- Develop, issue, and maintain information security requirements in the form of policies and standards;
- Create an information security awareness program to include senior management briefings, employee training, and education;
- Create and maintain an information security officer network comprised of senior business unit managers;
- Provide information security consulting support to the business units;
- Implement a compliance assessment program to evaluate the effectiveness of the information security program;
- Collaborate with Audit on resolution of significant information security control issues; and
- Report annually to the Board of Directors or appropriate Senior Management on the effectiveness of the overall information security program.

Each ABC Financial Institution's business unit senior managers have the responsibility to maintain the confidentiality, integrity, and availability of their information assets and must comply with all policies, standards, and procedures published by the Information Security Department concerning the protection of corporate information assets.

All employees have a continuing responsibility to understand, support, and abide by all corporate policies, standards, and procedures governing the protection of information assets.

A.3 Sample Employee Awareness Form

The Corporation considers information to be an asset which should be protected.

It is my duty to understand, support, and abide by corporate policies, standards, and procedures governing the protection of information assets.

I have been given a copy of the Corporate Information Security Handbook, and agree to follow the rules in it.

I agree to use corporate information and information processing equipment to which I have access only for the purpose of discharging the duties of my job.

I understand that the institution may review any information or messages I may generate using information processing resources of the institution. This includes, but is not limited to, word processors, E-Mail systems, and personal computers.

I agree to report any suspicious behavior or situation which may endanger corporate information assets to my supervisor immediately.

I understand that misuse of corporate information assets may result in my dismissal.

Date _____

_____ _____

Printed Name of Employee Signature

_____

Witness (or supervisor)

A.4 Sample Sign-On Warning Screens

This is a private computer system with access restricted to those with proper authorization. Authorized parties are restricted to those functions which have been assigned to perform related duties. Any unauthorized access will be investigated and prosecuted to the full extent of the law. If you are not an authorized user, disconnect now.

Alternatively:

This computer system is restricted to authorized users. Unauthorized access/attempts will be prosecuted. If unauthorized, disconnect now.

A.5 Sample Facsimile Warnings

Payment Warning

WARNING

Do not rely on this transmission for paying money or initiating other transactions without independent verification of its authority

Proprietary Statement

The documents included with this facsimile transmittal sheet contain information from the ABC Corporation which is confidential and/or privileged. This information is for the use of the addressee named on this transmittal sheet. If you are not the addressee, please note that any disclosure, photocopying, distribution, or use of the contents of this faxed information is prohibited. If you have received this facsimile in error, please notify the sender by telephone immediately so that we can arrange for the retrieval of these documents at no cost to you.

A.6 Sample Information Security Bulletin

COMPUTER VIRUS ALERT

According to national reports, a computer virus known as "The Michelangelo Virus" has been spreading rapidly throughout the world and could be the most damaging virus in years. It is known to infest DOS-based systems running version 2.xx or higher.

IMPACT

This virus sits passively on infected computers until the trigger date of March 6th (Michelangelo's birthday). On that date, it overwrites critical system data, rendering the disk unusable. Data infected includes the boot record and the file allocation table (FAT) on the boot disk (whether floppy or hard disk).

Recovering user data from a damaged disk will be very difficult.

SYMPTOMS

Reported symptoms include:

- a reduction in the free/total memory by 2048 bytes, and
- floppy disks which become unusable or display odd characters during DIR (directory) commands.

It is important to note that the Michelangelo virus does **not** display any messages on the PC screen at any time.

INFECTION RISK

The virus is spread by:

- booting from an infected diskette (even if the boot is unsuccessful), or
- by booting from a hard disk while there is an infected diskette in the "A" drive and the drive door is closed.

Diskettes which are used on both business and home computers may present a higher risk than normal.

Sample Information Security Bulletin

(continued)

ACTION

If your PC has any of the above mentioned symptoms or you feel that your system is at risk, immediately contact one of the following for diagnostic assistance and virus eradication:

- your local computing services representative,
- the computing services help desk, or
- the computer virus response team.

LOCAL INFORMATION SECURITY OFFICERS SHOULD DISTRIBUTE THIS BULLETIN TO APPROPRIATE MANAGERS AND STAFF FOR INFORMATION.

A.7 Sample Risk Acceptance Form

INFORMATION SECURITY RISK ACCEPTANCE

This form should be completed only where a business process or system does not comply with the Information Security Policies and Standards, and there is no plan to comply with the policy in question in the foreseeable future.

