TC 68

TECHNICAL REPORT

ISO/TR 13569

First edition
1996-11-15

Banking, securities and other financial services — Information security guidelines

Banque, valeurs mobilières et autres services financiers — Lignes directrices pour la sécurité de l'information

Reference number
ISO/TR 13569:1996(E)

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
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 Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.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 Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 2, *Strategy, security and general operations*.

Banking, securities and other 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 8730:1990, *Banking - Requirements for message authentication (wholesale).*

ISO 8732:1988, *Banking - Key management (wholesale).*

ISO 9564-1:1991, *Personal Identification Number management and security - Part 1: PIN protection principles and techniques.*

ISO 9564-2:1991, *Personal Identification Number management and security - Part 2: Approved algorithm(s) for PIN encipherment.*

ISO 10126-1:1991, *Banking - Procedures for message encipherment (wholesale) - Part 1: General principles.*

ISO 10126-2:1991, *Banking - Procedures for message encipherment (wholesale) - Part 2: DEA algorithm.*

ISO 10202:1991-1996, *Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards* (all parts).

National Standards:
ANSI X9/TG-2, *Understanding and Designing Checks* (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.

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 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 guideline 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. An excerpt from the US Office of the Comptroller of the Currency, Banking Circular BC-226 Policy Statement illustrates this concern.

> "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 programme.

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 programme. It sets out minimum requirements for an adequate information security programme. It may also serve as a measure against which an institution can evaluate the state of its information security programme.

Clause 6: Information security programme components: This clause contains more specific information on how an Information Security Programme 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 programme.

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 cheque processing subclauses finish this clause.

Clause 8: Sources of further help: This clause lists the types of organisations 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: Sources of Further Assistance: This annex lists the names and contact information for national organisations which can be of assistance to Information Security personnel.

5 Requirements

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 centred 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 programme requires participation by multiple disciplines in the organisation. 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 programme. Information security is a team effort and an individual responsibility.

The basic requirement of this technical guideline is the establishment of an information security programme 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 programme,

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 programme 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 programme,

j. provides for the review and update of the programme 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 programme components

Subclause 6.1 addresses the information security responsibilities within the institution. Subclauses 6.2 and beyond address 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 managment 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 programme.

6.1.2 Chief Executive Officer

The Chief Executive Officer, 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 programme 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 programmes. 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 Inforamtion 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 programme,
- 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.

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

- be responsible for the classification of information or information processing systems he controls.
- 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 organisational 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. Chinese Walls.

NOTE — Security programme 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 programme 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 programme for protecting the information assets of the institution.

The Information Security Officers should:

- manage the overall information security programme,

- have responsibility for developing Information Security Policies and Standards for use throughout the organisation. 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

- apply management and organisational 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 programmes,

- 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 organisation'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 programme 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.

6.3 Insurance

In planning the information security programme, 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 programme 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 programme. 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 organisation to examine and evaluate its activities as a service to the organisation. The objective of internal auditing is to assist members of the organisation 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 Programme 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 that 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 Programme is to promote information security. The programme 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 Programme is directly related to the Information Security Officer's ability to gain support and commitment from all levels of staff within the organisation. Failure to gain this support reduces the programme's effectiveness.

Without Management support, the information security programme 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 guideline examines these areas in more detail.

To function properly, the Information Security Programme 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 Programme 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 organisation of the institution to better protect and advise the institution. By acting in concert with other groups within the organisation, 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 programme, 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 programme 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.

6.9 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.

6.10 Privacy

Financial institutions possess some of the most sensitive information about individuals and organisations. 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 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 European 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 relevant and accurate information 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 2 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 cheques 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.

It is most important that the institution address all 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 programme 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.

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 organisation 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 clause. 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 clause 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

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.

- use distress passwords for sensitive operations.

- 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 organisational terminology would provide better checking.

- consider requiring that passwords include both alphabetical and numerical components.

- forbid the writing down of passwords.

- 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.

7.3 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-out 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 centre 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 centre" is becoming increasingly rare. However, there may be circumstances when physical controls may be adequate.

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

- chose the site of processing areas away from flight paths, geologic fault lines, powerlines, 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 programme.

- 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.

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 go through a secure erasure procedure prior to disposal.

7.5.10 Distributed Computing

The increased use of connected mini and micro computers in normal business premises to store business information may result in greater risks to the information, due to the somewhat lower physical security controls than normally applied to mainframes.

To minimize this increased vulnerability,

- impose more stringent logical access controls on computers executing distributing computing than would ordinarily be applied to the same information stored in a mainframe computer.

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, 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.

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 eanble corruption or modification of HIGHLY SENSITIVE information during transmission to be detected,

- 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

7.7 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 monitered 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)

Application 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 processed or the impact of decisions made.

7.7.4 System software

System software is that set of instruction which function as 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 programme 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 Remote control

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

- require remote control 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

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.

7.8 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 programme. 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 programme, a communications and awareness programme 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.

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 programme,

- 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 programme 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 cheques, 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.

7.9 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 (wiretap) of cellular and cordless telephone conversations has become 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 Programme, 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 cheques.

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.

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.

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 programme appropriate to business and regulatory requirements.

- purge unread and unsaved messages after a specified time.

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 cheques and currency. Cheques 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 Labeling

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 programmes, 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 used 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 were 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 Cheques

Cheques, 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 cheques should raise security concerns to financial institutions. Cheque-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 cheque processing operations. Particular attention is drawn to ANSI X9/TG-2, Understanding and Designing Checks. To achieve consistency among financial institutions and improved processing performance, financial institutions are strongly urged to follow the recommendations of X9/TG-2.

8 Sources of further help

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

8.1 Financial Services institutions

Financial services institutions or trade organisations 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.

8.2 Standards bodies

National standards organisations can provide financial and non-financial standards on security issues. Participation in these bodies can proved useful in learning of security concerns of others. Use of standards promote interoperability as well as help secure operations.

8.3 Building, fire, and electrical codes

Adherence to these codes promote a safer, more secure environment.

8.4 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 identify 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.

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.

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.

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 user.

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 programme 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 programme 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 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 include 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.

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: SENSITIVE

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 organisations noted with an asterisk (*).

Australia

Financial Service Trade Association

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

Central Bank

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

Taxation Authority

Australian Taxation Office
Commissioner of Taxation
21 Constitution Avenue
CANBERRA ACT 2600
Tel. 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
Tel. 61 2 888 3922

National Standards Body *

Standards Australia
1 The Crescent
HOMEBUSH NSW 2140
Tel. 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
Tel. 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
Tel. 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
Tel. 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
Tel. 416-362-6092
Fax 416-362-7705

Canadian Payments Association
1212 - 50 O'Connor Street
OTTAWA, Ontario K1P 6N7
Tel. 613-238-4173
Fax 613-233-3385

Central Bank

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

National Standards Body

Standards Council of Canada
1200 - 45 O'Connor Street
OTTAWA Ontario K1P 6L2
Tel. 613-238-3222
Fax 613-995-4564