Division _____ Requesting Unit Number _____

Unit Manager _____ Requesting Unit Name _____

Page and Item Number in Policy/Stds _____ Date _____

Risk Acceptance Requested For (describe) _____

_____

_____

_____

Description of Business Process (attach additional documentation as appropriate)

_____

_____

_____

Total number of transactions by period _____

Total dollar volume of transactions by period _____

Are transactions time dependent? (describe) _____

Are general ledger accounts affected? _____

Level of management receiving output _____

Significance of decisions based on output _____

Regulatory/legal considerations _____

Is output distributed to customers? (describe) _____

Highest classification of information processed _____

Description of System Used to Support the Business Process (attach additional documentation as appropriate)

_____

_____

_____

Describe type of equipment (number of computers, models, etc.) _____

_____

Describe type of network connectivity (LAN, VTAM, dial-up, etc.) _____

_____

Processing locations _____

Number of users _____

Geographic distribution of users _____

Describe interfaces to other systems _____

_____

Availability requirements _____

Are other applications run on this equipment? (describe) _____

_____

Are systems supported by Central Systems Group? If not, describe support arrangements.

_____

_____

Describe business/system requirements for policy compliance _____

_____

_____

Estimated cost of compliance _____

Describe current or proposed controls to mitigate risk _____

_____

_____

Estimated cost of current or proposed controls _____

Other factors to consider in this decision (other alternatives considered, additional business factors, what other companies do, etc.) _____

_____

_____

Recommended by _____ Date _____
Unit Manager

Reviewed by : _____ Date: _____
Information Security Officer

Comments: _____

_____

_____

Approved by: _____ Date _____
Senior Officer with Delegated Authority

Risk Acceptance Number (assigned by Security Officer) _____

Date of next review _____

Information Security Classification:

A.8 Telecommuter Agreement & Work Assignment

EMPLOYER - EMPLOYEE TELECOMMUTING AGREEMENT

This agreement, effective _____ is between _____ , (hereinafter referred to as "Employee"), and _____ (hereinafter referred to as "Company"). The parties, intending to be legally bound, agree as follows:

SCOPE OF AGREEMENT
Employee agrees to perform services for Company as a "Telecommuter." Employee agrees that telecommuting is voluntary and may be terminated at any time, by Company with or without cause.

Other than those duties and obligations expressly imposed on Employee under this agreement, the duties, obligations, responsibilities and conditions of Employee's employment with Company remain unchanged.

The terms "remote work location" or "remote workplace" shall mean Employee's residence or any remote office location approved by Employee's management.

TERMS OF AGREEMENT
This agreement shall become effective as of the date first written above, and shall remain in force and effect as long as Employee telecommutes, unless sooner terminated.

TERMINATION OF AGREEMENT
Employee's participation as a telecommuter is entirely voluntary and is available only to employees deemed eligible at Company's sole discretion. There exists no right to telecommute. However, when you volunteer and are selected to telecommute, Employee will make a commitment to telecommute for a period of no less than "x" months. Company will not be held responsible for costs, damages or losses resulting from cessation of participation as a telecommuter. This writing is not a contract of employment and may not be construed as such.

COMPENSATION
Work Hours, Overtime, Shift Differentials, Vacations: Employee agrees that work hours, overtime compensation, shift differentials and vacation schedule will conform to the terms agreed upon by Employee and Company.

TELECOMMUTING AND INCIDENTAL EQUIPMENT
Employee agrees that use of equipment, software, data supplies, and furniture, provided by Company for use at the remote work location, is limited to authorized persons for purposes relating to the business, including self development, training and tasks. Telecommunications equipment will be used by Employee strictly for business use. Company will in no way be responsible for telecommunications charges incurred by employee while conducting personal business.

TELECOMMUTING AND INCIDENTAL EQUIPMENT con't

The Company, at its sole discretion, may choose to purchase equipment and related supplies for use by Employee while telecommuting or permit the use of Employee-owned equipment. The decision as to the type, nature, function and/or quality of electronic hardware (including, but not limited to, computers, faxes, video display terminals, printers, modems, data processors and other terminal equipment), computer software, data and telecommunications equipment (i.e.: phone lines) shall rest entirely with the Company.

The decision to remove or discontinue use of such equipment, data and/or software shall rest entirely with the Company. Equipment purchased for use by Employee shall remain the property of the Company. The Company does not assume liability for loss, damage or wear of Employee-owned equipment.

Employee agrees to designate a work space within Employee's remote work location for placement and installation of equipment to be used while working. Employee shall maintain this workspace in a safe condition, free from hazards and other dangers to Employee and equipment. The site chosen as the Employee's remote workplace must be approved by the Company. If any changes to the initial installation and set-up location of telecommunications equipment by the Company, Employee is responsible for expenses.

Employee agrees that Company may make on-site visits to the remote work location for the purpose of determining that the site is safe and free from hazards, and to maintain, repair, inspect or retrieve Company-owned equipment, software, data and/or supplies. In the event legal action is necessary to regain possession of Company-owned equipment, software, data and/or supplies. Employee agrees to pay all cost of suit incurred by Company, including attorney's fees, should Company prevail.

In the event of equipment failure or malfunction, Employee agrees to immediately notify Company in order to effect immediate repair or replacement of such equipment. In the event of delay in repair or replacement, or any other circumstance under which it would be impossible for Employee to telecommute, Employee understands that Employee may be assigned to do other work and/or assigned to another location, at Company's sole discretion.

Furniture, lighting, environmental protection and household safety equipment incidental to use of Company-owned equipment, software and supplies shall be appropriate for their intended use and shall be used and maintained in a safe condition, free from defects and hazards.

TELECOMMUTING AND INCIDENTAL EQUIPMENT con't

Employee agrees that all Company-owned data, software, equipment, facilities and supplies must be properly protected and secured. Company-owned data, software, equipment and supplies must not be used to create Employee-owned software or personal data. Employee will comply with all Company policies and instructions regarding conflicts of interest and confidentiality. Any software, products or data created as a result of work-related activities are owned by Company and must be produced in the approved format and medium. Employee agrees that upon termination of employment, Employee will return to Company all things belonging to Company.

LIABILITY FOR INJURIES

Employee understands that Employee remains liable for injuries to third persons and/or members of Employee's family on Employee's premises. Employee agrees to defend, indemnify and hold harmless Company, its affiliates, employees, contractors and agents from and against any and all claims, demands or liability (including any related losses, costs, expenses and attorneys fees) resulting from or arising in connection with any injury to persons (including death) or damage to property, caused directly or indirectly, by the services provided hereunder by Employee or by Employee's willful misconduct or negligent acts or omissions in the performance of Employee's duties and obligations under this Agreement, except where such claims, demands or liability arise solely from the gross negligence or willful misconduct of the Company.

MISCELLANEOUS CONDITIONS

Employee agrees to participate in all studies, inquiries, reports or analyses relating to telecommuting for Company, including inquiries which Employee might consider personal or privileged. Company agrees that Employee's individual responses shall remain anonymous on request by Employee, but that such data may be compiled and made available to the general public without identification of Employee.

Employee remains obligated to comply with all Company rules, policies, practices, instructions, and this Agreement and understands that violation of such may result in a preclusion from telecommuting and/or disciplinary action, up to and including termination of employment.

I affirm by my signature below that I have read this agreement and understand its subject matter. I affirm that I was given the opportunity to have this agreement reviewed by my own counsel prior to entering into it.

Employee's Signature: _____

Date: _____

TELECOMMUTING AGREEMENT

Telecommuting, or working from another location such as home, is an assignment that may choose to make available to some employees when a mutually beneficial situation exists.

Telecommuting is not an employee benefit, but rather is an alternate method of meeting the needs of this Company. Employees do not have a "right" to telecommute; the arrangement can be terminated by the Company at any time.

These are the conditions for telecommuting agreed upon by the telecommuter and his or her supervisor:

1) The employee agrees to work at the following location;

2) The employee will telecommute _____ days per week.

3) The employee's work hours will be as follows:

4) The following are the assignments to be worked on by the employees at the remote location with the expected delivery dates:

5) The following equipment will be used by the employee in the remote work location:

6) The following is the arrangement agreed upon for handling telephone calls made by the telecommuter from the remote work location for Company business:

7) The employee agrees to obtain from _____ all supplies needed for work at the alternate location; out-of-pocket expenses for supplies regularly available at the Company office will not normally be reimbursed.

8) Employee will be required to make regular visits to the _____ Center to attend training and team/supervisor meetings.

I have reviewed the above material with _____ prior to his or her participation in the Company's telecommuting program.

Date _____

Supervisor's Signature_____

The above material has been discussed with me.

Date _____

Employee's Signature_____

Annex B

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

CHAPTER II

Basic Principles For Data Protection

Article 4

Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5

Quality of Data

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6

Special Categories of Data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7

Data Security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

Article 8

Additional Safeguards for the Data Subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity of habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9

Exceptions and Restrictions

1. No exception to the provisions of Articles 5, 6, and 8 of this convention shall be allowed except within the limits defined in this article.
2. Derogation from the provisions of Articles 5, 6, and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offenses;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c, and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10

Sanctions and Remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11

Extended Protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

Annex C

Names and Addresses of National Organisations

Unless otherwise noted, further information should be sought from the organizations noted with an asterisk (*).

Australia

Financial Service Trade Association

Australian Bankers Association
42/55 Collins Street
MELBOURNE NSW 2140
Phone 61 3 654 5422
Fax 61 3 650 1756

Central Bank

Reserve Bank of Australia
65 Martin Place
SYDNEY NSW 2000
Phone 61 2 551 8111
Fax 61 2 906 8535

Taxation Authority

Australian Taxation Office
Commissioner of Taxation
21 Constitution Avenue
CANBERRA ACT 2600
Phone 61 6 275 2222
Fax 61 6 216 2743

Government Standards Body - Weights and Measures

National Standards Commission
12 Lyon Park
NORTH RYDE NSW 2113
Phone 61 2 888 3922

National Standards Body *

Standards Australia
1 The Crescent
HOMEBUSH NSW 2140
Phone 61 2 746 4700
Fax 61 2 746 8450

IT/5/4 Authentication & Security, Financial Transaction Systems

Producer of Building Codes

Standards Australia

Producer of Electrical Codes

Standards Australia

Producer of Fire Codes

Standards Australia

Other sources

Standards Australia
IT11 EDI
IT 11/3 EDI Security

Belgium

Bankers Association

Association belge des Banques
Rue Ravenstein 36 bte5
B- 1000 Bruxelles
Belgium
Phone: 32 2 507 68 11
Fax: 32 2 507 69 59

Central Bank

Banque nationale de Belgique
Boulevard de Berlaimont 5
B- 1000 Bruxelles
Belgium
Phone: 32 2 221 21 11
Fax: 32 2 221 31 00

National Standards Body

Institut belge de normalisation (IBN)*
Avenue de la Brabançonne 29
B- 1000 Bruxelles
Belgium
Phone: 32 2 738 01 11
Fax: 32 2 733 42 64

Canada

Financial Services Associations

Canadian Bankers Association
199 Bay Street, Suite 3000
P.O. Box 348, Commerce Court Postal Station
TORONTO, Ontario M5L 1G2

Phone: 416-362-6092
Fax: 416-362-7705

Canadian Payments Association
1212 - 50 O'Connor Street
OTTAWA, Ontario K1P 6N7

Phone: 613-238-4173
Fax: 613-233-3385

Central Bank

Bank of Canada
234 Wellington Street
OTTAWA, Ontario K1A 0G9
Phone: 613-782-8111
Fax: 613-782-8655

National Standards Body

Standards Council of Canada
1200 - 45 O'Connor Street
OTTAWA Ontario K1P 6L2

Phone: 613-238-3222
Fax: 613-995-4564

National Standards Writing Organisations

Canadian Standards Association
178 Rexdale Boulevard
REXDALE, Ontario M9W 1R3

Phone: 416-747-4044
Fax: 416-747-2475

Canadian General Standards Board
222 Queen Street, Suite 1402
OTTAWA, Ontario K1A 1G6

Phone: 613-941-8709
Fax: 613-941-8706

Taxation Authority

Revenue Canada
OTTAWA, Ontario K1A 0L5

Phone: 613-995-2960
Fax: 613-952-6608

Government Standards

Supply & Services Canada
45, Sacré-Coeur Boulevard
HULL, Quebec K1A

Phone: 819-956-4800 or 4802

Also of Interest

Interac Association
121 King Street West, Suite 1905
P.O. Box 109
Standard Life Building
TORONTO, Ontario
M5H 3T9
Phone: 416-362-8550
Fax: 416-362-2993

Finland

Financial Service Trade Association

The Finnish Bankers' Association*
P.O. Box 1009
FIN 00101 HELSINKI
Phone +358-9-4456 120
Fax +358-9-4056 1291

Central Bank

Bank of Finland
P.O. Box 160
FIN 00101 HELSINKI
Fax +358-9-174 872

Bank Examiners

Financial Supervision
P.O. Box 159
FIN 00101 HELSINKI
Fax +358-9-183 5328

National Standards Body

Suomen Standardisoimisliitto SFS ry
P.O. Box 116
FIN 00241 HELSINKI
Phone +358-9-149 9331
Fax +358-0-146 4925

Producer of Telecommunications Codes

Telecommunications Administration Centre
P.O. Box 53
FIN 00211 HELSINKI
Phone +358-9-696 61
Fax +358-9-696 6410

Security Inspection for EFTPOS Terminals

SETEC Oy
P.O. Box 31
FIN 01741 VANTAA
Phone +358-9-894 11
Fax +358-9-891 887

Italy

Financial Service Trade Association

ASSOCIAZIONE BANCARIA ITALIANA
piazza del Gesu, 49
00187 Rome
tel. +39-6-67671

Central Bank

BANCA D'ITALIA
via Nazionale, 91
00187 Rome
tel. +39-6-47921

Bank Examiners

UFFICIO ITALIANO CAMBI
via quattro Fontane, 123
00184 Rome
tel. +39-6-46631

CONSOB
via Isonzo, 19
00198 Rome
tel. +39-6-8477300

Taxation Authority

MINISTERO DELLE FINANZE
viale Boston
00144 Rome
tel. +39-6-59971

National Standards Body

UNI ENTE NAZIONALE ITALIANO DI UNIFICAZIONE
via Battistotti Sassi, 11
20133 Milan
tel. +39-2-70105955

UNINFO*
corso G. Ferraris, 93
10138 Turin
tel. +39-11-501027/591964

Producer of Electrical Codes

CEI
viale Monza, 259
20126 Milan
tel. +39-2-25771

the Netherlands

All inquiries should be made to:

Nederlands Normalisatie-instituut
P.O. Box 5059
2600 GB Delft
Netherlands
tel. +31 15 690 126
fax. +31 15 690 242
E-Mail: john.bijlsma@nni.nni.400net.ne

Japan

Financial Service Trade Association

Federation of Bankers Associations of Japan

Central Bank

Bank of Japan*
Institute for Monetary and Economic Studies
2-1-1 Hongoku-cho Nihonbashi, Chuoku
Tokyo 103
tel. +81-3-3277-1483
fax: +81-3-3277-1473

Bank Examiners

Bank of Japan
Ministry of Finance

Taxation Authority

Ministry of Finance

Government Standards Body

Agency of Industrial Science and Technology
Ministry of International Trade and Industry

Producer of Building Codes

Ministry of Construction

Producer of Electrical Codes

Ministry of International Trade and Industry

Producer of Fire Codes

Ministry of Home Affairs

United Kingdom

NOTE — Some services are specific to Scotland or Northern Ireland and are dealt with separately to the rest of the United Kingdom. Where these exist, separate address have been provided.

Financial Service Organisations

Association for Payment Clearing Services
Mercury House, triton Court
14 Finsbury Square
LONDON, EC2A 1BR

British Bankers Association
10 Lombard Street
LONDON, EC3V 9AA

Confederation for British Industry
Centre Point
103 New Oxford Street
LONDON, WC1A 1DU

Standards Bodies

British Standards Institute
PO Box 375
MILTON KEYNES, MK13 6LE

Fire and Building Regulators

Department of the Environment
Building Regulation Division
2 Marsham Street
LONDON SW1P 3EB

Home Office
Fire Safety Division
50 Queen Anne Gate
LONDON SW1H 9AT

Health & Safety Commission

Baynards House
1 Chepstow Place
Westbourne Grove
LONDON W2 4TF

Government Regulators

Data Protection Register
Wycliff House
Water Lane
WILMSLOW CHESHIRE SK9 5AF

Office of Electricity Regulation
11 Belgrave road
LONDON SW1

Office of Gas Supply
Southside
105 Victoria Street
LONDON SW1E 6QT

Office of Water Services
15 Ridgemount Street
LONDON WC1E 7AU

Office of Telecommunications
Export House
50 Ludgate Hill
LONDON EC4M 7JJ

Personal Investment Authority (PIA)
3-4 Royal Exchange Buildings
LONDON EC3V 3NL

Telephone Wiring

Institute of Electrical Engineers
Savoy Place
LONDON WC2R

Government Standards Bodies

Department of Trade and Industry
Commercial IT Security Group
Technology Programme Services Division
151 Buckingham Palace Road
LONDON SW1W 9SS

Central Bank

Bank of England
Threadneedle Street
LONDON EC2R 8AH

Taxation Authority

Inland Revenue
Lancaster House
70 Newington Causeway
LONDON SE1

Examiners of Financial Institutions

Accountant and Controller General
National Audit Office
Lancaster House
70 Newington Causeway
LONDON SE1

Securities and Investment Board (SIB)
2 Bunhill Row
LONDON EC1Y 8RA

Investment Management Regulatory Organisation (IMRO)
Broadwalk House
5 Appold Street
LONDON EC2A 2LL

Life Assurance & Unit Trust Regulatory Organisation (LAUTRO)
Centrepoint
103 New Oxford Street
LONDON WC1A 1QH

SCOTLAND SPECIFIC

Committee of Scottish Clearing Banks
19 Rutland Square
EDINBURGH EH1 2DD

Heath & Safety (Scottish Directorate)
Belford House
59 Belford Road
EDINBURGH

Scottish Offices (Includes Fire and Building Regulation)
Central Services Head Office
St. Andrews House
EDINBURGH EH1 3DE

NORTHERN IRELAND SPECIFIC

Fire Authority for Northern Ireland
Administrative Head Office
1 Seymour Street
LISBON

Department of the Environment (Northern Ireland)
(includes Building and Planning Regulations)
Stormont
BELFAST 4

Health and Safety Agency for Northern Ireland
Canada House
North Street
BELFAST 1

United States

Financial Services Organisations

American Bankers Association
Security and Risk Management Division
1120 Connecticut Avenue
Washington, DC 20036
202-663-5308

Bank Administration Institute Foundation
2550 Golf Road
Rolling Meadows, Illinois 60008-4097

Standards Bodies

Accredited Standards Committee X9, Financial Services
Secretariat, American Bankers Association*
Standards Department
1120 Connecticut Avenue
Washington, DC 20036
202-663-5284

Accredited Standards Committee X12,
Electronic Data Interchange
The Data Interchange Standards Association, Inc.
1800 Diagonal Road
Suite 355
Alexandria, VA 22314-2852

Government Standards Body

National Institute for Standards and Technology
Gaithersburg, MD 20899

Producer of Fire Codes

National Fire Protection Association
Post Office Box 9101
Quincy, MA 02269

Producers of Building Codes

International Conference of Building Officials
5360 South Workman Mill Road
Whittier, CA 90601

Building Officials and Code Administrators International
17926 South Halsted Street
Homewood, IL 60430

Southern Building Code Conference International
900 Montclair Road
Birmingham, AL 35213

Producer of Electrical Codes

Institute of Electrical and Electronic Engineers
445 Hoes Lane
Post Office Box 1331
Piscataway, NJ 08855

Telephone Wiring

Federal Communications Commission
1919 M St. NW
Washington, DC 20554
- See part 68 of FCC Regulations

Government Regulators

Central Bank

Board of Governors of the
Federal Reserve System
Washington, DC 20551
-See regulations J, E, and P

Also of interest:

Security Steering Group Chairman
Federal Reserve Bank of Atlanta
104 Marietta Street, NW
Atlanta, GA 30303

Examiners of Financial Institutions:

In addition to the central bank, these government agencies have supervision responsibilities over some financial services institutions. No attempt is made to here to identify the jurisdiction of these agencies.

Office of the Comptroller of the Currency
250 E Street SW
Washington, DC 20219

- See Banking Circulars BC 229, BC 226, BC 187, BC 177, BC 119, and Advisory letter AL 91-4.

Federal Deposit Insurance Corp.
550 17th Street, NW
Washington, DC 20429

Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

Resolution Trust Corporation
801 17th Street NW
Washington, DC 20552

National Credit Union Administration
1776 G Street, NW
Washington, DC 20456

Security and Exchange Commission
450 5th Street NW
Washington, DC 20549

Taxation Authority

Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224
-See section 5 of Revenue Procedure 91-59

Annex D
Other security standards

This list includes security standards under development outside of the financial industry. This list does not include ANSI X9 or ISO TC68 standards.

Cryptographic Standards

These are standards for cryptographic algorithms or techniques.

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*. This is basically RSA and Rabin signatures; it forms the basis of ANSI X9.31 Part 1 as well.

ISO/IEC 9797, *Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm*. How to generate an *m*-bit MAC with an *n*-bit cipher algorithm; a generalization of X9.9.

ISO/IEC 9798 (all parts), *Information technology — Security techniques — Entity authentication*. A 3-part standard consisting of Model, Symmetric Techniques, and Asymmetric Techniques.

ISO/IEC 9979, *Data cryptographic techniques — Procedures for the registration of cryptographic algorithms*. The ISO registry of algorithms.

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*. I believe this might include a registry function as well.

ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*. Another multi-part standard. Part 3 discusses public key techniques in an algorithm-independent fashion.

PKCS #1: RSA Encryption. Padding mechanisms for RSA encryption and signature, along with ASN.1 key formats.

PKCS #3: Diffie-Hellman Key Agreement. Simple Diffie-Hellman exchange, and ASN.1 key formats.

PCKS #5: Password-Based Encryption. How to derive a symmetric key from a password, using a hash function.

Secure Session Protocols

These standards provide a way to secure communications between two entities.

ISO/IEC 10736, *Information technology — Telecommunications and information exchange between systems — Transport layer security protocol*. Provides transport layer security.

ISO/IEC 11577, *Information technology — Open Systems Interconnection — Network layer security protocol*. Provides network layer security.

IEEE 8012.10 (SILS) provides confidentiality and integrity (and access control) at layer 2 for LANs. The encapsulation protocol is similar to that used in NLSP and TLSP. See below for the associated key management protocol.

The *IP Security Protocol (IPSP)* is a new set of standards to provide confidentiality and integrity on the Internet, by encapsulating IP datagrams.

The *Secure Socket Layer (SSL)* is a proposed Internet standard for securing data at the socket layer (between the application and TCP). It provides server and (optionally) client authentication, integrity (using a keyed hash function), and confidentiality (using DES, triple DES, RC4, or IDEA). Microsoft has proposed an enhanced

version of SSL called Private Communications Technology (PCT); it's likely these two proposals will be merged into one.

The *Simple Public Key Mechanism (SPKM)* provides application-layer confidentiality, integrity, and authentication. It is meant to be used with GSS-API; the security processing is performed underneath the API and is relatively transparent to the application. It is algorithm-independent, and is currently an Internet Draft. For symmetric algorithms, the analogous mechanism is *RFC 1510 (Kerberos)*, which uses a key center for client authentication and session key distribution.

Secure Message Formats

This section describes message formats, which might be used for Email, EDI, and other store-and-forward applications.

X.400 is an international standard for message handling systems (MHS). It defines the components of an MHS and the protocols between them. Origin authentication and integrity are provided using either a MAC or a digital signature. The MAC key may be conveyed in the digital envelope, which also conveys the bulk encryption key used to provide confidentiality. Non repudiation is provided using digital signatures. X.400 security elements are placed in the message envelope, along with addressing and other information. X.400 provides a variety of additional security services, including many which protect the operation of the message transfer system itself e.g., authentication between adjacent MHS components).

X.435 is an X.400 content type which is used to convey EDI interchanges. X.435 provides a number of additional security services, built on the underlying X.400 services. For example, non repudiation of received content is provided by signing an EDI notification containing the signature from the originally received EDI message (interchange).

ANSI ASC X12 defines formats for Electronic Data Interchange (EDI). EDI supports the communication of business transactions between entities. The format is three-tiered, with individual *transaction sets* enveloped into *functional groups,* which are then enveloped into an "interchange" which is conveyed between the entities. Interchanges may be transported over a variety of communications protocols and media. X12.58 (version 2) defines security structures for EDI. Origin authentication and integrity can be provided using a digital signature or MAC, with no repudiation being provided if digital signatures are not used. Confidentiality is provided using digital envelopes; the envelope may be encrypted under the recipient's public key, or under a shared symmetric key. EDI is inherently point-to-point, so there is no support for multiple recipients. Support for multiple signatures is provided, and a variety of signature attributes are defined, including signature purpose, timestamp, and "assurance text".

PKCS #7: Cryptographic Message Syntax was developed by RSA Data Security, Inc., and its licensees. Origin authentication, integrity, and non repudiation are provided using digital signatures, and confidentiality is provided using digital envelopes. Multiple recipients are supported. Multiple signatures and countersignatures are supported. A variety of signature attributes are defined including timestamp, signature purpose, role, and comments, and user-defined attributes may easily be added. PKCS #7 forms the basis of the X9.30-3 multiple signature syntax.

The *Message Security Protocol (MSP)* was developed by DoD as part of the Security Data Network Systems (SNS) program. It provides an ASN.1 structure for a secure message. Although originally designed to be carried over X.400, MSP messages can easily be conveyed over any mail transport supporting 8-bit transparent communication. Origin authentication and non repudiation are provided using digital signatures. Integrity is provided by conveying a hash of the message in the digital envelope (along with the message encryption key). The envelope is encrypted under a symmetric key computed using a key agreement algorithm; multiple recipients are supported. Public key management is done using certificates.

Privacy Enhanced Mail (PEM) was developed by the Internet Engineering Task Force. In many ways, PEM is an Internet (text-based) version of MSP. Origin authentication, integrity, and non repudiation are provided using digital signatures. Confidentiality (to multiple recipients) is provided using digital envelopes. Encrypted data (and optionally signed data) is encoded into a 7-bit representation for transport; this encoding increases the size of the data by 33%. Public key management is done using certificates. PEM is currently available as a set of Internet RFCs.

MIME Object Security Services (MOSS) is an alternative to PEM. It can provide the same services as PEM, but the message format is restructured, to place signature information and digital envelope information in separate

body parts from the message. (PEM places all this information in message headers.) As with PEM, encrypted (and optionally signed) data is encoded into a 7-bit character set prior to transmission. This structure is superior to PEM in some respects. In particular, it is easy to extend MOSS (using standard MIME mechanisms such as multipart messages and new content types) to accommodate multiple signatures and signature attributes. MOSS supports certificate-based public key management, but also allows other mechanisms. These range from conveying the public key itself within the message, to conveying the name or Email address of the signer in the message, with another body part containing the corresponding public keys (with the body part signed by a trusted third party). One concern about this approach is that, depending on the mechanism used and the protection (or not) of the public keys, the user may get the level of trust he is expecting. RFCs for MOSS were published last month.

S/MIME is a new proposal from RSADSI to encapsulate MIME messages within the PKCS #7 format. The resulting PKCS #7 message is conveyed as a MIME body part. This format provides all of the PKCS #7 security services. It was proposed as an alternative to MOSS. Both MOSS and PKCS #7 are cryptographically compatible with PEM, but there is some concern about the potential security weaknesses which might be introduced by using non-certificate-based MOSS key management.

Pretty Good Privacy (PGP) is a freeware package that signs and encrypts messages. It used IDEA for bulk encryption, and RSA for key management and signature, and provides all of the basic security services. No certificates are required; key management is done by face-to-face interchange of public keys, or "introduction" by some entity that two parties both trust (effectively, a one-level CA hierarchy). The scalability of this approach is very doubtful.

Key Management

ISO/IEC 9594-8 (X.509), *Information technology — Open Systems Interconnection — The Directory: Authentication framework* is the Directory Authentication Framework. It defines several authentication protocols, as well as the use of certificates for public key management.

IEEE 802.10c defines protocol for key management and security attribute negotiation for LAN security. The protocol is open-ended, and X9F3 has adopted it as the protocol for X9.41 (Security Services Management). The protocol can use either symmetric or asymmetric algorithms to establish a key for protection of attribute negotiation (and optionally application data transfer).

Photuris is a proposed key management protocol of IPSP. It uses Diffie-Hellman key exchange, and RSA or DSS signatures. It also includes a novel mechanism to defend against "clogging" (denial of service by flooding with bogus IP datagrams), based on the use of tokens ("cookies") which can be authenticated without using public key computation. The use of cookies prevents replay of IP packets with random addresses, so an adversary must either use their own address (allowing easy detection) or subvert the Internet routing protocols.

Simple Key Management for IP (SKIP) is another proposed IPSP key management protocol. It also uses Diffie-Hellman for key agreement, and RSA or DSS for signature. However, the derived key is used to encrypt a short-term (possibly one-time) packet encryption key, to limit exposure of the derived key.

Payment Protocols

This section presents current proposals for payment protocols. These are all (with the possible exception of STT) currently entering the IETF standards process. They all use the existing credit card networks for interbank-clearing.

The *Secure Electronic Payment Protocol (SEPP)* was produced by IBM, MasterCard, GTE, Netscape, and Cybercash. It uses X.509 certificates (with v3 extensions) for the cardholder, merchant, and acquirer. RSA is used for signature and key transport, and DES is used for bulk encryption. Note this is for payments only; other message traffic (e.g., browsing and setting up an order) would be secured with something like SSL. This lets SEPP take advantage of the export controls on financial cryptography. SEPP includes a complete CA architecture, as well. Cardholder names do not appear in certificates; simple "pseudonymous" serial numbers are used. Cardholder certificates may be issued online (authorization for issuance comes from the card issuer via extensions to the current credit card message set). The PIN is not used in the protocol (although it will be during the certificate registration process); a separate 360-bit random code is used. IBM has documented the abstract version of the protocol, as an Internet draft and on the World Wide Web (WWW). The SEPP protocol encodes messages in ASN.1, and uses PKCS #7 message structures wherever possible.